CyberProof®
A UST Company

How to leverage automation to mitigate risk

Securely managing enterprise-scale cloud transformation

Contents

How cloud transformation increases the likelihood of cyberattack

> **"There is no business strategy without a cloud strategy."**
>
> **According to Gartner, by 2025 over 95% of new digital workloads will be deployed on cloud-native platforms. As more than 85% of organizations will be cloud-first by 2025, Gartner believes that enterprises "will not be able to fully execute on their digital strategies without the use of cloud-native architecture and technologies."**

The move to cloud-native architecture is a strategic shift, enabling agility, accelerating time to market, and allowing enterprises to focus on their core value while outsourcing infrastructure to a reliable third party.

However, for most enterprises, there is no such thing as a simple "lift and shift." Moving IT architecture from on-premises to the public cloud has a serious impact on security resilience and processes.

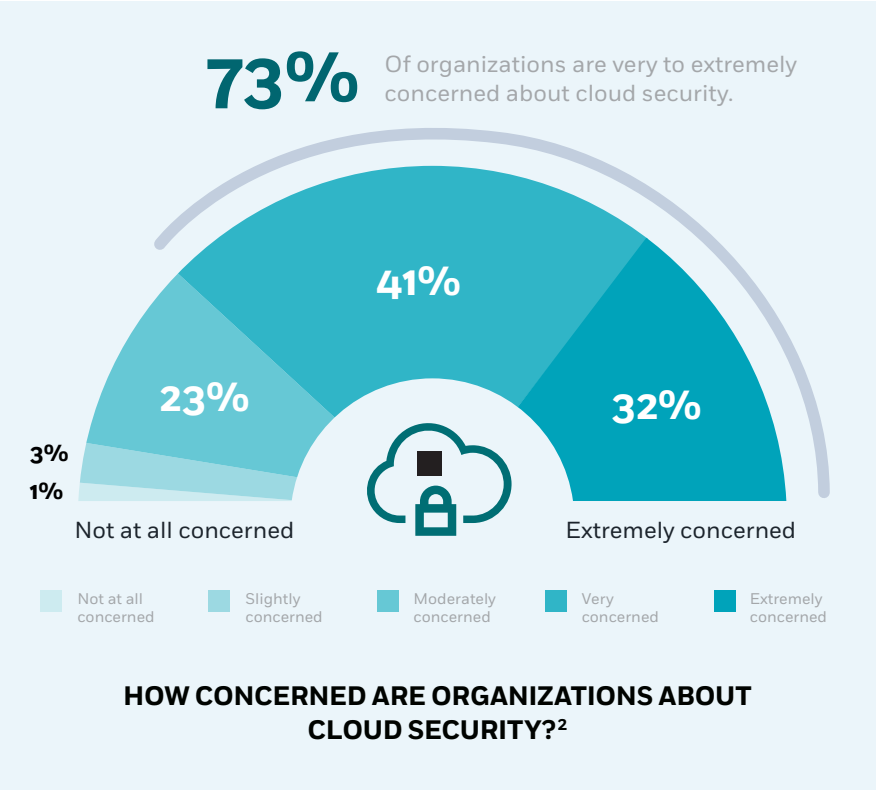
It's likely that existing security solutions were designed for on-premises environments, which means they:

- Are not equipped to handle **a greater number of endpoints**, including new connected devices such as IoT and OT.
- Will not be built to work with **a Zero Trust model** on the cloud, where handling data, access and privileges are significantly more complex.
- Cannot efficiently handle **cloud data volumes**, including cost-effectively collecting, storing, analyzing and scaling data from new sources.
- Do not include cloud-native tools such as **automation** to enhance threat detection and response capabilities.

With cloud migration, attack surface management becomes more complex, data security & privacy may be harder to protect, there are likely to be issues with interoperability – and, if the process is not handled correctly, your costs go up.

---

[1] Gartner Press Release, Cloud Will Be The Centerpiece of New Digital Experiences



HOW CONCERNED ARE ORGANIZATIONS ABOUT CLOUD SECURITY?[2]

Cloud migration means handling Big Data

According to Forbes, "Enterprises cannot afford to lag behind in their data modernization efforts." Migrating data to the cloud is a critical element of this, but it's only step one.

With the move to the cloud, enterprises can begin to build a strategy for how to use Big Data to train AI models that can offer better security and data protection, and enhance digital transformation projects exponentially over time. Big Data can't be handled without automation. But by leveraging Big Data correctly, you can open the doors for complex trend analysis and pattern detection – by tracking data over time.

However, Big Data needs to be optimized, filtered and stored in a cost-effective way, or cloud costs will quickly spiral out of control.

This is where cloud-native tools such as Microsoft Azure's Data Explorer (ADX), Google Cloud Dataflow, or AWS Data Analytics services come in. These tools can parse, tag and process data at speed and scale, providing real-time analysis as data enters the network. Enterprises can use cloud-native offerings to manage large volumes of data over time at significantly lower cost.

Cloud-native technologies are a great start, and can also be augmented for cybersecurity purposes with the help of Managed Detection and Response (MDR) services. For example, an MDR can enhance the use of automation and Big Data by enabling custom logs to be collected and ingested to perform security analytics. Together, the use of cloud-native offerings alongside a robust MDR service allows for immense flexibility when dealing with data, reduced storage costs, full data compliance, and faster threat detection and risk reduction.

---

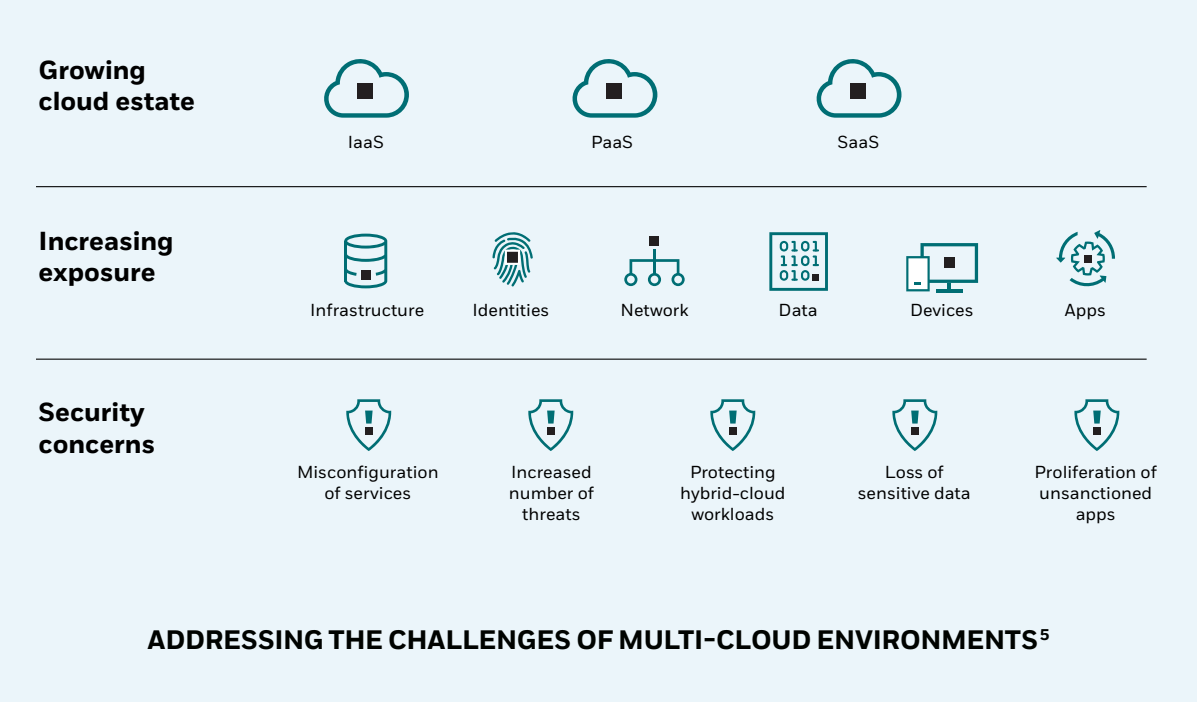
[2] https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/ar-cybersecurity-cloud-security.pdf

[3] Forbes: "Unlock more value from your data with data modernization".

Why a multi-cloud strategy is critical for effective transformation

According to Enterprise Strategy Group, 86% of companies use Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) offerings from two or more providers.[4] Some use as many as five or six different cloud providers to meet their enterprise needs.

A multi-cloud environment is one in which enterprises use two or more cloud providers, either public or private, for their cloud computing services. Multi-cloud helps organizations avoid vendor lock-in, leverage best-of-breed services from each provider, and maximize availability and reliability on the cloud.



ADDRESSING THE CHALLENGES OF MULTI-CLOUD ENVIRONMENTS[5]

However, one of the most critical elements to consider when embracing a multi-cloud strategy is cyber security. A robust MDR solution can support security operations center (SOC) teams in:

- **Managing access permissions:** Identity and Access Management (IAM) frameworks are crucial in a multi-cloud environment. This should be considered both for users, and for devices themselves.
- **Duplicating security processes:** When teams are working across multiple clouds, identical security settings should be used, automating where possible to reduce the likelihood of human error.
- **Adopting a single pane of glass:** One dashboard to see everything in an enterprise environment is the only way to ensure there are no blind spots or gaps in security.
- **Supporting transformation:** When security best practices are incorporated from day one, rather than added in retroactively – risk is greatly reduced. Look for a solution that offers in-depth planning as well as monitoring and threat response.

[4] Tech Target: "The features of Multi-Cloud Networking Architecture"
[5] Microsoft Ignite: 26:22

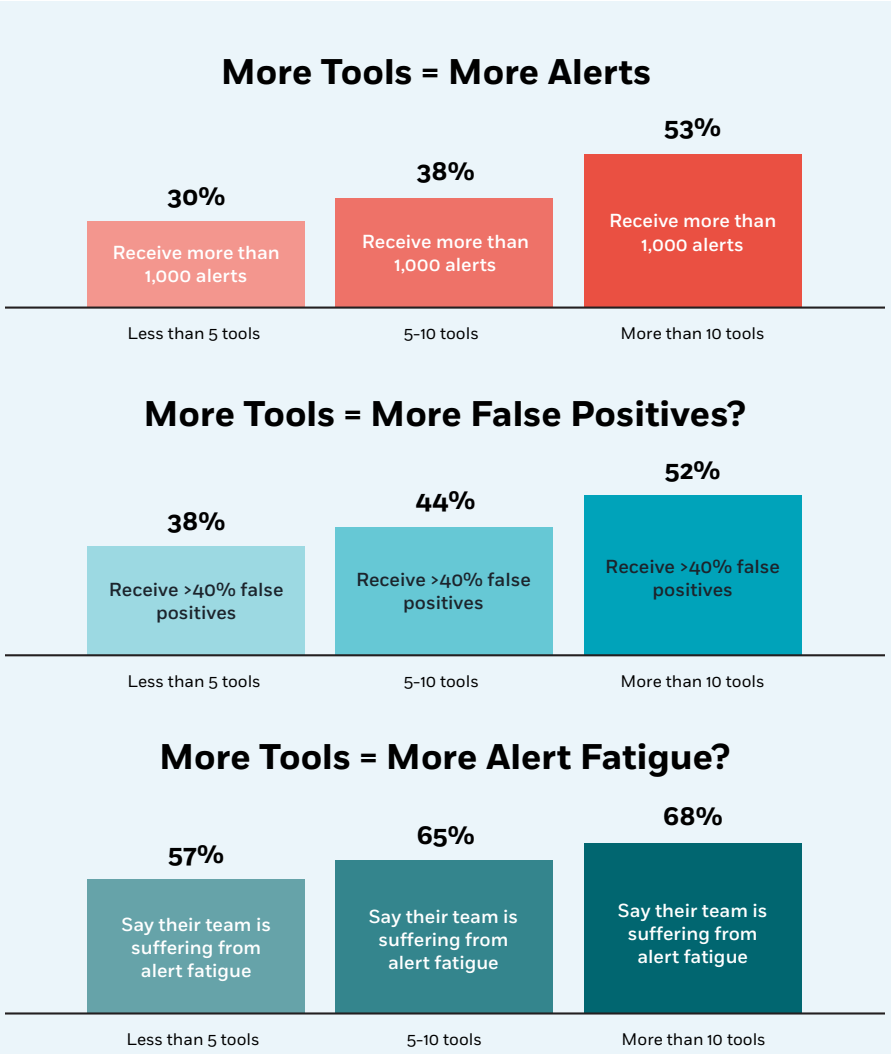
Leveraging automation to improve efficiency, scalability and reduce risk

For today's SOC teams, alerts have become a necessary evil. More than half of organizations are receiving over 500 alerts every single day, with 20%-40% false positive alarms.[6] The more tools they use, the more challenges they experience.

The result? Critical alerts are missed, competing tools lead to confused mitigation, SOC teams are experiencing alert fatique, and there's a desperate need for a way to distinguish the signal from the noise.

Adding context to alerts through alert enrichment is a mainstay of cloud-native security operations, allowing enterprises to prioritize their response to critical events on the cloud, act quicker in a crisis, and eliminate the risk of false positives. Alert enrichment can:

- Correlate and consolidate multiple alerts into one
- Chain together potential attack scenarios from multiple events
- Prioritize critical incidents in line with business context
- Uncover signature techniques used by specific types of threat



ALERT FATIGUE: THE MORE TOOLS, THE MORE PROBLEMS

[6] Virtualization and Cloud Review, "New Cloud Cybersecurity Worry: 'Alert Fatigue'"

While automation supports scalability – the human element is crucial

Forbes calls humans the "unexpected game changer in cybersecurity."[7] The vast majority of security operations today can be managed by machine, and automation is critical in the cloud for maximizing the effectiveness of your SOC and improving the speed and accuracy of detection and response.

However, human capabilities offer creative insight and expertise that can make all the difference. The following table highlights some of the distinctions between reactive, preemptive and proactive hunting styles, and indicates which activities are best performed through automation and which are best handled by human experts:

Reactive	Pre-emptive	Proactive
▪ Manual search and investigation methods ▪ Relies on known Indicators of Compromise (IOC) ▪ Often triggered by a known threat or recorded anomaly ▪ Utilizes suspicious hashes, IP addresses, or domain names	▪ Utilizes automation to collect more data and search at scale ▪ Relies on anomalies in behavioral patterns ▪ Hunting for malicious actions based on unusual activity ▪ May use attacker's Tools Tactics and Procedures (TTPs) to inform the hunt	▪ Creative and freestyle hunting ▪ Relies on human threat hunters forming hypotheses about attacker behavior ▪ Assumes attackers have evaded existing security controls ▪ Focuses on activities after initial breach – What will the hacker do next?

HALLMARKS OF DIFFERENT HUNTING APPROACHES

Proactive threat hunting is a compelling example of how human intervention is critical, where technology is limited.

Threat hunters will develop a security baseline by comprehensively evaluating the network, and then pinpointing potential policy violations, reducing the attack surface proactively.

Human intervention allows for deeper investigative conversations, following hypotheses through to validation, and hunting for malicious activity which flies under the radar of technology-led security controls.

[7] Forbes: "Why Humans are the Unexpected Game Changer in Cyber Security"

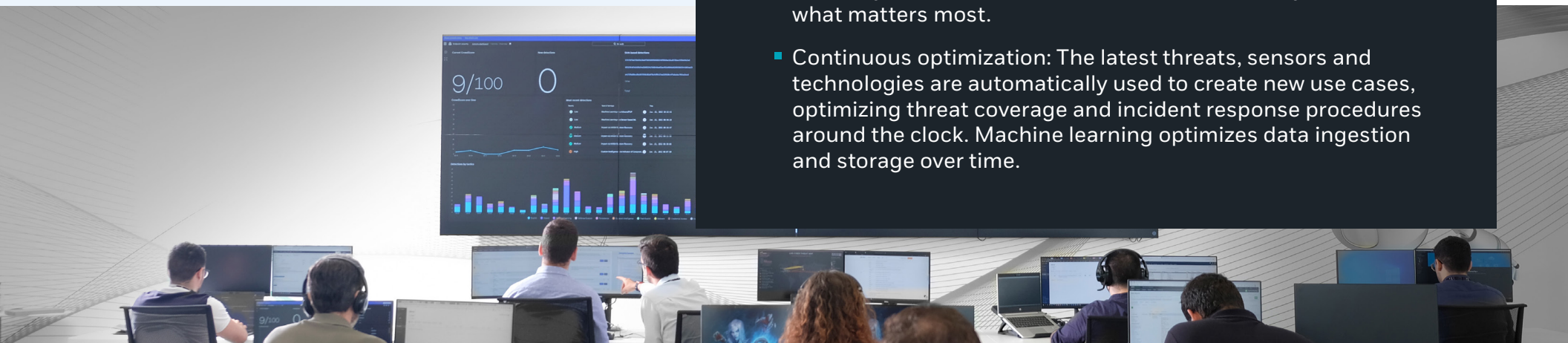
Advanced MDR services reduce the risk of cyberattack

In the cloud, leveraging automation can provide higher levels of efficiency and consistency, and add smart capabilities to a business' security toolbelt, but only when all your solutions and processes are integrated so that your SOC has a single view.

Automation can support enterprises in scaling their operations to keep pace with the new volumes of data being generated by detection technology. Automation takes the place of missing staff, providing the new skills necessary to manage must-haves such as zero trust and cost management in the cloud. However, automation can never replace the human element.

An advanced MDR service is built to support enterprises that are moving to the cloud, and offers a hybrid blend of human and automated capabilities. At CyberProof, we offer:

- Human and machine intelligence: Automate your security processes, and ensure you have top-tier cyber expertise for that the threats that require human intervention. Utilize frameworks such as MITRE ATT&CK for full visualization and mapping, alongside creative thinking and threat hunting, out of the box.
- Transparency and collaboration: Access a single dashboard to oversee your cybersecurity operations on the cloud, with visibility over your contextualized, consolidated threat landscape. Communicate in real time, both internally and with our experts to make the right decisions.
- Operational efficiency: Automated deployment lets you hit the ground running, with airtight detection and response working for you from day one. As threats arise, alert enrichment slashes your MTTR and contextual response lets you focus on what matters most.
- Continuous optimization: The latest threats, sensors and technologies are automatically used to create new use cases, optimizing threat coverage and incident response procedures around the clock. Machine learning optimizes data ingestion and storage over time.



Key takeaways

Automation is key to mitigating risk in a cloud-native environment – and working with an MDR provider like CyberProof can help you navigate the complexity and optimize the work of your security operations team.

When managing enterprise-scale security operations, keep in mind that:

- **Big Data** must be optimized, filtered and stored in a cost-effective way, to prevent costs from spiraling out of control.
- **Multi-cloud environments,** which have many advantages for enterprises, must be handled with care to avoid security gaps, and require a strategy that relates to access permissions, duplicate security processes and more.
- **Alert enrichment** is key to ensuring enterprises can prioritize their response to critical events and act quickly in a crisis.
- **Human expertise** must be leveraged correctly, ensuring human capabilities are used for creative insight and the expertise that can make all the difference to responding to an attack in real time.

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com.

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum

cyberproof.com