TLP:CLEAR

CENTRE FOR
CYBERSECURITY
BELGIUM

CLOUD THREAT LANDSCAPE

CYBER THREAT INTELLIGENCE REPORT

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: 20 November 2024
Version: 1.0 EN
Author: CyTRIS, intelligence (CTI) department of the CCB

Target audience:
Organisations using cloud environments on strategic and operational level (especially SMEs), cloud vendors, cloud risk managers.

Permitted distribution of TLP:CLEAR:
Disclosure is not limited.
More information: https://www.first.org/tlp/

Table of Contents

EXECUTIVE SUMMARY

In 2023, the average cost of a data breach hit USD 4.45 million, a 2.3% increase from USD 4.35 million in 2022[1]. **Notably, 82% of these data breaches involved cloud-stored data, encompassing both public and private environments, with 39% affecting multiple environments**[2]. Moreover, cloud security breaches became more costly due to the longer time needed to identify and contain them. Companies with 500 to 5,000 employees saw data breach costs rise by at least 20% from 2022. This highlights the accumulating challenges in cloud security.

Given the specific characteristics of cloud environments and the capabilities of adversaries, **it is very likely that cloud environments will increasingly become favoured targets for threat actors in the coming years**.

The growing reliance on cloud environments by companies is expected to accelerate due to the accessibility and cost-effectiveness of cloud solutions. As cloud adoption increases, threat actors are evolving their tactics to exploit the expanding landscape of potential victims.

Many organisations struggle with selecting appropriate cloud deployment models and services, often resulting in overwhelmed and disorganized cloud environments. Unlike on-premises infrastructures, cloud environments offer unique features such as scalability and integration with third-party components. Additionally, **confusion over delineating responsibilities in the shared responsibility model leads to issues like shadow IT**.

Cloud environments come with multiple risks, including scaling attacks, cryptojacking, third-party reliability concerns, and supply chain attacks. Studies indicate that cloud environments are frequently misconfigured, creating vulnerabilities that adversaries can easily exploit. Small and medium-sized enterprises (SMEs) are particularly vulnerable and often targeted by attackers, as they lack the resources and knowledge to fully secure their assets. Despite these misconfigurations, phishing attacks remain the most exploited method for breaching organisations, as the human factor is the weakest link in defences. Adversaries primarily exploit existing, legitimate accounts that lack multi-factor authentication (MFA) to breach and manoeuvre within cloud environments.

[1] IBM, *"Cost of a Data Breach Report 2024"*, https://www.ibm.com/downloads/cas/1KZ3XE9D, p. 4.
[2] K. Chin, *"What is the Cost of a Data Breach in 2024?",* https://www.upguard.com/blog/cost-of-a-data-breach-2024, UpGuard, 28 October 2024.

Despite these challenges, solutions are available for managing cloud environments. **The most essential security measure is multi-factor authentication (MFA), as it forms the very core of cloud environment security.** Organisations can adopt other various security measures as presented also in the Appendix D.

The ongoing issue of unsecured clouds can be addressed by individuals or more capable and knowledgeable entities like vendors and corporations responsible for cloud solutions. By employing strategies like security by default, security by design, and opt-out options, these entities can significantly enhance the security of their cloud solutions, alleviating the burden on less capable SMEs and individuals.

Data from threat sources reveals dangerous new trends such as **cryptojacking** and **big game hunting**, with threat actors specifically targeting cloud environments using various malware and techniques. Recent security incidents underscore these emerging threats. According to various threat intelligence data, the most active actors targeting cloud environments mainly originate from **Russia** and **China**.

While cloud environments face significant threats, implementing robust security measures like multi-factor authentication can greatly mitigate these risks. Vigilance and proactive strategies from vendors and organizations are essential to stay ahead of evolving threats and ensure the security of cloud solutions.

INTRODUCTION

This report is designed for organisations that currently possess cloud environments or are in the process of moving their assets to the cloud. It aims to help them understand the fundamental principles of cloud environments and the associated issues.

The report is intended to **assist organisations in making informed decisions regarding their cloud environments** by catering to both the technical and managerial parts of the organization. It presents data in a way that facilitates coordination between these two groups and helps organisations manage their risks, focus on the most crucial aspects of cloud environments, and provides best practices for managing and securing these environments.

Additionally, the report offers live data on trends, predictions, and ongoing threats in cloud environments, enabling organisations to understand the threat landscape and direct their efforts towards addressing essential issues.

An important aspect of this report is raising awareness among affiliated cloud vendors and associated organisations about the increasing threats in cloud environments. Its purpose is to inform and motivate these stakeholders to adopt and implement unified security practices by default at the production level.

In conclusion, this report also addresses cloud providers and vendors, emphasizing the significance of their role in making cloud environments safer for everyone.

Scope

The report focuses on the leading cloud providers dominating the cloud services market, covering the most widely used cloud models and solutions.

This report primarily encompasses the following key sections:

1. **Essential knowledge regarding cloud environments**
    - Detailed specifications and characteristics of various cloud environments, solutions, architectures, and unique features.
2. **Advantages and Disadvantages of Cloud Environments**
    - Analysis of the benefits and potential drawbacks of adopting cloud solutions.
3. **Main providers and their cloud services**
    - Overview of the leading cloud service providers.

4. **Security aspects of cloud environments**
    - In-depth analysis of the present state of cloud security, leading security issues, and common targets of threat actors in the cloud.
5. **Security measures for cloud environments**
    - Strategies and methodologies for mitigating risks, along with practical solutions to address security challenges in cloud settings.
6. **Main threats against cloud environments**
    - Examination of current and emerging trends within cloud computing, including dangerous threats, detailed cases of security incidents, changes in techniques employed by attackers, technological advancements, and market dynamics.
7. **Legislation related to cloud security**
    - Overview of the legal frameworks and directives related to cloud security.
8. **Conclusions and outlook**
    - Summarized insights and actionable conclusions derived from the analysis of trends and threats, providing guidance for future actions and improvements.

What is the cloud?

Organisations and people often perceive the cloud as something extraordinary, difficult to comprehend, and out of reach. In fact, **the cloud is simply a network of interconnected servers and devices, designed to operate as a single ecosystem or several micro-ecosystems**. These interconnected systems might sometimes differ in operational system's distribution or hardware, but they typically function similarly to standard desktop devices in terms of logic and operation[3].

The main idea behind the cloud is to provide scalable, on-demand access to computing power, services, applications, and data from anywhere with an internet connection. The cloud allows users to access their files from multiple devices, whether it's their work computer, personal phone while traveling abroad, or any other device located anywhere in the world. By logging into their cloud account, users can retrieve their data.

How does it actually differ from a regular client-server model? Specifically, cloud instances do more than just respond to requests from clients to servers. In addition to responding to client requests, cloud instances run services or programs and store

[3] Microsoft, *„What is the cloud?",* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud, 22 October 2024.

customer data. This makes cloud computing more complex than a traditional client-server relationship.

Cloud deployment models

There are five main models of cloud deployment:

- **Public Cloud** shares resources across multiple organisations over the Internet. It can be used by various organisations simultaneously, as it supports multi-tenancy.
- **Private Cloud** l involves a server dedicated solely to one organization. Access is restricted and limited, providing proprietary value to the organization.
- **Hybrid Cloud** combines the principles of both public and private clouds, depending on the specific purposes and needs of the organization.
- **Community Cloud** involves shared infrastructure among several communities or organisations. They share resources based on common requirements and goals.
- **Multi-Cloud** consists of multiple public clouds, allowing organisations to leverage the advantages of different cloud services and providers[4].

Cloud service models

Apart from the deployment models, there are three main on-demand access service models of cloud instances as shown on Figure 1:

- **“IaaS**, **or infrastructure as a service**, cloud-hosted physical and virtual servers, storage and networking—the backend IT infrastructure for running applications and workloads in the cloud.
- **PaaS**, or **platform as a service**, a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications.
- **SaaS**, or **software as a service**, ready-to-use, cloud-hosted application software”.

[4] Cloudflare, *„What is the cloud”,* https://www.cloudflare.com/learning/cloud/what-is-the-cloud/, 22 October 2024.

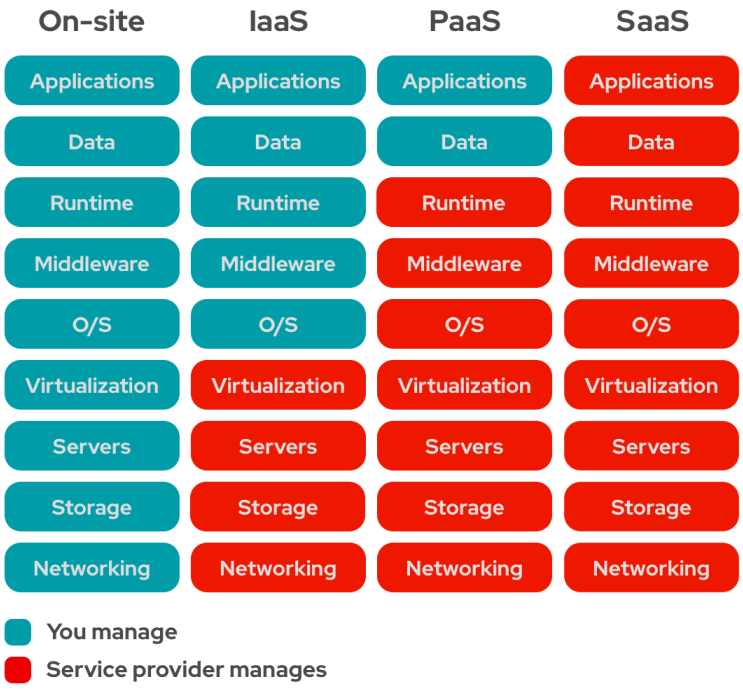

Figure 1: Overview of the cloud solutions models with technical aspect[5].

The main purpose of these models is to **distinguish how much effort the client needs to make to run their infrastructure or manage their data within the cloud**.

> While a typical on-premises (on-site) model requires the company to handle everything on their own—such as building server racks, deploying virtual machines, setting up routers and switches to connect the internal network, providing the correct amount of storage, and installing the necessary software and applications—in the SaaS model, the cloud provider handles the majority of the work for you.

Advantages and Disadvantages of Cloud Environments

As with any type of deployment, cloud environments have both pros and cons that every organization must evaluate.

Advantages of Cloud Environments:

- **Scalability** - cloud environments can be scaled according to the organization's requirements without the need for physical expansion of hardware or other instances within the organization itself.
- **Cost Savings** - when an organization orders a cloud instance, it pays only for the resources consumed, no more and no less.
- **Improved Collaboration** - cloud storage enables almost seamless collaboration across the globe, regardless of where the collaborating members reside, as long as they have an internet connection.

[5] Red Hat, *"IaaS, PaaS, SaaS"*, https://www.redhat.com/rhdc/managed-files/iaas-paas-saas-diagram5.1-1638x1046.png, 15 October 2024.

- **Security** - in certain instances, especially when a company has limited capabilities, it is easier to migrate to the cloud. This shift allows the organization to offload some of the weight and responsibility of cybersecurity to a more mature and capable cloud vendor.
- **Data Loss Prevention** - vendors often offer backup plans and disaster recovery features, which can be easily applied to cloud instances[6].

Disadvantages of cloud environments:

- **Internet Reliant** - if an organization stores its services and resources in the cloud, a loss of internet connection will result in a disruption of access to these services and resources.
- **Limited Control** - using the cloud essentially means renting someone else's hardware or resources to complete the organization's tasks. This means that some of the tasks cannot be performed by the organisation's technicians, but by the cloud vendor.
- **Security Risks** - while relying on the vendor's security principles might be suitable and comfortable for smaller, less mature companies, it may not be the same for larger companies. Shared infrastructure means shared responsibility, an increased attack surface, and other security concerns[7].
- **Privacy Concerns** - while cloud computing offers many benefits, it also raises privacy concerns, especially when sensitive data is stored on infrastructure managed by a third-party provider.

  Cloud providers typically have security protocols in place, such as encryption and access controls, to limit who can access the data. However, users should be aware that in some cases, cloud providers may have the technical ability to access or manage the data they host.
- **Limited Control** - scalability can be both a pro and a con. While the on-demand increase in resources can be beneficial in terms of flexibility and running demanding tasks on the company's cloud, it can be a disadvantage if the same principle is used by a threat actor to scale up their attacks.

Of course, the pros and cons will differ based on the chosen model and vendor. That's why it is crucial to understand the specific needs of the organization.

Main providers

At time of analysis, the top three providers continue to dominate the cloud computing market with a 67% of total market share. The leading cloud providers, ranked from the

[6] Google Cloud, *„Advantages and Disadvantages of Cloud Computing",* https://cloud.google.com/learn/advantages-of-cloud-computing?hl=en, Google, 22 October 2024.
[7] Ibidem.

largest, as Figure 2 shows:

1. Amazon Web Services (AWS)
2. Microsoft Azure
3. Google Cloud Platform (GCP)
4. Alibaba Cloud
5. Oracle Cloud
6. IBM Cloud
7. Tencent Cloud
8. OVHcloud
9. DigitalOcean
10. Linode (Akamai)[8].

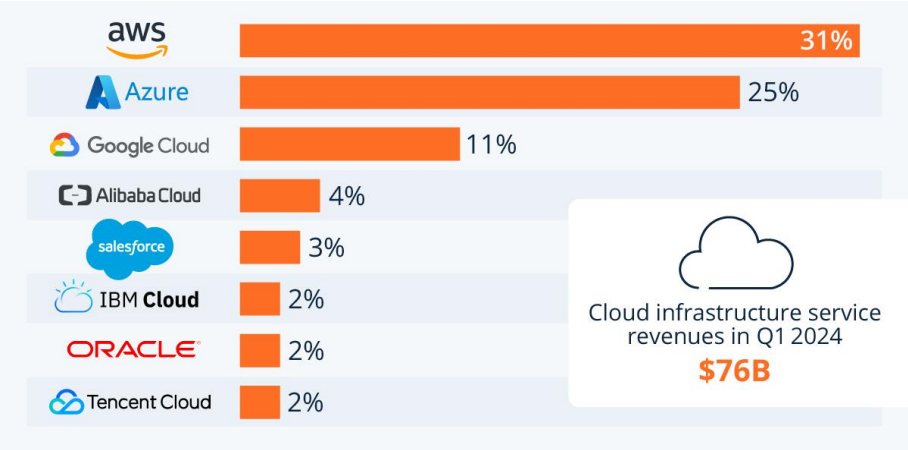

Figure 2: Worldwide market share of leading cloud infrastructure service providers in Q1 2024[9].

Cloud Security - overview

It is certain that **an increasing number of organisations are migrating to the cloud**—a trend that is clearly observable. As they do so, their cloud attack surface expands, leading to a rise in cloud-related incidents, originating from various security issues.

Present state of the cloud – cloud related trends

Following the data on the usage of cloud services in Europe, it is evident that cloud adoption is on the rise, with no signs of slowing down. According to research conducted

[8] M. Zhang, *"Top 10 Cloud Service Providers Globally in 2024"*, https://dgtlinfra.com/top-cloud-service-providers/, Dgtl Infra, 15 October 2024.
[9] F. Richter, *"Amazon Maintains Cloud Lead as Microsoft Edges Closer"*, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/, Statista, 2 May 2024.

by Eurostat, the number of enterprises purchasing cloud services has increased noticeably across most European countries between 2021 and 2023 (Figure 3)[10]. To provide some perspective on the trend and its scale, data from Synergy Research Group in 2022 revealed that the European cloud market has grown more than fivefold since early 2017, reaching EUR 10.4 billion (US$10.9 billion) in the second quarter of 2022[11]. According to a report by Cybersecurity Ventures, the total amount of data stored in the cloud is projected to reach an impressive 100 zettabytes by 2025 (10^{21} bytes), accounting for 50 percent of the world's data[12].

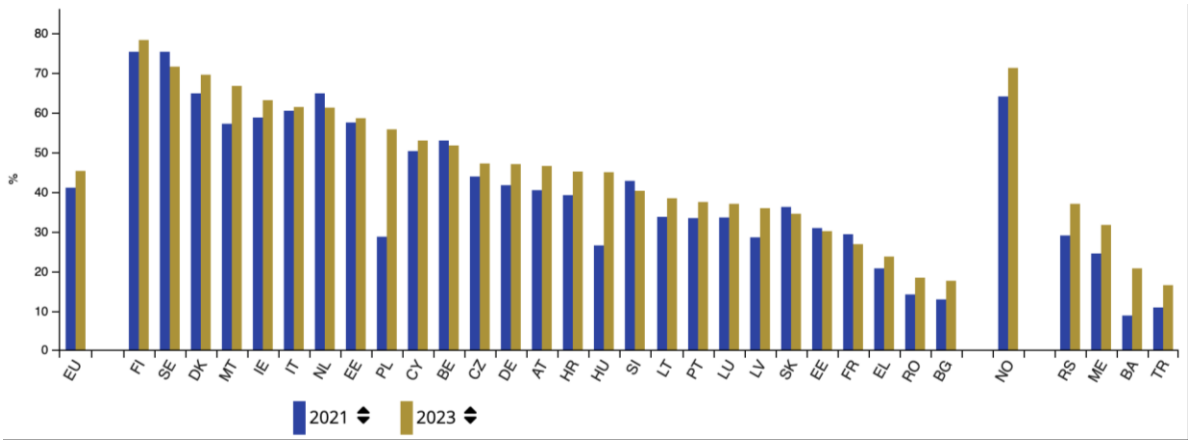

Figure 3: Enterprises buying cloud computing services, EU, 2021 and 2023.

The increasing reliance on cloud solutions has expanded the attack surface, which is often mismanaged, misconfigured, and vulnerable - providing adversaries with more opportunities to exploit these weaknesses.

As for the sector's usage of cloud storage, these are as follows (Figure 4)[13]:

- BFSI (banking, financial services, and insurance)
- IT and telecommunication
- Government and public sector
- Manufacturing
- Healthcare and life science

[10] Eurostat, *"Cloud computing - statistics on the use by enterprises"*, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises&oldid=632772, December 2023.
[11] Synergy Research Group, *„European Cloud Providers Continue to Grow but Still Lose Market Share",* https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share, 27 November 2022.
[12] S. Morgan, *"The World Will Store 200 Zettabytes Of Data By 2025",* https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/, 1 February 2024.
[13] Acumen Research and Consulting, *"Cloud Storage Market Size - Global Industry, Share, Analysis, Trends and Forecast 2022 – 2030"*, https://www.acumenresearchandconsulting.com/cloud-storage-market, February 2023.

- Retail and consumer goods
- Media and entertainment

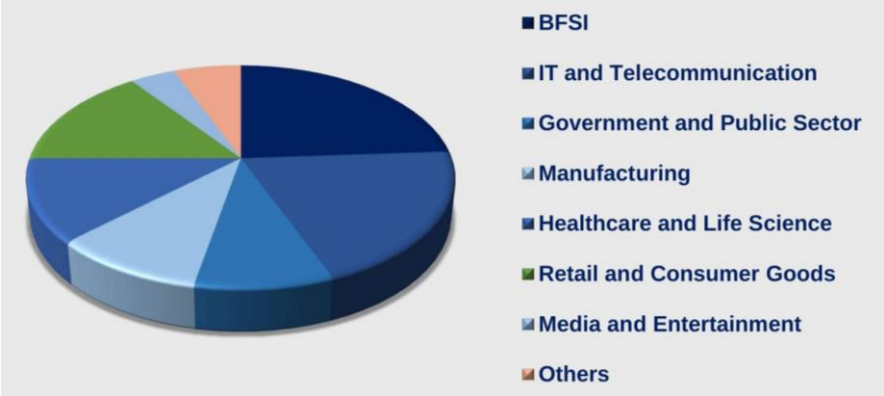

Figure 4: Global cloud storage market by industry 2021 (% share).

operators of essential services (OES), such as banking are utilizing cloud environments to this extent, with plans to extend it even further in the future.

According to the Trend Micro 2024 Midyear Cybersecurity Threat Report, *"high-risk cloud applications dominated the list of risk events in the first half of the year"* (Figure 5). The incidents involving these risky applications numbered in the hundreds of millions, surpassing all other indicators[14].

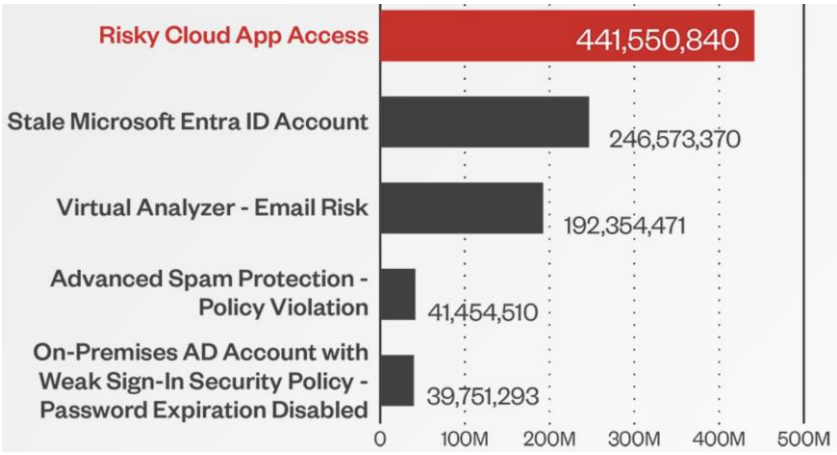

Figure 5: Top 5 risk events during the first half of 2024.

High-risk applications are those that pose potential threats to an organization due to potential vulnerabilities, exposure to threats, the critical nature of the data they handle,

[14] Trend Micro, *„Pushing The Outer Limits Trend Micro 2024 Midyear Cybersecurity Threat Report"*, https://www.trendmicro.com/vinfo/be/security/research-and-analysis/threat-reports/roundup/pushing-the-outer-limits-trend-micro-2024-midyear-cybersecurity-threat-report, 15 August 2024.

their malicious nature, or their potential for compromising the organization[15].

According to Gartner, cloud computing will transition from being a technological disruptor to an essential element for sustaining business competitiveness by 2028[16].

As the cloud computing networks grows, so does the attack surface – and the threat actors are fully aware of it. The 2024 yearly report of CrowdStrike revealed a **110% increase in cloud-conscious cases, where threat actors exploit cloud features, from 2022 to 2023**[17].

It also highlighted:

- the widespread use of "interactive intrusion" techniques, where adversaries actively execute actions on a host.
- the difference between normal behaviour and attacks, which is increasingly challenging[18]. As for the numbers:
    - the 75% increase in cloud environment intrusions from 2022 to 2023.
    - the focus on eCrime, as 84% of adversary-attributed cloud-conscious intrusions were focused on eCrime.

The increase in cloud exploitations is driven by several factors inherent to the cloud's nature. One of them is **the pressure to innovate rapidly which often prioritizes new features over security patches. This results in "rogue" and shadow cloud environments outside the security team's control.** Developers can quickly experiment and push projects to production, leading to more vulnerabilities and misconfigurations[19].

Misconfiguration – the leading issue

When managing security, the top priority should be identifying the attack vector, which, according to CrowdStrike, is often misconfiguration. **Cloud misconfigurations are the leading risk factor, necessitating better collaboration between DevOps and security teams**. According to the Zscaler's report, nearly all organizations, 98.6%, have cloud environment misconfigurations that pose significant risks to their data and infrastructure[20].

---

[15] Examples of the high-risk apps are as follows: anonymizers (Tor, Hide.me), torrents (uTorrent, BitTorrent), remote access apps (TeamViewer, RealVNC).
Allot, *„Threat Bulletin – High Risk Apps",* https://www.allot.com/resources/Threat_Bulletin_High-risk-Apps.pdf, May 2019.
[16] Gartner, *"Gartner Says Cloud Will Become a Business Necessity by 2028"*, https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028, 29 November 2023.
[17] CrowdStrike, *"Insider's Playbook: Defending Against Cloud Threats",* https://www.crowdstrike.com/resources/white-papers/insiders-playbook-defending-against-cloud-threats/, 28 August 2024, p. 4.
[18] Ibidem.
[19] Ibidem, p. 5.
[20] D. Desai, D. Parekh, E. Laufer, *"2022 Cloud (In)Security Report",* https://www.zscaler.com/blogs/security-research/2022-cloud-security-report, Zscaler, 15 February 2023.

These misconfigurations result from incorrect or missing security settings, exposing systems to risk. Detection and resolution are challenging due to cloud complexity and the need for teams to align on priorities.

Examples of misconfigurations are as follows:

- Access management rules: overly permissive role policies; guest users in Azure AD.
- Serverless: hosting a website that has vulnerabilities; HTTP not triggered towards HTTPS.
- Networking: enabled IP forwarding; public IP on virtual machine.
- Virtual environment: no limits on OnDemand vCPU Instances; custom ports enabled.
- Databases: publicly accessible database; data at rest encryption disabled[21].

Other primary attack vectors and techniques, in order of frequency, include:

- **Unsecured APIs** - APIs that lack proper security measures can be exploited by attackers to gain unauthorized access to systems and data.
- **Weak Authentication and Access Controls** - inadequate authentication mechanisms and lax access controls can allow unauthorized users to infiltrate systems.
- **Vulnerabilities in Shared Resources** - laws in shared resources, such as libraries and services, can be leveraged by attackers to compromise systems[22].
- **Social Engineering and Credential Stuffing** - attackers use social engineering tactics and credential stuffing to deceive users and gain access to systems by exploiting weak or reused passwords.
- **SQL Injection and Cross-Site Scripting (XSS)** - these common web application vulnerabilities allow attackers to execute malicious code and access sensitive data by injecting harmful scripts[23].

[21] A. Chaudhary, *„Managing Cloud Misconfigurations Risks",* https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks, Cloud Security Alliance, 14 August 2023.
[22] Between June 2022 and June 2023, the IBM X-Force team identified 632 new cloud-related common vulnerabilities and exposures (CVEs), representing a 194% increase compared to the previous year. G. Smith, *"75+ Surprising Cloud Security Statistics You Should Know in 2024",* https://www.stationx.net/cloud-security-statistics/, StationX, 10 April 2024.
[23] SentinelOne, *„Cloud Security Attacks: Types & Best Practices",* https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-attacks/, 30 September 2024.

There is a specialized MITRE ATT&CK Matrix dedicated to cloud solutions, which covers all techniques abused by attackers to breach the cloud and spans the entire kill chain[24]. It can be found in Appendix B - Cloud Matrix – MITRE ATT&CK[25].

A robust cloud security solution should offer real-time visibility, continuous protection, and threat detection across all stages of development and operations. According to the CrowdStrike[26], organization willing to secure its cloud assets, should work on:

- **Real-Time Visibility** - continuous, real-time visibility across cloud components, such as infrastructure, identities, and workloads, is essential for detecting and mitigating threats in dynamic environments.
- **Risk Prioritization** - a system that correlates threat intelligence with business impact and data sensitivity helps prioritize alerts, ensuring critical risks are addressed first.
- **Runtime Protection** - implementing runtime security measures allows for real-time threat blocking in production, enhancing response times and reducing manual effort.
- **Cloud Detection and Response** – a cloud-native security provider ensures 24/7 monitoring, threat detection, and rapid threat neutralization, improving overall security management.
- **Centralized Processes** - unifying security, DevOps, and engineering workflows with live threat intelligence helps prioritize security actions and reduces the likelihood of breaches.

Favourite targets in the cloud – SMEs

Small and Medium-sized Enterprises (SMEs) are the most vulnerable and likely to be attacked[27]. Several factors contribute to this:

- **Cloud migration challenges** - as more enterprises migrate to the cloud, the process often results in unattended and unsecured resources, increasing the risk of attacks.
- **Lack of dedicated cybersecurity teams** - SMEs frequently lack dedicated cybersecurity teams, leading to insufficient audits, security implementations, and reviews, including basic measures like Multi-Factor Authentication (MFA).
- **Reliance on third-party dependencies** - SMEs often depend on third-party

[24] Lockheed Martin, *„The Cyber Kill Chain”,* https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, 24 October 2024.
[25] MITRE ATT&CK, *„Cloud Matrix”*, https://attack.mitre.org/matrices/enterprise/cloud/#, 24 October 2024.
[26] CrowdStrike, *“Insider's Playbook: Defending Against Cloud Threats”*…, p. 7-8.
[27] K. Harpsoe, *“Why SMEs are now a prime target for ransomware”*, https://www.smeweb.com/why-smes-are-now-a-prime-target-for-ransomware/, SME Web, 7 October 2024.

services, such as cloud providers. When these third parties are compromised, SMEs are also at risk[28].

For instance, the breach of Microsoft's Azure by the Storm-0558 group highlighted how a single vulnerability in a cloud provider can expose thousands of customers' sensitive data[29].

Responsibility for the security in the cloud

When we speak about security in the cloud, there is an aspect that is not necessarily addressed to its full extent, which is the responsibility of the cloud solution.

Essentially, **we have three main models of cloud solutions, which are also the responsibility models themselves** (IaaS, PaaS, SaaS). Naturally, SaaS will require the least amount of management and responsibility from the consumer, in contrast to IaaS. As you choose a model, you will have to share some responsibility with the vendor (Figure 6). This creates the **issue of shared responsibility between the cloud service provider and the customer**.

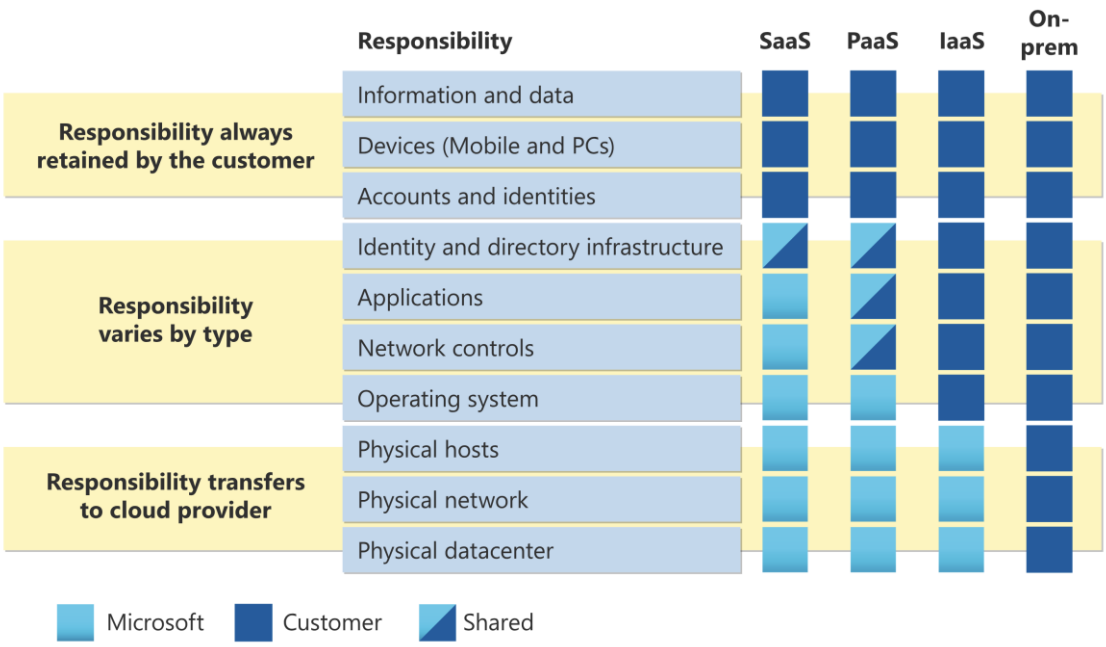

Figure 6: Overview of the cloud solutions models with responsibility[30].

[28] Tenable, *"6 Cloud Security Tips For 3rd-Party Risk"*, https://www.tenable.com/blog/6-cloud-security-tips-for-3rd-party-risk, 16 November 2022.
[29] Microsoft Threat Intelligence, „*Analysis of Storm-0558 techniques for unauthorized email access*", https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/, Microsoft, 14 July 2023.
[30] Microsoft, *"Shared responsibility in the cloud"*, https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility, 29 September 2024.

No matter which model is chosen by the customer, he will always retain the following responsibilities:

- **Data** refers to any pieces of information that are collected, stored, and processed by computer systems. This can include text, numbers, images, videos, and any other type of information that can be digitally stored and manipulated.
- **Endpoints** are devices that are connected to a network and communicate back and forth with the network. These can include computers, smartphones, tablets, servers, and IoT devices.
- **An account** in the context of computing and cybersecurity typically refers to a user's profile or credentials that allow them to access a system, application, or service.
- **Access Management** is the process of controlling who has access to various resources within an organization.

This is largely consistent among the majority of cloud vendors. Depending on the model chosen by the customer, the amount of liability for the contract sides will differ. This also requires varying levels of engagement, effort, and resources from both sides. **In this dual model of shared responsibility, people sometimes find it confusing what actually belongs to their duties**. *"According to the Palo Alto Networks: "73% of organisations struggle to understand the shared responsibility of cloud security, which ultimately leads to blind spots"*[31]. Even when the customer chooses SaaS, it still requires a solid amount of effort to implement security measures.

To tackle the challenge of the shared responsibility model, organisations should follow these best practices:

1. **Ensure that they understand the service level agreement (SLA)**, which clearly defines the responsibilities of both the provider and the customer.
2. **Utilize cloud security and visibility tools** - modern tools with robust capabilities can evaluate the security posture of cloud resources and identify unattended or unmanaged sections[32].
3. **Focus on securing the data** – data is the most important and fragile part of any organization and should be handled with caution and best practices, such as encryption of data in transit and at rest and enforcing strong encryption protocols.

[31] Palo Alto Networks, *"Cloud Security Is a Shared Responsibility"*, https://www.paloaltonetworks.com/cyberpedia/cloud-security-is-a-shared-responsibility, 17 October 2024.
[32] Zscaler, *"What Is a Shared Responsibility Model?",* https://www.zscaler.com/br/resources/security-terms-glossary/what-is-shared-responsibility-model, 15 October 2024.

4. **Implement identity and access management (IAM)** – Access control is a crucial part of cyber defence, involving the management of user roles, account permissions, and identity verification[33].

While cloud service providers (CSPs) usually take care of the infrastructure security, customers are responsible for securing their own applications and data. This can be tough for customers who might not have the right expertise or resources. According to a report published by Tenable, **the vast majority of cloud solution's customers have suffered from cloud breaches**. *"Some 95% of cloud security professionals reported cloud-related breaches, with 92% reporting that their sensitive data was exposed and 58% of those acknowledging that the sensitive data exposure caused harm"*[34].

Security measures for cloud environments

5 essential steps to secure the cloud

To establish a secure cloud environment and achieve a higher level of protection, organizations should first follow these five essential steps to ensure the minimum requirements are met:

1. **Identify your assets** - this fundamental step involves recognizing all assets within your possession, including hardware, software, and the boundaries of your environment.
    - Identifying these assets is crucial because you cannot protect what you cannot see, such as shadow IT[35]. Properly evaluating the extent of your cloud assets is key to a robust security strategy.
2. **Choose and design architecture** - every environment requires a well-defined hierarchy, model, and approach. Without a structured architecture, the environment becomes unmanaged, disorganized, and difficult to control.
    - Establishing a proper management model is crucial, as it is impossible to manage something chaotic that is spread across numerous endpoints or instances.
3. **Automation** - implementing automation is one of the best strategies for managing understaffed organisations or those burdened with repetitive tasks. If a process can be automated without compromising its integrity, it should be.

[33] A. Sheps, *„Cloud Shared Responsibility Model: Examples & Best Practices"*, https://www.aquasec.com/cloud-native-academy/cspm/shared-responsibility-model/, Aquasec, 13 July 2023.
[34] Tenable, *"2024 Cloud Security Outlook Navigating Barriers and Setting Priorities"*, https://static.tenable.com/marketing/research-reports/ResearchReport-2024_Cloud_Security_Outlook.pdf, 2024, p. 4.
[35] Cisco, *"What is Shadow IT"*, https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html, 23 October 2024.
"Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization."

Automation can help establish standardized baselines or settings across the entire environment.

- **Infrastructure as Code (IaC)**: IaC involves managing and provisioning infrastructure through code rather than manual processes. It is an efficient way to automate environments, including cloud environments. Automation through IaC ensures consistency and speed in deploying and managing infrastructure[36].

4. **Assessment** - once the organization has a clear understanding of its assets and established architecture, the next step is to assess the security posture.
    - Utilize fully or semi-automated tools to evaluate the organization's security posture, identify deviations from security baselines, misconfigurations, and unattended assets.
5. **Detection** - after setting up the cloud environment, it is essential to detect any new threats. This includes conducting vulnerability analyses after patches and performing security checks following the offboarding of employees.

In addition to the outlined steps, each organization should stay informed about the current threat landscape in cloud security.

This can be achieved by addressing questions such as[37]:

- What are the most exploited vulnerabilities in the cloud currently?
- Which adversaries are targeting cloud environments?
- What tools are these adversaries leveraging?

Guides, benchmarks, security baselines

To effectively secure cloud environments, there are various security controls and best practices available, often provided through guidance and recommendations from different sources. These security controls can be grouped into several categories:

- **Security Baselines** - these are the minimum-security standards that should be met to protect cloud environments. For instance:
    - CIS Controls v8[38]
    - Cloud Controls Matrix (CCM)[39].

- **Benchmarks** - these are standardized configurations and best practices aimed at securing specific technologies and platforms. For instance:

[36] Red Hat, *„What is Infrastructure as Code (IaC)?”*, https://www.redhat.com/en/topics/automation/what-is-infrastructure-as-code-iac, 23 October 2024.
[37] By answering these questions, organisations can adjust their security measures to align with current cloud trends and avoid potential breaches.
[38] Center for Internet Security, *“CIS Controls v8 Cloud Companion Guide”,* https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide, 15 October 2024.
[39] Cloud Security Alliance, *“Cloud Controls Matrix (CCM)”,* https://cloudsecurityalliance.org/research/cloud-controls-matrix, 15 October 2024.

- SAP Standard Application Benchmarks[40]
- Cloud Computing Security Requirements Guide (CC SRG)[41]
- Microsoft cloud security benchmark[42].

- **Frameworks** - these are comprehensive security models and methodologies that provide a structured approach to managing and securing cloud environments. For instance:
  - NIST Cybersecurity Framework (CSF 2.0): A set of guidelines and best practices to help organisations manage and reduce cybersecurity risks[43]
  - Centre for Cybersecurity Belgium's CyberFundamentals Framework[44]
  - ISO/IEC 27001: An international standard for managing information security[45].

- **Guidelines** - these are recommendations and best practices published by various entities, including vendors, government bodies, and security communities, to ensure compliance and enhance security.

- **Other Controls** - these might include industry-specific standards, audit requirements, or custom configurations designed to meet the unique needs of an organization[46].
  - FS-ISAC Principles for Financial Institutions' Security and Resilience in Cloud Service Environments[47].

Depending on the source of the guidance, the controls can vary in specificity. They may range from a high-level overview and general principles to highly detailed security measures targeting specific areas, such as endpoint device protection.

These security controls are **provided by various sources**, each providing a unique but complementary perspective:

---

[40] Standard Application Benchmark, *"SAP Standard Application Benchmarks"*, https://www.sap.com/about/benchmark/appbm/cloud.html, 15 October 2024.
[41] DoD Cyber Exchange Public, *"DoD Cloud Computing Security"*, https://public.cyber.mil/dccs/, 15 October 2024.
[42] Microsoft, *"Microsoft cloud security benchmark documentation",* https://learn.microsoft.com/en-us/security/benchmark/azure/, Microsoft Learn, 1 November 2024.
[43] National Institute of Standards and Technology, *"The NIST Cybersecurity Framework (CSF) 2.0",* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, 26 February 2024.
[44] Safeonweb, *"CyberFundamentals Framework"*, https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework, 17 October 2024.
[45] ISO, *"ISO/IEC 27001:2022",* https://www.iso.org/standard/27001, October 2022.
[46] The provided list of security controls is not exhaustive.
[47] FS-ISAC, *"FS-ISAC Principles for Financial Institutions' Security and Resilience in Cloud Service Environments"*, https://www.fsisac.com/hubfs/Knowledge/Cloud/PrinciplesForFinancialInstitutionsSecurityAndResilienceInCloudServiceEnvironments.pdf?hsLang=en, July 2024.

- **Vendor Guidance** - recommendations provided by cloud service providers like AWS, Google Cloud, and Microsoft Azure on how to best secure their platforms.
- **Government Guidance** - security frameworks and standards set by governmental agencies such as the National Institute of Standards and Technology (NIST) or the European Union Agency for Cybersecurity (ENISA).
- **Community Guidance** - best practices and frameworks developed by industry groups, cybersecurity organisations, or open-source communities, such as the Center for Internet Security (CIS) or the Cloud Security Alliance.

Multi-factor authentication (MFA) is very likely the most important security measure that should be enabled at all times and at every level of access to resources. This measure can significantly decrease the possibility of a security breach. According to a study conducted by Google on consumer accounts, challenges and MFA prevented 100% of automated attacks, 96% of bulk phishing attacks, and 76% of targeted attacks[48]. **MFA is of utmost importance for internet-facing systems, such as remote access, which is how organisations typically access their cloud resources**. These notable numbers underscore the importance and necessity of having MFA in place.

By using a combination of these controls and guidelines, organisations can more effectively secure their cloud environments, ensuring they meet industry standards and protect against evolving threats.

> Regular security controls used in traditional enterprise environments are often suitable for cloud environments in most cases. Therefore, when selecting appropriate security controls, one does not necessarily need to focus exclusively on cloud-specific controls, as many general security principles and practices still apply effectively in the cloud.

To sum up, the resources required to establish a secure posture for an organization in the cloud are **virtually unlimited and the only limiting factor is human capacity**.

Security by Default as a strategy to mitigate a cloud threats

It's fundamentally better to prevent problems before they occur. This is where the concept of **security by default** becomes crucial. To illustrate this concept, consider the opposite scenario: the use of default generic or simple passwords in IoT devices. IoT devices are among the most vulnerable types of technology, primarily due to the

[48] P. Doerfler, M. Marincenko, J. Ranieri, Y. Jiang, A. Moscicki, D. McCoy, K. Thomas, *"Evaluating Login Challenges as a Defense Against Account Takeover"*, https://storage.googleapis.com/gweb-research2023-media/pubtools/5021.pdf, New York University, Google.

widespread use of default passwords[49].

Example 1

Imagine if manufacturers programmed IoT devices with algorithms that generated unique passwords instead of relying on default ones. These passwords wouldn't need to be overly long or complex—just unique, consisting of 12 to 14 characters. If this approach had been implemented, we wouldn't have thousands of vulnerable IoT cameras exposed on platforms like Shodan[50], easily accessible to attackers through simple dictionary or brute-force attacks based on default passwords.

Implementing security by default could have significantly reduced these vulnerabilities and enhanced overall device security.

Example 2

Another example can be found in the security of Windows 10 and 11 devices, which are not inherently secure by default. Regular users can access PowerShell, and while the User Account Control (UAC)[51] prompts for confirmation, it does not require a password, allowing potentially malicious scripts to run without sufficient barriers.

Additionally, the command line is accessible with unlimited usage, and tools like BitsAdmin within PowerShell can be exploited to download payloads using simple one-liners.

Imagine a threat actor using a BadUSB[52] device to compromise a system. Once connected, the BadUSB could open a PowerShell window and create a new registry key for persistence while disabling the firewall. However, if the PowerShell command required elevated privileges that triggered a UAC prompt with a password requirement, the attack could be thwarted at that critical step.

By implementing stronger security measures, such as requiring a password for UAC prompts, the entire attack chain could be disrupted, significantly enhancing overall system security.

Example of solution

The "Secure by Default" Cluster VPC Networking in IBM Cloud Kubernetes Service is an example of a security-by-default approach, where security configurations are automatically implemented to ensure a safe environment without requiring manual

[49] TrendMicro, *"Smart Yet Flawed: IoT Device Vulnerabilities Explained"*, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained, 28 May 2020.
[50] Shodan, https://www.shodan.io/, 15 October 2024.
[51] Microsoft Learn, *"User Account Control Overview"*, https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/, Microsoft, 26 March 2024.
[52] A BadUSB attack occurs when the firmware of a USB device is reprogrammed by a hacker. Once this is done, the USB device can impersonate other device types, such as a keyboard. This impersonation can lead to the execution of arbitrary commands when the USB is plugged into a computer.
L. Ballejos, *"What Is BadUSB? Definition and How to Prevent It",* https://www.ninjaone.com/it-hub/endpoint-security/what-is-badusb/, Ninja One, 2 February 2024.

setup by users (Figure 7)[53].

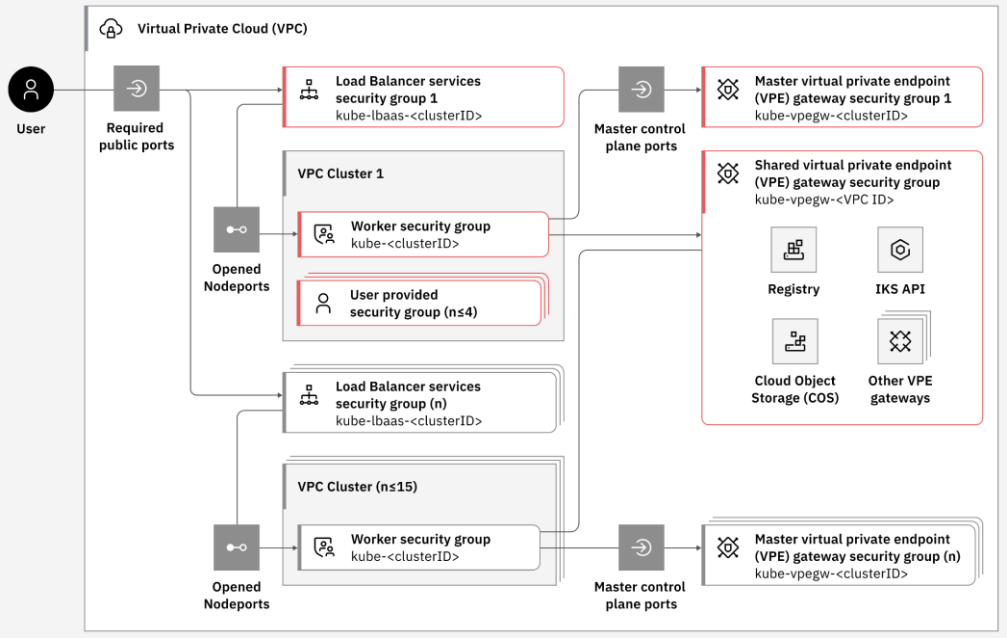

Figure 7: Overview of the VPC security groups applied to the VPC and clusters.

It achieves the principle for instance by:

- **Automatic Configuration of Security Groups and Rules** - when a new Virtual Private Cloud (VPC) cluster is created, the system automatically provisions security groups and their associated rules, restricting access only to essential traffic required for the cluster to function.
- **Isolation of Resources** - each cluster is provided with its own dedicated security groups, ensuring that workloads and traffic between different clusters are isolated by default[54].

Security by Design as a strategy to mitigate cloud threats

Configuration is one way to address security issues, but there's a stronger approach. Instead of relying on configuring an out-of-the-box solution with a pre-set security baseline, what if the manufacturer designed the product with robust security principles **built into the code itself**? This is known as **Security by Design**.

[53] Cloud IBM, *"Understanding Secure by Default Cluster VPC Networking"*, https://cloud.ibm.com/docs/containers?topic=containers-vpc-security-group-reference, IBM Cloud Docs, 14 October 2024.

[54] Similar to IBM's solution, **Google Cloud** implements Security by Default by automatically applying secure predefined security policies when a new customer or organization resource is created. This ensures that new organisations start with a secure posture without the need for manual configuration by users.
Google Cloud, *"Managing secure-by-default organization resources"*, https://cloud.google.com/resource-manager/docs/secure-by-default-organizationsorganisations, 15 October 2024.

Security by Design can be achieved in various ways, such as **adopting secure coding practices**:

- **Avoid Hard-Coding Secrets**: Do not store sensitive data like API keys or passwords directly in code. Instead, use secure vaults or environment variables.
- **Input Validation**: Always validate and sanitize inputs to prevent injection attacks, such as SQL injection and cross-site scripting (XSS).
- **Use Strong Cryptography**: Implement encryption and hashing algorithms (e.g., AES, RSA, SHA-256) for data at rest and in transit.

Another important consideration is to **avoid reusing outdated code**, or at the very least, ensure its security by thoroughly checking it against modern secure coding practices. It is well known that new products are often released containing vulnerabilities inherited from older ones[55] [56].

A prime example of this can be seen in the research published on Cisco's Talos Vulnerability Spotlight site, where **vulnerabilities from earlier software were discovered in supposedly new products**.

The researcher of Cisco Talos found an issue in a wireless router where the unescape function, used to decode URL-encoded characters (like %20 for spaces), didn't perform proper size checks. The vulnerable code originated from **Broadcom**, a major hardware manufacturer. It was likely distributed as part of a **reference implementation -** a sample code package provided by Broadcom to help developers use their products, including HTTP server functionality.

The researcher identified several specific products affected by this vulnerability, each exposing users to potential attacks: CVE-2022-28664[57], CVE-2022-27631[58], CVE-2022-26376[59], CVE-2022-28711[60].

Identifying the vulnerable code, revealed multiple vulnerabilities across completely different hardware sharing the same dependency[61].

[55] L. Constantin, *"Why code reuse is still a security nightmare"*, https://www.csoonline.com/article/571073/why-code-reuse-is-still-a-security-nightmare.html, CSO, 26 July 2021.
[56] ByteHyde, *"What Are Code Vulnerabilities?"*, https://dev.to/bytehide/what-are-code-vulnerabilities-3lgj, Dev.to, 31 July 2024.
[57] Affects FreshTomato firmware (used in routers), which was fixed in version 2022.1. This allows an attacker to exploit memory corruption by sending a specially crafted HTTP request.
[58] Affects DD-WRT firmware (used in embedded systems and routers) from version 32270 to 48599.
[59] Affects Asuswrt and Asuswrt-Merlin (an open-source alternative). The issue arises in the HTTP server functionality of the firmware, again leading to memory corruption.
[60] Affects ArduPilot APWeb (an open-source software for autonomous vehicles like drones), in which the vulnerability exists in the web interface, allowing for potential remote memory corruption.
[61] Ibidem.

Both **Security by Design** and **Security by Default** share a common goal: **the manufacturer should provide a secure product to the consumer from the start**. This ensures security as a core feature, rather than leaving it as the consumer's responsibility—especially when they may have little to no technical knowledge. It's about shifting the responsibility to the vendor, ensuring security is a standard, not an afterthought.

Opt-out as a measure to secure the cloud

Another good approach, particularly in terms of security by default, would be establishing the approach of opt-out by default. Opt-out means users are automatically included in a program or service unless they explicitly choose not to participate. In this case, organisations may collect data or implement security measures by default.

> This could lead to privacy concerns if users are not fully aware of what data is being collected or how it is being used. However, if data is used solely for security measures and does not violate users' privacy, it could bring significant improvements in the general security of end devices[62].

For instance, SELinux in Linux systems is a very extensive security baseline. If it were enabled by default on all new Linux systems of some distributions, it would significantly increase security. At the same time, SELinux can be disabled using a simple command and the necessary permissions[63].

The proposed process of establishing a security might be as follows:

1. Automate baseline security with default settings that incur minimal or no additional cost.
2. Establish secure baselines through a guided workflow where automatic implementation is not feasible.
3. Provide clear communication about opt-in services, such as logging and secure backups, with transparent explanations of their benefits[64].

[62] F. Dezeure, L. Moerel, G. Webster, *"Improving the World's Cyber Resilience, at Scale. Implementing Baseline Security by Default"*, SSRN, 16 February 2024, p. 1-6.
[63] Red Hat Documentation, *"Chapter 2. Changing SELinux states and modes",* https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/using_selinux/changing-selinux-states-and-modes_using-selinux#changing-selinux-states-and-modes_using-selinux, 15 October 2024.
[64] F. Dezeure, L. Moerel, G. Webster, *"Improving the World's Cyber Resilience, at Scale. Implementing Baseline Security by Default"…,* p. 6.

Automated security solutions for cloud

Figure 8: Factors that reduced the average breach cost.

Cloud environments can be complex and difficult to fully understand in terms of topology and management. However, there are several fully automated or semi-automated solutions available to manage and secure cloud environments at scale — an essential capability for rapidly growing organisations that rely on the cloud. Research has shown that employing automation and automated security measures in organizations positively impacts the potential costs of an average breach (Figure 8). These measures include the Cloud Workload Protection Platform, Cloud Security Posture Management, and Cloud Access Security Broker, which are further explained in Appendix D.

All the mentioned solutions in the Appendix D are integral components of a **DevSecOps** approach, which is considered one of the most effective security strategies for cloud environments[65]. **In DevSecOps, security is a fundamental part of the DevOps process, embedded deeply into the structure and present at every stage**. This approach ensures that security is a shared responsibility throughout the entire development, deployment, and operations lifecycle. Key elements of DevSecOps include automation, continuous monitoring, security testing, incident response, policy as code, and collaboration.

By adopting a DevSecOps approach, organisations can enhance their security posture, reduce risks, and ensure faster and more secure delivery of applications.

Threat landscape

Attacks targeting cloud environments are not fundamentally different from those

[65] IBM, *"Cost of a Data Breach Report 2024"*, https://www.ibm.com/downloads/cas/1KZ3XE9D, s. 23.

targeting on-premises systems. Based on data from SentinelOne[66], the most common security breaches in cloud environments are caused by phishing attacks[67]. According to other data from Statista (Figure 9), the most frequently occurring security incidents in the cloud worldwide in 2024 are phishing (73%), user account compromise (38%), and ransomware or malware attacks (31%)[68].

Phishing is a form of social engineering attack aimed at manipulating victims into performing actions desired by the attacker, such as clicking on a malicious link, downloading a harmful attachment, or divulging account credentials.

Ransomware is a type of cyberattack where data on an infected machine is encrypted, with the attacker demanding a ransom payment or coercing the victim into taking a specific action to regain access.

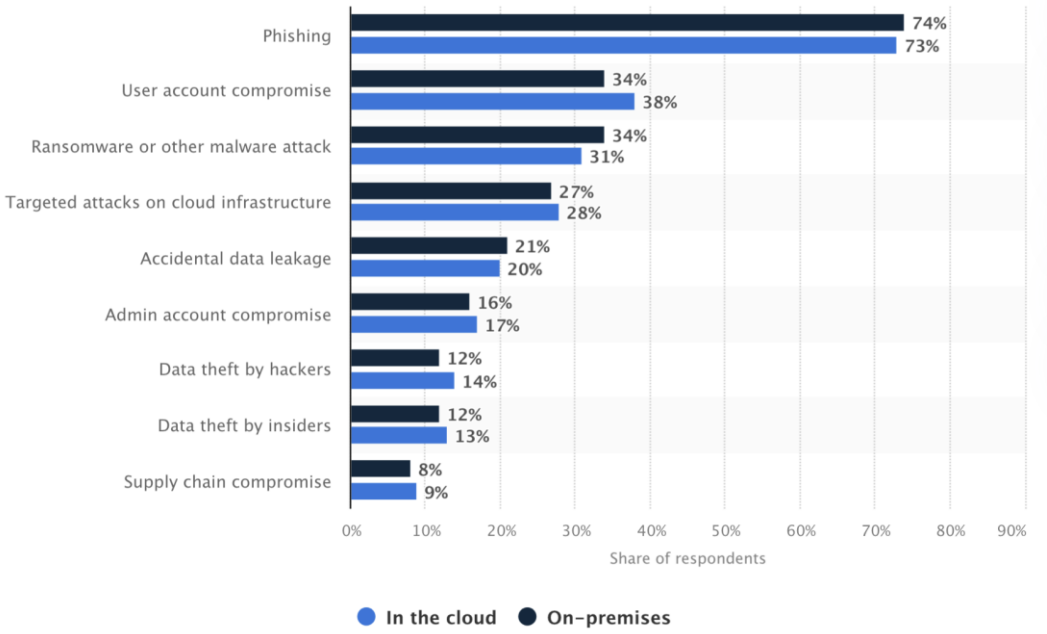

Figure 9: Most common security incidents in the cloud and on-premises worldwide in 2024.

The conclusion is straightforward: **just as with on-premises devices, the human factor (phishing attacks) is the most prevalent cause of breaches in the cloud.**

Regarding the rest of the data, security attacks on-premises and in the cloud are quite similar, with one notable difference: cloud users seem to experience more issues with account compromises.

What is surprising is the amount of accidental data leakage, which is approximately 20% of all security breaches, from cloud environments. The biggest issue with cloud

[66] SentinelOne, *„Top 10 Cloud Security Breaches in 2024”*, https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-breaches/, 31 July 2024.
[67] G. Smith, *“75+ Surprising Cloud Security Statistics You Should Know in 2024”…, Ibidem.*
[68] A. Borgeaud, *„Most common security incidents in the cloud and on-premises worldwide in 2024”*, https://www.statista.com/statistics/1320178/common-cloud-security-attacks-worldwide/, Statista, 8 October 2024.

services is misconfiguration, and this only highlights the importance of addressing this problem. **Data leakage not only leads to financial loss but also results in reputational damage and potential legal repercussions**[69].

Cryptojacking

There is a visible trend in the increase of attacks called cryptojacking. Cryptojacking is the unauthorized use of a victim's computing resources to mine cryptocurrencies. According to several intelligence sources:

- *"Cisco Talos reported a 127% rise in cryptojacking detections in the first half of 2023.*
- *Check Point Research highlighted that cryptojacking accounted for 41% of all cyberattacks in Q3 2023.*
- *Sophos observed a resurgence in cryptojacking campaigns targeting vulnerable cloud infrastructures throughout 2023"*[70].

Why is it particularly interesting in terms of cloud environments? There are several significant reasons why **cryptojacking is one of the most favoured types of attacks against cloud environments**:

- **Scalable computing power** - cloud environments offer vast and scalable computing resources, making them ideal targets for cryptojacking. Attackers can harness this power to mine cryptocurrencies efficiently.
- **Pay-per-use model (costs paid by victims)** - in cloud services, users pay for the resources they use. When attackers hijack these resources for cryptojacking, the costs are borne by the victims, not the attackers, making it a cost-effective strategy for them[71].
- **Weak security configuration** - many cloud environments suffer from weak or misconfigured security settings. These vulnerabilities make it easier for attackers to infiltrate and exploit these systems for cryptojacking.
- **Constant availability** - cloud services are designed to be constantly available, ensuring that the hijacked resources can be used for mining cryptocurrencies around the clock without interruption.

---

[69] Breachsense, *„Data Breaches Cause Loss of Customer Trust",* https://www.breachsense.com/blog/data-breach-trust/, 17 April 2024.,
[70] Cyber Strategy Institute, *„The Rise of Cryptojacking Threat in 2023 by 650%"*, https://cyberstrategy1.medium.com/the-rise-of-cryptojacking-threat-in-2023-by-650-547ef4e29ad3, Medium, 17 July 2024.
[71] R. Sujatha, *„What is pay-as-you-go Cloud Computing (PAYG)?"*, https://www.digitalocean.com/resources/articles/pay-as-you-go-cloud-computing, DigitalOcean, 18 October 2024.

- **Large attack surface** - the extensive, interconnected nature of cloud environments creates a large attack surface, offering numerous entry points for attackers to exploit.
    - This interconnectivity can also impact reliability, as disruptions in one part of the cloud environment may cascade to others, similar to interconnected vessels where a disturbance in one affects the rest.
- **Elastic nature of cloud resources** - cloud resources can be easily scaled up or down based on demand. Attackers can take advantage of this elasticity to maximize their mining efforts without drawing immediate attention[72].

As for the general nature of attacks, cloud environments will also be attractive for attacks like DDoS, which are heavily reliant on resources, as well as cryptojacking. It is not surprising that threat actors adapt their techniques to fit these means. Once an attacker is in the cloud environment and has the ability to deploy additional instances at the cost of the victim, they can scale the attack and launch much bigger attacks than with the base amount of resources of initially compromised devices[73]. Thus, **launching attacks from within the cloud will become more prevalent in the coming years.**

Big Game hunting

Many adversaries shifted to a different approach called big game hunting (BGH). **Big game hunting** refers to a type of cyberattack, often involving ransomware, aimed at large, high value organisations or prominent individuals. Attackers select victims based on their capacity and willingness to pay a ransom, either to restore operations or prevent reputational damage. Common targets include:

- Major corporations
- Financial institutions, such as banks
- Utility companies
- Healthcare providers, including hospitals
- Government agencies
- High net worth individuals, like celebrities and executives
- Organisations that manage sensitive data, including intellectual property, trade secrets, personal information, or medical records[74].

[72] Microsoft Threat Intelligence, *„Cryptojacking: Understanding and defending against cloud compute resource abuse"*, https://www.microsoft.com/en-us/security/blog/2023/07/25/cryptojacking-understanding-and-defending-against-cloud-compute-resource-abuse/, Microsoft, 25 July 2023.
[73] A. Sasson, „Analysing Web Application and API Attacks: The Cloud as a Target and a Launch Pad", https://unit42.paloaltonetworks.com/web-api-attacks-in-cloud/, Unit42, 2 June 2023.
[74] B. Lenaerts-Bergmans, *"Cyber Big Game Hunting"*, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/big-game-hunting/, CrowdStrike, 22 February 2024.

These types of attacks are often initiated using legitimate credentials, such as Microsoft 365 logins, obtained through phishing schemes. According to CrowdStrike, **five of the top ten MITRE tactics observed are identity-based**. Threat actors like FANCY BEAR and SCATTERED SPIDER have been known to exploit these techniques to gain initial access and establish persistence within targeted networks[75].

Cloud malware

According to Bitdefender's analysis, approximately 61% of all malware was directly delivered via cloud environments in 2021[76]. Furthermore, around 43.7% of malware discovered in enterprise cloud applications delivered ransomware, and 55.9% of malware-infected files found in cloud applications were shared publicly[77]. These figures are significant, especially considering that a large portion of today's web traffic is cloud related. *"On average, 5 out of every 1000 enterprise users attempted to download malware in Q1 2023"*[78]. As of 2023, more than 50% of all HTTP/HTTPS malware downloads originated from the SaaS applications[79].

Malicious campaigns targeting cloud environments

Based on the data, the primary adversary groups targeting cloud instances **originate predominantly from Russia or China**. Threat actors from these countries have shown significant interest in attacking and exploiting cloud environments, driven by motivations such as financial gain or advancing their countries' interests.

Moreover, malware targeting cloud environments is becoming increasingly prevalent, which is understandable given the rapid growth of the cloud sector.

It is already known that cloud environments are common targets for various threat actors. Below are several examples of specialized attacks targeting cloud environment users:

Description of the incident	Attack vector (initial access)	Recommendations
The exposure of AWS Identity and Access Management (IAM) access keys enabled attackers to establish a malicious	**Data leak** - This attack occurred due to exposed AWS IAM access keys obtained from publicly	Ensure that your organization has well-configured

[75] CrowdStrike, *"Insider's Playbook…,* p. 6-7.
[76] G. V. Hulme, *„Malware Delivered Via Cloud Services Rises",* https://www.bitdefender.com/en-us/blog/businessinsights/malware-delivered-via-cloud-services-rises/, Bitdefender, 23 March 2021.
[77] Note: this data comes from 2016, so the actual data now might be slightly different.
Netskope, *„Netskope Report Reveals 43.7% of Cloud-Based Malware Delivers Ransomware",* https://www.netskope.com/pt/press-releases/netskope-report-reveals-43-7-cloud-based-malware-delivers-ransomware, September 2016.
[78] Netskope, *„Cloud and Threat Report: Global Cloud and Web Malware Trends",* https://www.netskope.com/wp-content/uploads/2023/05/cloud-and-threat-report-global-cloud-and-web-malware-trends.pdf, May 2023, p. 3.
[79] G. Smith, *„75+ Surprising Cloud Security Statistics You Should Know in 2024"…, Ibidem.*

presence, leading to the scanning of over 230 million unique targets in search of sensitive information[80].	accessible .env files.	access controls to secure the data.
The Securonix Threat Research team uncovered a new infection chain, CLOUD#REVERSER, which uses cloud storage services like Google Drive and Dropbox to facilitate malicious operations[81].	**Phishing** - The attack chain began when a user received a phishing email and downloaded a ZIP archive attached to the message.	Avoid downloading files or attachments from external sources.
In late November 2023, Proofpoint researchers detected a new malicious campaign integrating credential phishing and cloud account takeover (ATO) techniques. The campaign, still active, involves threat actors targeting users with individualized phishing lures embedded within shared documents[82].	**Phishing** - Threat actors targeted users with individualized phishing lures within shared documents.	Avoid downloading files or attachments from external sources.
On May 15, 2023, Storm-0558 used forged authentication tokens to access user email accounts from approximately 25 organizations, including government agencies and related consumer accounts hosted in the public cloud[83].	**Authentication key forgery** - The initial vector involved acquiring an inactive Microsoft Account (MSA) consumer signing key, which the threat actor used to forge Azure Active Directory tokens.	Implement strict isolation between consumer and enterprise key stores to prevent overlap in key validation and token issuance between systems.

Table 1: Main techniques utilized to perform the attacks on cloud environments (MITRE ATT&CK framework).

The techniques most commonly employed by threat actors to attack cloud environments can be found in Appendix B.

Legislation related to cloud security

Security solutions and hardening practices are essential in addressing the insecure state of the cloud, but they are not the only tools available. A complementary approach, one with a different influence and broader reach, is legislation. For instance, implementing an **opt-out model** for certain default cloud configurations could

[80] M. Kelley, S. Johnstone, W. Gamazo, N. Quist, *"Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments"*, https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/, Unit42, 15 August 2024.
[81] D. Iuzvyk, T. Peck, O. Kolesnikov, *"Analysis and Detection of CLOUD#REVERSER: An Attack Involving Threat Actors Compromising Systems Using A Sophisticated Cloud-Based Malware"*, https://www.securonix.com/blog/analysis-and-detection-of-cloudreverser-an-attack-involving-threat-actors-compromising-systems-using-a-sophisticated-cloud-based-malware/, Securonix, 21 May 2024.
[82] The Proofpoint Cloud Security Response Team, *"Community Alert: Ongoing Malicious Campaign Impacting Microsoft Azure Cloud Environments"*, https://www.proofpoint.com/us/blog/cloud-security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments, Proofpoint, 12 February 2024.
[83] Microsoft Threat Intelligence, *„Analysis of Storm-0558 techniques for unauthorized email access*"…, Ibidem.

significantly enhance cloud security. This approach would require cloud providers and big tech companies to modify their deployment models and instance management practices to make secure configurations the default. Without these changes at the provider level, the proposed model cannot be effectively implemented.

This approach is emphasized in the new **National Cybersecurity Strategy of the United States**, as stated in The White House press release on March 2, 2023: *"We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organisations that are most capable and best positioned to reduce risks for all of us"*[84].

The Cyber Resilience Act

There is an interesting example of a missed opportunity for improvements in terms of security that could have enhanced cloud security: **The Cyber Resilience Act (CRA)** that came into effect this Autumn. According to the regulation, it states: *"On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall: (a)be delivered with a secure by default configuration, including the possibility to reset the product to its original state;*[85]*"* While it's a good step towards collective cybersecurity, it does not regulate services such as **Software-as-a-Service (SaaS),** which is a prime example of a complete cloud solution[86]. This is partially because SaaS is already regulated under NIS2[87]. To some extent, it's a lost opportunity to put pressure on big tech companies in the process of securing the cyber landscape in Europe. Pushing the CRA towards cloud solutions would surely impact their resilience.

Network and Information Systems Directive (NIS2)

Probably the most significant and important law related to cloud security established in recent years is the NIS2 Directive. NIS2 serves as a continuation and expansion of the original EU cybersecurity directive, NIS.

The primary objective of NIS2 is to enhance the security of network and information

---

[84] The White House, *"FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy"*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/, 2 March 2023.

[85] European Commission, *"Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020"*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454, 15 September 2022.

[86] Microsoft, *"What is SaaS ?"*, https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-saas, Microsoft Azure, 15 October 2024.

[87] Centre for Cybersecurity Belgium, *"Questions and answers on the Cyber Resilience Act (CRA)"*, https://ccb.belgium.be/en/questions-and-answers-cyber-resilience-act-cra, 15 October 2024.

systems across the EU. It mandates that operators of critical infrastructure and essential services implement suitable security measures and report any incidents to the relevant authorities[88].

NIS2 broadens the scope of EU-wide security requirements, and the range of organisations and sectors covered compared to the original NIS directive. This expansion aims to improve the security of supply chains, simplify reporting obligations, and enforce stricter measures and sanctions throughout Europe. As part of this expanded scope, cloud service providers are now included and required to meet these stringent requirements.

> Organisations providing cloud services are considered essential entities, which imposes specific requirements and obligations upon them. This means that vendors and cloud service providers will be held accountable, thereby enhancing the overall security of cloud services[89].

To support organisations in meeting these requirements, the CCB developed clear guidance through the creation of the CyberFundamentals (CyFun®) framework. This framework not only helps organisations secure their postures but also provides an opportunity to obtain a CyFun® or ISO/IEC 27001 certification/label.

[88] Safeonweb, *"The NIS2 Law",* https://atwork.safeonweb.be/nis2, 30 October 2024.
[89] *Ibidem.*

CONCLUSION

Given the specific characteristics of cloud environments and the relatively low maturity of organisations utilizing them, it is likely that cloud environments will increasingly become favoured targets for threat actors.

Cloud-related data indicates that more and more companies are increasingly reliant on cloud environments, a trend that is expected to accelerate due to the accessibility and cost-effectiveness of cloud solutions. As cloud adoption expands, threat actors are becoming more aware of the growing number of potential victims, adapting their tactics to exploit the new landscape.

Data from multiple threat sources reveals new dangerous trends, such as cryptojacking and big game hunting, along with threat actors specifically targeting cloud environments using various malware and techniques. Recent security incidents in cloud environments highlight these emerging threats.

Organisations often struggle to choose the correct cloud deployment models and services for their needs, which can lead to overwhelmed capabilities and result in unattended, unorganized cloud environments. Additionally, many organisations find it challenging to delineate their responsibilities and understand what falls under their jurisdiction, leading to issues with shadow IT.

Cloud environments have unique characteristics compared to on-premises infrastructures, such as scalability and connectivity with various parts of the infrastructure, including third parties. Studies have shown that cloud environments are frequently misconfigured, creating dangerous vulnerabilities that are easy targets for adversaries. Small and medium-sized enterprises (SMEs) are particularly vulnerable and are often primary targets for attackers.

Despite these challenges, there are solutions available for both small and large companies managing cloud environments. Organisations can implement various security measures tailored to their needs, such as guides, benchmarks, and adopting a DevSecOps approach. This includes multiple types of automated security measures like Cloud Access Security Brokers (CASB) and AI solutions.

Outlook of cloud threat landscape for 2025

The CCB projects the following key trends for 2025:

- **Increase in cloud environment attacks** - The number of attacks targeting cloud environments is very likely to rise, with small and medium-sized enterprises (SMEs) being the primary focus due to their relatively limited defensive capabilities.
- **Origins of threat actors** - the majority of threat actors are very likely to originate from Russia and China, driven primarily by motivations such as financial gain and national interests.
- **Adoption of AI by attackers** - it is likely that attackers will increasingly employ AI technologies to enhance their capabilities, particularly for executing phishing attacks and scaling automated attacks.
- **Increased reliance on automation for defence** - organizations are likely to expand their use of automated security measures, including AI and machine learning, to better safeguard their assets and respond to the complexity of cyber threats.
- **Growth in malware use** - the deployment of info-stealers and ransomware is likely to increase as attackers continue to use these tools to disrupt operations, steal sensitive data, and extort funds.

REFERENCES

1. A. Borgeaud, *„Most common security incidents in the cloud and on-premises worldwide in 2024”*, https://www.statista.com/statistics/1320178/common-cloud-security-attacks-worldwide/, Statista, 8 October 2024.
2. A. Chaudhary, *„Managing Cloud Misconfigurations Risks”,* https://cloudsecurityalliance.org/blog/2023/08/14/managing-cloud-misconfigurations-risks, Cloud Security Alliance, 14 August 2023.
3. A. Sasson, „Analysing Web Application and API Attacks: The Cloud as a Target and a Launch Pad”, https://unit42.paloaltonetworks.com/web-api-attacks-in-cloud/, Unit42, 2 June 2023.
4. A. Sheps, *„Cloud Shared Responsibility Model: Examples & Best Practices”,* https://www.aquasec.com/cloud-native-academy/cspm/shared-responsibility-model/, Aquasec, 13 July 2023.
5. Acumen Research and Consulting, *“Cloud Storage Market Size - Global Industry, Share, Analysis, Trends and Forecast 2022 – 2030”*, https://www.acumenresearchandconsulting.com/cloud-storage-market, February 2023.
6. Allot, *„Threat Bulletin – High Risk Apps”,* https://www.allot.com/resources/Threat_Bulletin_High-risk-Apps.pdf, May 2019.
7. B. Lenaerts-Bergmans, *“Cyber Big Game Hunting”,* https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/big-game-hunting/, CrowdStrike, 22 February 2024.
8. Breachsense, *„Data Breaches Cause Loss of Customer Trust”,* https://www.breachsense.com/blog/data-breach-trust/, 17 April 2024.
9. ByteHyde, *“What Are Code Vulnerabilities?”*, https://dev.to/bytehide/what-are-code-vulnerabilities-3lgj, Dev.to, 31 July 2024.
10. Center for Internet Security, *“CIS Controls v8 Cloud Companion Guide”,* https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide, 15 October 2024.
11. Centre for Cybersecurity Belgium, *“Questions and answers on the Cyber Resilience Act (CRA)”*, https://ccb.belgium.be/en/questions-and-answers-cyber-resilience-act-cra, 15 October 2024.
12. Cisco, *“What is Shadow IT”*, https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html, 23 October 2024.
13. Cloud IBM, *“Understanding Secure by Default Cluster VPC Networking”*, https://cloud.ibm.com/docs/containers?topic=containers-vpc-security-group-reference, IBM Cloud Docs, 14 October 2024.
14. Cloud Security Alliance, *“Cloud Controls Matrix (CCM)”,* https://cloudsecurityalliance.org/research/cloud-controls-matrix, 15 October 2024.
15. Cloudflare, *„What is a cloud workload protection platform (CWPP)?”,* https://www.cloudflare.com/learning/cloud/what-is-cwpp/, 24 October 2024.
16. Cloudflare, *„What is the cloud”,* https://www.cloudflare.com/learning/cloud/what-is-the-cloud/, 22 October 2024.
17. CrowdStrike, *“Insider's Playbook: Defending Against Cloud Threats”,* https://www.crowdstrike.com/resources/white-papers/insiders-playbook-defending-against-cloud-threats/, 28 August 2024.
18. Cyber Strategy Institute, *„The Rise of Cryptojacking Threat in 2023 by 650%”*, https://cyberstrategy1.medium.com/the-rise-of-cryptojacking-threat-in-2023-by-650-547ef4e29ad3, Medium, 17 July 2024.
19. D. Desai, D. Parekh, E. Laufer, *“2022 Cloud (In)Security Report”,* https://www.zscaler.com/blogs/security-research/2022-cloud-security-report, Zscaler, 15 February 2023.
20. D. Iuzvyk, T. Peck, O. Kolesnikov, *“Analysis and Detection of CLOUD#REVERSER: An Attack Involving Threat Actors Compromising Systems Using A Sophisticated Cloud-Based Malware”*, https://www.securonix.com/blog/analysis-and-detection-of-cloudreverser-an-attack-involving-threat-actors-compromising-systems-using-a-sophisticated-cloud-based-malware/, Securonix, 21 May 2024.
21. DoD Cyber Exchange Public, *“DoD Cloud Computing Security”*, https://public.cyber.mil/dccs/, 15 October 2024.
22. European Commission, *“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020”,* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0454, 15 September 2022.
23. Eurostat, *“Cloud computing - statistics on the use by enterprises”*, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-

_statistics_on_the_use_by_enterprises&oldid=632772, December 2023.
24. F. Dezeure, L. Moerel, G. Webster, *"Improving the World's Cyber Resilience, at Scale. Implementing Baseline Security by Default"*, SSRN, 16 February 2024.
25. F. Richter, *"Amazon Maintains Cloud Lead as Microsoft Edges Closer"*, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/, Statista, 2 May 2024.
26. FS-ISAC, *"FS-ISAC Principles for Financial Institutions' Security and Resilience in Cloud Service Environments"*, https://www.fsisac.com/hubfs/Knowledge/Cloud/PrinciplesForFinancialInstitutionsSecurityAndResilienceInCloudServiceEnvironments.pdf?hsLang=en, July 2024.
27. G. Smith, *"75+ Surprising Cloud Security Statistics You Should Know in 2024",* https://www.stationx.net/cloud-security-statistics/, StationX, 10 April 2024.
28. G. V. Hulme, *„Malware Delivered Via Cloud Services Rises",* https://www.bitdefender.com/en-us/blog/businessinsights/malware-delivered-via-cloud-services-rises/, Bitdefender, 23 March 2021.
29. Gartner, *"Gartner Says Cloud Will Become a Business Necessity by 2028"*, https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028, 29 November 2023.
30. Google Cloud, *„Advantages and Disadvantages of Cloud Computing",* https://cloud.google.com/learn/advantages-of-cloud-computing?hl=en, Google, 22 October 2024.
31. Google Cloud, *"Managing secure-by-default organization resources"*, https://cloud.google.com/resource-manager/docs/secure-by-default-organizationsorganisations, 15 October 2024.
32. IBM, *"Cost of a Data Breach Report 2024"*, https://www.ibm.com/downloads/cas/1KZ3XE9D.
33. ISO, *"ISO/IEC 27001:2022",* https://www.iso.org/standard/27001, October 2022.
34. K. Chin, *"What is the Cost of a Data Breach in 2024?",* https://www.upguard.com/blog/cost-of-a-data-breach-2024, UpGuard, 28 October 2024.
35. K. Harpsoe, *"Why SMEs are now a prime target for ransomware"*, https://www.smeweb.com/why-smes-are-now-a-prime-target-for-ransomware/, SME Web, 7 October 2024.
36. L. Ballejos, *"What Is BadUSB? Definition and How to Prevent It",* https://www.ninjaone.com/it-hub/endpoint-security/what-is-badusb/, Ninja One, 2 February 2024.
37. L. Constantin, *"Why code reuse is still a security nightmare"*, https://www.csoonline.com/article/571073/why-code-reuse-is-still-a-security-nightmare.html, CSO, 26 July 2021.
38. Lockheed Martin, *„The Cyber Kill Chain",* https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, 24 October 2024.
39. M. Kelley, S. Johnstone, W. Gamazo, N. Quist, *"Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments"*, https://unit42.paloaltonetworks.com/large-scale-cloud-extortion-operation/, Unit42, 15 August 2024.
40. M. Zhang, *"Top 10 Cloud Service Providers Globally in 2024"*, https://dgtlinfra.com/top-cloud-service-providers/, Dgtl Infra, 15 October 2024.
41. Microsoft Learn, *"User Account Control Overview"*, https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/, Microsoft, 26 March 2024.
42. Microsoft Threat Intelligence, *„Analysis of Storm-0558 techniques for unauthorized email access*", https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/, Microsoft, 14 July 2023.
43. Microsoft Threat Intelligence, *„Cryptojacking: Understanding and defending against cloud compute resource abuse"*, https://www.microsoft.com/en-us/security/blog/2023/07/25/cryptojacking-understanding-and-defending-against-cloud-compute-resource-abuse/, Microsoft, 25 July 2023.
44. Microsoft, *"Microsoft cloud security benchmark documentation",* https://learn.microsoft.com/en-us/security/benchmark/azure/, Microsoft Learn, 1 November 2024.
45. Microsoft, *"Shared responsibility in the cloud",* https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility, 29 September 2024.
46. Microsoft, *„What is a cloud access security broker (CASB)?",* https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb, 24 October 2024.
47. Microsoft, *„What is CSPM?"*, https://www.microsoft.com/en-us/security/business/security-101/what-is-cspm, 24 October 2024.
48. Microsoft, *"What is SaaS ?",* https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-saas, Microsoft Azure, 15 October 2024.
49. Microsoft, *„What is the cloud?",* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud, 22 October 2024.
50. MITRE ATT&CK, *"Cloud Matrix"*, https://attack.mitre.org/matrices/enterprise/cloud/, 15 October 2024.
51. MITRE ATT&CK, *"Data Encrypted for Impact",* https://attack.mitre.org/techniques/T1486/, 24 October

2024.
52. MITRE ATT&CK, *„Data from Cloud Storage",* https://attack.mitre.org/techniques/T1530/, 24 October 2024.
53. MITRE ATT&CK, *„Exploit Public-Facing Application",* https://attack.mitre.org/techniques/T1190/, 24 October 2024.
54. MITRE ATT&CK, *"Exploitation for Client Execution",* https://attack.mitre.org/techniques/T1203/, 24 October 2024.
55. MITRE ATT&CK, *"Exploitation for Privilege Escalation",* https://attack.mitre.org/techniques/T1068/, 24 October 2024.
56. MITRE ATT&CK, *„Valid Accounts: Cloud Accounts",* https://attack.mitre.org/techniques/T1078/004/, 24 October 2024.
57. MITRE ATT&CK, *„Valid Accounts",* https://attack.mitre.org/techniques/T1078/, 24 October 2024.
58. MITRE ATT&CK, *Data from Local System",* https://attack.mitre.org/techniques/T1005/, 24 October 2024.
59. National Institute of Standards and Technology, *"The NIST Cybersecurity Framework (CSF) 2.0",* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, 26 February 2024.
60. Netskope, *„Cloud and Threat Report: Global Cloud and Web Malware Trends",* https://www.netskope.com/wp-content/uploads/2023/05/cloud-and-threat-report-global-cloud-and-web-malware-trends.pdf, May 2023.
61. Netskope, *„Netskope Report Reveals 43.7% of Cloud-Based Malware Delivers Ransomware",* https://www.netskope.com/pt/press-releases/netskope-report-reveals-43-7-cloud-based-malware-delivers-ransomware, September 2016.
62. P. Doerfler, M. Marincenko, J. Ranieri, Y. Jiang, A. Moscicki, D. McCoy, K. Thomas, *"Evaluating Login Challenges as a Defense Against Account Takeover"*, https://storage.googleapis.com/gweb-research2023-media/pubtools/5021.pdf, New York University, Google.
63. Palo Alto Networks, *"Cloud Security Is a Shared Responsibility"*, https://www.paloaltonetworks.com/cyberpedia/cloud-security-is-a-shared-responsibility, 17 October 2024.
64. Palo Alto Networks, *„What Is CSPM? | Cloud Security Posture Management Explained",* https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-security-posture-management, 24 October 2024.
65. R. Sujatha, *„What is pay-as-you-go Cloud Computing (PAYG)?"*, https://www.digitalocean.com/resources/articles/pay-as-you-go-cloud-computing, DigitalOcean, 18 October 2024.
66. Red Hat Documentation, *"Chapter 2. Changing SELinux states and modes",* https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/using_selinux/changing-selinux-states-and-modes_using-selinux#changing-selinux-states-and-modes_using-selinux, 15 October 2024.
67. Red Hat, *"IaaS, PaaS, SaaS"*, https://www.redhat.com/rhdc/managed-files/iaas-paas-saas-diagram5.1-1638x1046.png, 15 October 2024.
68. Red Hat, *„What is Infrastructure as Code (IaC)?"*, https://www.redhat.com/en/topics/automation/what-is-infrastructure-as-code-iac, 23 October 2024.
69. S. Morgan, *"The World Will Store 200 Zettabytes Of Data By 2025",* https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/, 1 February 2024.
70. Safeonweb, *"CyberFundamentals Framework"*, https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework, 17 October 2024.
71. Safeonweb, *"The NIS2 Law",* https://atwork.safeonweb.be/nis2, 30 October 2024.
72. SentinelOne, *„Cloud Security Attacks: Types & Best Practices",* https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-attacks/, 30 September 2024.
73. SentinelOne, *„Top 10 Cloud Security Breaches in 2024"*, https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-breaches/, 31 July 2024.
74. Shodan, https://www.shodan.io/, 15 October 2024.
75. Standard Application Benchmark, *"SAP Standard Application Benchmarks"*, https://www.sap.com/about/benchmark/appbm/cloud.html, 15 October 2024.
76. Synergy Research Group, *„European Cloud Providers Continue to Grow but Still Lose Market Share",* https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share, 27 November 2022.
77. Tenable, *"2024 Cloud Security Outlook Navigating Barriers and Setting Priorities"*, https://static.tenable.com/marketing/research-reports/ResearchReport-2024_Cloud_Security_Outlook.pdf, 2024.
78. Tenable, *"6 Cloud Security Tips For 3rd-Party Risk"*, https://www.tenable.com/blog/6-cloud-security-tips-for-3rd-party-risk, 16 November 2022.

79. The Proofpoint Cloud Security Response Team, *"Community Alert: Ongoing Malicious Campaign Impacting Microsoft Azure Cloud Environments"*, https://www.proofpoint.com/us/blog/cloud-security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments, Proofpoint, 12 February 2024.
80. The White House, *"FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy",* https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/, 2 March 2023.
81. Trend Micro, *„Pushing The Outer Limits Trend Micro 2024 Midyear Cybersecurity Threat Report"*, https://www.trendmicro.com/vinfo/be/security/research-and-analysis/threat-reports/roundup/pushing-the-outer-limits-trend-micro-2024-midyear-cybersecurity-threat-report, 15 August 2024.
82. TrendMicro, *"Smart Yet Flawed: IoT Device Vulnerabilities Explained"*, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained, 28 May 2020.
83. Zscaler*, "What Is a Shared Responsibility Model?",* https://www.zscaler.com/br/resources/security-terms-glossary/what-is-shared-responsibility-model, 15 October 2024.

ABOUT THE CCB

The **Centre for Cybersecurity Belgium (CCB)** is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through optimal information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately.

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

The **CyTRIS (Cyber Threat Research and Intelligence Sharing)** Department of the Centre for Cybersecurity Belgium monitors cyber threats and publishes regular reports. The Team collects, analyses and distributes information on threats, vulnerabilities and attacks on the information and communication systems of Belgium's vital sectors (critical infrastructure, government systems, critical data).

CyTRIS is also responsible for the Early Warning System (EWS). The EWS includes the information exchange platforms of the Belgian CSIRT. CyTRIS is responsible for the operational communication and information exchange with other national CSIRT. CyTRIS also provides the "Spear Warning" procedure. A "Spear Warning" is an individual warning about an infection or vulnerability sent to organisations.

The CCB Connect & Share events, such as the Quarterly Cyber Threat Report (QCTR) events organised by CyTRIS, bring together different stakeholders and consultation platforms at least once a quarter and inform all participants as well as the Organisations of Vital Interest about the active cyber threats. At the QCTR event, the operation of the Early Warning System (EWS) is also discussed. Through this platform, the CyTRIS Team sends pertinent and analysed threat information to national security agencies, Vital Interest Organisations, their sectoral authorities and other partners.

The QCTR is also offered as a webinar and is open to anyone, worldwide (https://app.livestorm.co/ccb?lang=en).

APPENDIX A: TECHNICAL TERMINOLOGY

This appendix consists of essential terminology required to understand the document.

Term	Explanation
Active Directory	A directory service developed by Microsoft for Windows domain networks, which manages and stores information about network resources and enables centralized administration of user and computer accounts.
Advanced Persistent Threat (APT)	A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period, typically to steal data or monitor activity.
API	A set of rules and protocols for building and interacting with software applications, allowing different software systems to communicate with each other.
Banker	A type of malware specifically designed to steal sensitive information related to online banking and financial transactions.
BitsAdmin	A command-line tool used to create, download, and monitor file transfer jobs, especially useful for managing Background Intelligent Transfer Service (BITS) jobs in Windows.
Blacklisting	A security measure that blocks access to specific applications, websites, or IP addresses known to be malicious or unauthorized.
Botnet	A network of compromised computers, known as bots, controlled by a single attacker or group of attackers to carry out various malicious activities, such as DDoS attacks, spamming, and data theft.
C++	A high-level programming language known for its performance and efficiency, widely used for system/software development and game programming.
Cloud Security Breach	An incident in which unauthorized access or damage occurs to data stored in a cloud computing environment, potentially leading to data loss or exposure.
Cluster	A set of connected computers that work together as a single system, often used to improve performance and provide redundancy.
Command and Control	The infrastructure used by cybercriminals to communicate with, and control compromised systems within a botnet or malware-infected network.
Command line	A text-based interface used to interact with software and operating systems, where users type commands to perform specific tasks.
CVE	A list of publicly disclosed information security vulnerabilities and exposures, maintained by the MITRE Corporation.
Cyber Resilience Act	Legislation aimed at ensuring that organisations can continue to operate and recover quickly from cyber incidents, focusing on preparedness, response, and recovery.

DevOps	A set of practices that combine software development (Dev) and IT operations (Ops) to shorten the development lifecycle and deliver high-quality software continuously.
Endpoint Detection and Response (EDR)	A cybersecurity technology focused on detecting, investigating, and responding to suspicious activities on endpoints, such as computers and mobile devices.
Firewalling	The process of using firewalls to protect a network by controlling incoming and outgoing network traffic based on predetermined security rules.
Identity Access Management (IAM)	A framework of policies and technologies for ensuring that the right individuals have access to the right resources at the right times for the right reasons.
Infostealer	A type of malware designed to steal sensitive information from infected systems, such as login credentials, financial information, and personal data.
JSON	A lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate.
Kubernetes	An open-source container orchestration platform that automates the deployment, scaling, and management of containerized applications.
Malware	Short for malicious software, malware refers to any software intentionally designed to cause damage to a computer, server, client, or computer network.
Managed detection and response (MDR)	A service that provides organisations with threat detection and response capabilities through a combination of technology, processes, and human expertise.
Memory corruption prevention	Techniques and technologies used to prevent the exploitation of vulnerabilities caused by errors in memory management, such as buffer overflows.
Multi-factor authentication	A security process that requires users to provide two or more verification factors to gain access to a resource, enhancing security by combining multiple forms of identification.
National Cybersecurity Strategy	A comprehensive plan developed by a government to protect national interests against cyber threats, outlining goals, priorities, and actions to improve cybersecurity.
NIS2	A European Union directive aimed at enhancing cybersecurity across member states by establishing common security requirements and improving cooperation among national authorities.
OS hardening	The process of securing an operating system by reducing its surface of vulnerability, which involves removing unnecessary services, applying patches, and configuring security settings.
PowerShell	A task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language.
Ransomware	A type of malware that encrypts a victim's data and demands a ransom payment to restore access to the data.

Ransomware-as-a-Service	A business model where ransomware creators lease their malware to affiliates, who then use it to carry out attacks and share the profits with the creators.
RAT	A type of malware that allows attackers to remotely control an infected computer, often used for spying, data theft, and other malicious activities.
Remote Desktop Protocol	A proprietary protocol developed by Microsoft that allows users to connect to and control another computer over a network connection.
Runtime	The period during which a program is running, as well as the environment in which the program is executed, including the software and hardware resources available to it.
Search Engine Optimization (SEO)	The practice of optimizing websites to improve their ranking on search engine results pages, thereby increasing visibility and attracting more visitors.
Security-by-design	A principle of system and software design that prioritizes security from the beginning of the development process, ensuring that security is built into the architecture and not added as an afterthought.
SELinux	A security module integrated into the Linux kernel that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC).
Service Level Agreement	A contract between a service provider and a customer that specifies the expected level of service, including performance metrics and responsibilities.
Shadow cloud	The use of cloud services by employees without the knowledge or approval of the IT department, potentially leading to security risks and compliance issues.
Shodan	A search engine that allows users to find specific types of computers connected to the internet using various filters, often used to identify vulnerable systems and devices.
Small and Medium-sized Enterprises (SMEs)	Businesses whose personnel numbers fall below certain limits, typically characterized by fewer employees and lower revenue compared to large enterprises.
Software-as-a-Service (SAAS)	A software distribution model in which applications are hosted by a service provider and made available to customers over the internet.
SQL Injection	A type of attack where malicious SQL code is inserted into an input field for execution, allowing attackers to manipulate the database and access unauthorized data.
System integrity check	The process of verifying the integrity of a system to ensure that it has not been tampered with or compromised.
Threat Actor	An individual or group responsible for carrying out malicious activities against targets, including cybercriminals, hacktivists, and state-sponsored attackers.
Trojan	A type of malware disguised as legitimate software that, once activated, can perform harmful actions on the infected system, such as stealing data or

	installing additional malware.
URL	The address used to access resources on the internet, such as web pages, images, and files.
User Account Control (UAC)	A security feature in Windows operating systems that helps prevent unauthorized changes to the system by prompting users for permission or an administrator password before allowing certain actions.
Virtual private cloud	A private cloud computing environment that exists within a shared public cloud infrastructure, offering the benefits of a private cloud while using public cloud resources.
XSS	A security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users, potentially leading to data theft, session hijacking, and other malicious activities.
Zero-day	A security vulnerability that is unknown to the software vendor and has no patch available, often exploited by attackers before the vendor becomes aware of it.
WannaCry	WannaCry is a type of ransomware that first appeared in May 2017, exploiting a vulnerability in the Windows operating system's Server Message Block (SMB) protocol. It rapidly encrypts files on infected systems and demands a ransom payment in Bitcoin for decryption.
LockBit	LockBit is ransomware detected in September 2019, known for its speed and efficiency in encrypting data. It often spreads through phishing emails and exploits vulnerabilities, targeting businesses and organisations by encrypting files and demanding a ransom for the decryption key.

Table 2: List of essential technical terminology.

APPENDIX B: CLOUD MATRIX – MITRE ATT&CK – TOP TECHNIQUES

This section highlights the most commonly employed techniques used to attack cloud instances.

Technique	Description	Example
T1190 - **Exploit Public-Facing Application**	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration[90].	Exploiting a SQL injection vulnerability in a web application, which can allow attackers to manipulate the database or execute arbitrary code on the server.
T1005 - **Data from Local System**	Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration[91].	Attackers may target .env files on web servers, which often store API keys, passwords, or sensitive environment variables, allowing them to escalate their attack or exfiltrate valuable information.
T1486 - **Data Encrypted for Impact (Ransomware)**	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources[92].	Ransomware such as **WannaCry** and **LockBit** encrypts files on the compromised system, and the attackers leave a ransom note instructing the victim on how to make a payment to retrieve the decryption key.
T1078 - **Valid Accounts**	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defence Evasion[93].	After conducting a phishing attack, an adversary gains login credentials to a cloud service like Microsoft Azure and uses the valid credentials to access sensitive information or escalate their privileges.
T1078.004 – **Valid Accounts: Cloud Accounts**	Valid accounts in cloud environments may allow adversaries to perform actions to achieve Initial Access, Persistence, Privilege Escalation, or Defence Evasion[94].	In a Microsoft Azure attack, an attacker may use compromised cloud account credentials to access email, databases, or virtual machines, enabling further data theft

[90] MITRE ATT&CK, *„Exploit Public-Facing Application",* https://attack.mitre.org/techniques/T1190/, 24 October 2024.
[91] MITRE ATT&CK, *Data from Local System",* https://attack.mitre.org/techniques/T1005/, 24 October 2024.
[92] MITRE ATT&CK, *"Data Encrypted for Impact",* https://attack.mitre.org/techniques/T1486/, 24 October 2024.
[93] MITRE ATT&CK, *„Valid Accounts",* https://attack.mitre.org/techniques/T1078/, 24 October 2024.
[94] MITRE ATT&CK, *„Valid Accounts: Cloud Accounts",* https://attack.mitre.org/techniques/T1078/004/, 24 October 2024.

		or the deployment of malware.
T1203 - Exploitation for Client Execution	Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behaviour[95].	A user might receive a malicious email attachment with a vulnerability in a PDF reader. When opened, the PDF exploits the vulnerability to execute arbitrary code and compromise the system.
T1530 - Data from Cloud Storage Object	Adversaries may access data from cloud storage[96].	Once access is obtained, the attackers can read, modify, or exfiltrate data stored in the cloud.
T1068 - Exploitation for Privilege Escalation	Adversaries may exploit software vulnerabilities in an attempt to elevate privileges[97].	An attacker exploits a known vulnerability in Kubernetes (e.g., CVE-2018-1002105) to gain unauthorized access to the Kubernetes API server.

Table 3: List of most used techniques by the threat actors.

[95] MITRE ATT&CK, *"Exploitation for Client Execution",* https://attack.mitre.org/techniques/T1203/, 24 October 2024.
[96] MITRE ATT&CK, *„Data from Cloud Storage",* https://attack.mitre.org/techniques/T1530/, 24 October 2024.
[97] MITRE ATT&CK, *"Exploitation for Privilege Escalation",* https://attack.mitre.org/techniques/T1068/, 24 October 2024.

APPENDIX B2: CLOUD MATRIX – MITRE ATT&CK

This appendix consists of all utilized techniques used for attacking the cloud[98].

Figure 10: Cloud Matrix – overview.

[98] MITRE ATT&CK, *"Cloud Matrix"*, https://attack.mitre.org/matrices/enterprise/cloud/, 15 October 2024.

APPENDIX C: TABLES & FIGURES

APPENDIX D: AUTOMATED CLOUD SECURITY

Cloud Workload Protection Platform (CWPP) is a tool designed to detect and remove threats within cloud environments. It can be likened to a traditional antivirus, but operates on a much larger scale, managing multiple instances simultaneously in a unified manner. CWPP constantly monitors workspaces, containers, and serverless functions to identify and eradicate threats. It handles firewalling, operating system hardening, system integrity checks, blacklisting of services and applications, memory corruption prevention, and a wide range of Endpoint Detection and Response (EDR) functions[99]. **CWPP is focused on securing the individual cloud workspaces.**

Cloud Security Posture Management (CSPM) a comprehensive solution designed to identify security issues and misconfigurations across cloud environments. CSPM tools help automate the remediation of these misconfigurations and compliance issues by providing continuous monitoring. Implementing CSPM tools is often considered a best practice after migrating to the cloud or switching to a different provider. CSPM tools also handle incident response, offer remediation recommendations, monitor compliance, and integrate with DevOps processes across hybrid and multi-cloud environments. Some CSPM solutions enable security teams to proactively identify and address vulnerabilities in cloud environments, preventing potential breaches before they occur[100]. **CSPM is focused on the overall security posture of the cloud environments.**

Cloud Access Security Broker (CASB) is a security policy enforcement point positioned between cloud service providers and enterprise users. Its main role is to ensure that the security policies of an organization are enforced when cloud-based resources are accessed. CASBs provide detailed visibility into cloud service usage across the organization. They help maintain compliance with regulatory requirements by enforcing relevant controls and policies. CASBs protect data both in transit and at rest by applying technologies such as data loss prevention (DLP). Additionally, they offer protection against cloud-specific threats like malware and account hijacking and enforce access control measures such as multi-factor authentication and other identity management techniques[101]. **CASB is focused on securing access to cloud services.**

---

[99] Cloudflare, *„What is a cloud workload protection platform (CWPP)?”,* https://www.cloudflare.com/learning/cloud/what-is-cwpp/, 24 October 2024.
[100] Microsoft, *„What is CSPM?”*, https://www.microsoft.com/en-us/security/business/security-101/what-is-cspm, 24 October 2024.
Palo Alto Networks, *„What Is CSPM? | Cloud Security Posture Management Explained”,* https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-security-posture-management, 24 October 2024.
[101] Microsoft, *„What is a cloud access security broker (CASB)?”,* https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb, 24 October 2024.

DISCLAIMER

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

This document contains technical information written mainly in English. Indeed, this technical information is taken directly from reports communicated to the CCB by various international partners (European network of CSIRTs, international organisations, foreign companies, etc.), which are written in English. Moreover, this information related to the security of networks and information systems is addressed to the organisations concerned under the benefit of urgency and to IT services which use the English terms of computer language.

A translation into Dutch, French or German of this technical information can nevertheless be requested from the CCB.

The CCB accepts no responsibility for the content of this document.

The information provided:

- are exclusive of a general nature and do not intend to take into consideration all particular situations;
- are not necessarily exhaustive, precise or up to date on all points;

Responsible editor:
Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 18
1000 Brussels

Legal Depot: D/2025/14828/001