

# Optimizing your cloud security transformation

# Contents

Introduction	3
The challenges of today's evolving threat landscape	5
Managing the risks of cloud adoption	7
The cost of the transition	9
Maintaining control with shared responsibility	11
Key takeaways: Partnering for success	12
About CyberProof	13
About UST	13

# Introduction

As enterprise organizations grow into cloud adoption, many are embracing the agility and scalability that cloud provides. Today, most enterprises have multi-cloud infrastructures. **The migration to cloud has led to a growth in assets, but this growth comes at a price of a parallel growth in discovered vulnerabilities. In fact, global cyberattacks increased by 38% in 2022, compared to 2021.**<sup>1</sup>

Finding a way to balance this dual growth of both assets and vulnerabilities - while simultaneously maintaining the agility gained from cloud transformation - can be difficult. The skills and tools required to maintain effective cybersecurity operations in the cloud may not match the available skills and technologies already employed by your organization. emerging only now.

## Combining digital, cloud and security

As your organization increasingly relies on digital technologies to operate and compete, these systems become mission-critical - often containing vast amounts of information about customers and employees. Consequently, they become prime targets for cyber threats. In the age of generative AI, this increased risk of cyberattacks can be addressed by successfully undergoing cloud security transformation, which provides several benefits:

### Flexibility

- Everything as code
- Standardized set of tools
- Accessibility anytime, anywhere
- Scalability

### Insights

- Advanced threat hunting
- Machine learning-based anomaly detection
- Correlation of data and analytics

### Speed

- Forensics and response automation
- Accelerate time to market

### Cost

- Reduced CapEx
- Efficient cloud storage
- SaaS SOAR, data lake, SIEM, EDR

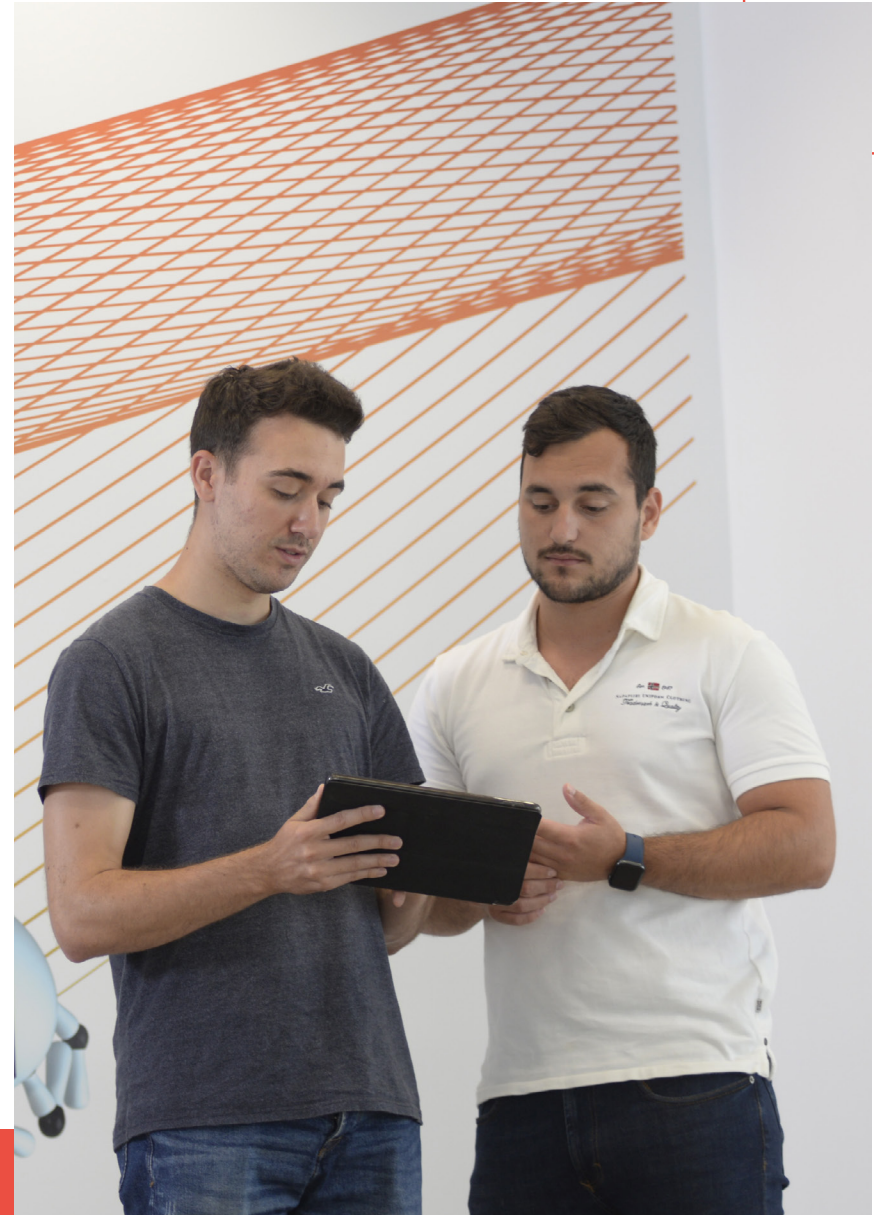
<sup>1</sup> <https://www.infosecurity-magazine.com/news/global-cyberattack-volume-surges/>



## Digital transformation - handle with care

Cloud security transformation is necessary to support the enterprise's digital transformation, which comes with certain challenges:

- Managing and securing cloud-based systems require retraining talent to become proficient in a new environment, as the shift to cloud security demands a different skill set.
- Application security also becomes more complex as attackers are even more likely to target vulnerabilities and APIs in cloud-based applications, misconfiguration, identity, and hosts as risks.
- The security portfolio needs to adapt. Many existing tools designed for on-premises environments may not provide the right level of protection, and this necessitates the adoption of new products.
- New kinds of cyberattacks, such as supply chain attacks, become a greater risk.
- Modern architectures become essential; legacy systems are usually designed as flat systems - and this can increase the risk of attack.



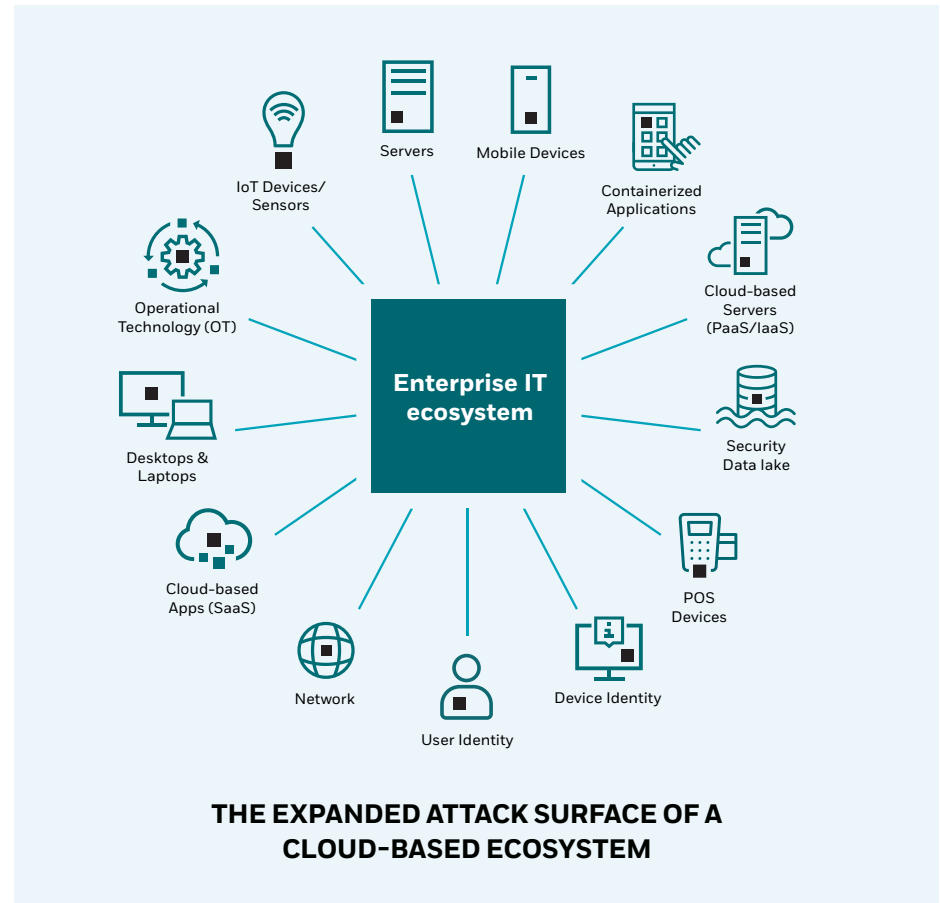
# The challenges of today's evolving threat landscape

Cybercriminals continue to improve in their sophistication, organization, and determination to target businesses across various industries. Moreover, cybercriminals have been drawn to the cloud as a new target in the attack surface.

**Current research<sup>2</sup> shows a 95% increase in cloud exploitation in 2022.**

The widespread adoption of remote work and reliance on cloud-based collaboration tools have further expanded the attack surface. Employees access sensitive data and applications from multiple locations and devices, making it crucial to secure these connections and ensure data privacy.

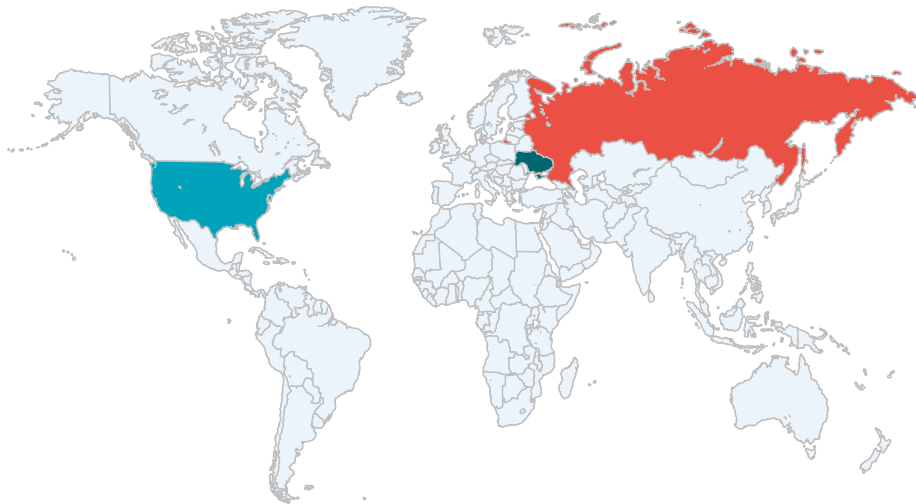
<sup>2</sup> Cloud exploitation is up 95%. What should you do about it?



## Global threats emerge





Together with the evolving cyber threats, there are additional factors that contribute to the changing nature of the threat landscape.

- **Geopolitical instability** – Cyber espionage and state-sponsored attacks targeting cloud infrastructures and services have increased, such as recent **Russian cyberattacks on Ukrainian infrastructures** as a direct tool of war. This geopolitical instability has had a direct impact on the changing nature of the threat landscape for enterprises.



AREAS OF INCREASED GEOPOLITICAL TENSIONS

- **Private sector attacks** – Forrester research<sup>3</sup> demonstrates that nation-state attacks are no longer purely targeting government data and equipment but have branched out to the private sector. Organizations in the private sector must beware. Nation-state actors easily access public cloud infrastructure.
- **Generative AI** – The launch of ChatGPT followed by other generative AI platforms has accelerated the cyber arms race, amplifying the potential for attacks on private enterprises. For example, WormGPT as well as PentestGPT, and many other new tools based on ChatGPT, are leveraged for malicious causes – to assist them in developing more sophisticated, AI-powered attacks.
- **Global recession** – As organizations face financial constraints and potential layoffs, their security posture may be compromised due to reduced investments in cybersecurity defense measures. This creates an opportunity for cybercriminals and internal threat actors, who can exploit vulnerabilities in the cloud.

 <p><b>Geopolitical tensions</b> Have a spillover effect in the cyber sphere</p>	 <p><b>Private enterprise</b> Is impacted by the increased cyber activity</p>	 <p><b>Global recession</b> Cyber defenses are spread thinner</p>	 <p><b>Generative AI</b> Amplifies attacks on the private sector</p>
--	---	---	--

THE CHANGING NATURE OF THE GLOBAL THREAT LANDSCAPE

<sup>3</sup>Forrester report 2023: Lessons learned from the world's biggest data breaches and privacy abuses

## The increased risks of legacy defenses

Legacy security solutions ill-suited for cloud environments leave organizations more vulnerable to cyber threats. There are way too many security tools in use, and the older tools are either not compatible with newer, software-as-a-service (SaaS) tools, or are nearing their end of life.

Moreover, rapid detection and response capabilities rely on ingesting and processing large volumes of data, which is impossible without cloud-native solutions that can scale and aggregate data across the entire IT environment.







## Managing the risks of cloud adoption

Cloud adoption creates new business risks that need to be addressed. The shift to the cloud introduces potential vulnerabilities, including data breaches, ransomware attacks, and intellectual property theft. To effectively mitigate these risks, security transformation becomes essential.

The process of cloud security transformation allows you to align your organization’s security posture with the evolving business landscape. It ensures that your security measures are robust and adaptable to the changing cloud environment.

The new standard utilizes real-time posture management to continuously monitor and assess your security posture, promptly detecting any anomalies or threats. By proactively identifying and addressing vulnerabilities, you can minimize the impact of potential security breaches and protect sensitive data.

			
<p><b>Transformation from on-prem.</b> especially for highly regulated industries</p>	<p><b>Optimizing costs of ingestion and storage</b> as data continues to grow</p>	<p><b>Meeting compliance &amp; regulatory requirements</b> in each region</p>	<p><b>Ensuring customer data protection</b> including privacy and intellectual property concerns</p>

### CHALLENGES DURING THE JOURNEY



## Leveraging your cloud toolkit

Effective monitoring plays a crucial role in promptly detecting and responding to security incidents. According to Forrester, given the dynamic nature of cloud environments, organizations should adopt real-time monitoring solutions that provide visibility into the network, applications, and user activities, such as:

- **Security Incident and Event Management (SIEM)** – A long-time standard for providing real-time analysis of security alerts generated by applications and network hardware, which becomes more effective when leveraging cloud scaling and resources.
- **Security Orchestration, Automation, and Response (SOAR)** – By orchestrating between different tools and people, SOAR automates investigation and response and provides a single view for the SOC team to plan, monitor and respond – unifying security tool communication and streamlining response activities.
- **Extended Detection and Response (XDR)** – Unifies endpoint and workload security capabilities with critical visibility into the network and cloud – collecting threat data from previously siloed security tools across an organization's technology stack.

In a cloud-based ecosystem, the use of proactive threat intelligence, advanced threat hunting and continuous monitoring continue to be key – helping enterprises prioritize, identify and mitigate potential security threats before they cause significant damage. By correlating threat patterns from internal data with MITRE ATT&CK techniques to identify potentially vulnerable entry points, an attack can be remediated more effectively.

## Getting started with the process

Any project requiring major change management is a cause for caution and concern – and this certainly applies to cloud security transformation. The complexity of the process means that extensive planning and coordination are necessary across various teams and departments. This can be overwhelming, and may cause reluctance – i.e., a preference to maintain the current security model.

For a smoother outcome, organizations should **establish a clear process**, breaking down the cloud security transformation into manageable phases and engaging stakeholders from different departments to ensure effective coordination.

**By creating a clear roadmap, setting realistic goals, and establishing open lines of communication, you can navigate the complexities of cloud security transformation more efficiently.**

If you don't have the required skillsets in-house, **seek out expertise externally** to fill in the gaps. Managed cloud security providers help give direction to transformative processes, using their expertise to map out a targeted process and avoid common stumbling blocks – to accelerate adoption of a more secure posture.



# The cost of the transition

Implementing cloud security solutions requires new hardware, software, and training investments. During the transitional period, costs may be a significant concern due to the need to dual run parallel processes during the migration period. However, you can optimize the cost of transformation and save funds without cutting corners, through:

- **Proper design and management** which can offset your initial costs through long-term savings
- **Optimization of cloud security architecture** with proper planning and design to align with specific needs and budget constraints
- **Thorough cost-benefit analysis** considering upfront and downstream costs, clarifying the potential return on investment (ROI)



A cost-benefit analysis is especially important when addressing data ingestion and storage costs for SIEM and EDR systems. For example, managing the ingestion cost for SIEM requires careful planning. At CyberProof, we use the CyberProof Log Collector coupled with a best-in-class big data analytics platform, to reduce annual storage costs for our clients, while ingesting significantly greater quantities of data.



**Automatically scale, ingest, store and retain structured & unstructured data**



**Run complex queries on large data sets to get near real-time responses**



**Advanced analytics to detect complex threats using large data sets**



**Build machine learning models & algorithms to define specific use cases**



**Create custom visualizations and reports to provide continuous visibility**

**USING A CENTRALIZED DATA LAKE WITH SECURE COLLECTION, PRE-PROCESSING AND RETENTION OF LOGS**

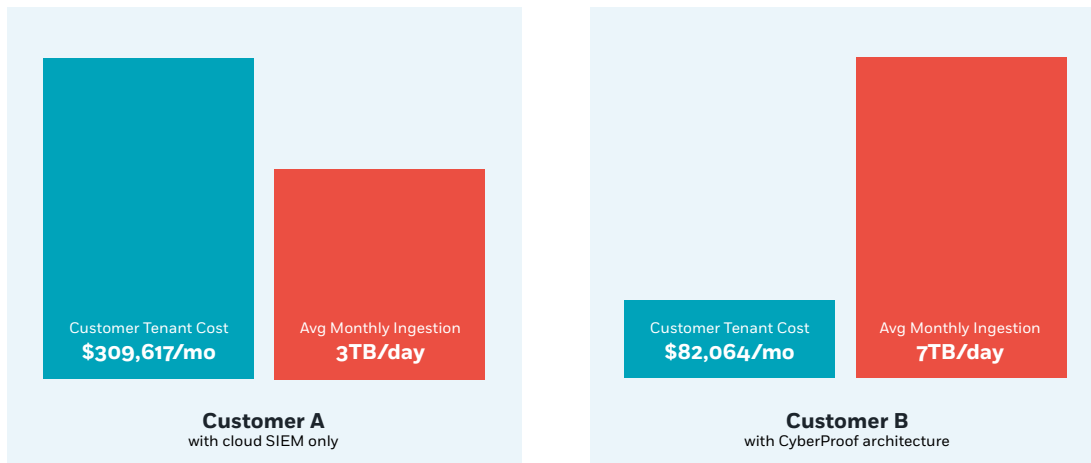
## Managed data collection and data lake solutions

Leveraging a well-designed and managed data collection and data lake solution can drastically reduce costs and create synergy with IT teams. You can extract actionable security intelligence from big data while controlling ingestion and storage costs by effectively collecting, analyzing, and storing log data.

Advanced managed service providers can provide real-time custom tagging, integration with custom data sources, and aggregation filtering to reduce up to 80% of large-scale cybersecurity costs. This type of approach allows you to prioritize real-time alerting for critical events while meeting compliance reporting requirements.

### Manage your data ingestion costs at scale

with our custom architecture approach



\*Real client examples

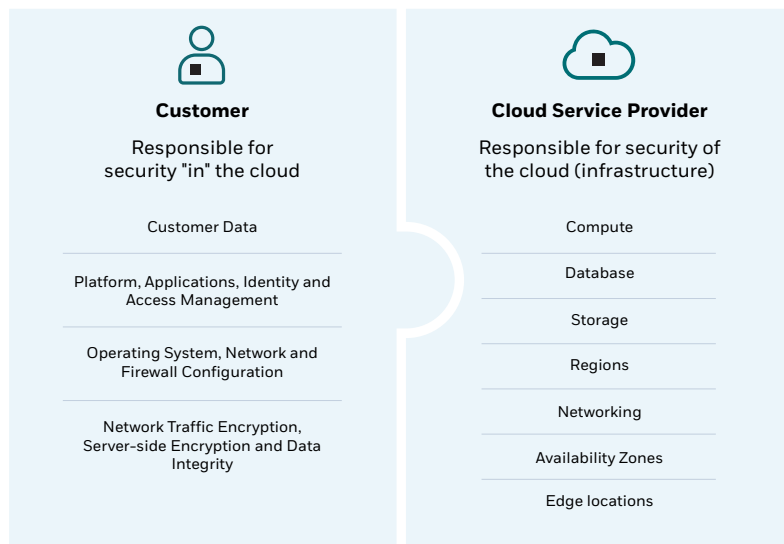
At CyberProof, we build scalable data lakes for our clients. The data in a data lake can be used for:

- **Fraud detection** – By leveraging machine learning (ML), data scientists can gain insights – using the enormous quantities of data to detect anomalies and thereby identify cases of fraud.
- **Investigations of rogue employees** – Using the data about users and hosts collected by the security team and by business applications. For example, data indicates which users were connected to which hosts, and what actions were done on which platforms. Security teams can investigate and track down rogue employees before they do damage and/or identify a user who performed malicious activity.

Moreover, a data lake can be shared with external business units – giving the security team and CISO the ability to “charge back” transactions, thereby amortizing costs. CISOs faced with budgetary restrictions can offer this capability to other business units and thereby gain added value, which can help optimize the organization’s financial resources.

# Maintaining control with shared responsibility

Moving security operations to the cloud requires a shift in how you manage control over the security infrastructure. The transition often requires relying on a third-party provider for various aspects of security. At the same time, a balance can be struck – so that you can leverage their advanced capabilities while still maintaining control.



## HOW ENTERPRISES WORK TOGETHER WITH A MANAGED CLOUD SECURITY PROVIDER

Managed cloud security providers enable you to gain access to security solutions that offer enhanced protection and scalability. These types of partnerships give you access to a providers' investments in the latest technologies, expert security professionals, and regulation compliance.

Working with managed cloud security providers, you can maintain control over your data and implement robust security governance and monitoring mechanisms:

- Regularly monitoring and auditing security controls
- Conducting penetration testing
- Enforcing strong access management practices

## Addressing compliance in new environments

For highly regulated companies, cloud security transformation must demonstrate parity or improvement in the security posture relative to the existing implementation. But even for organizations that are not highly regulated, meeting compliance is a financial must.

**In 2022 alone, organizations such as Didi Global were fined \$1.19 billion for privacy violations.<sup>1</sup> Amazon's fine of \$888 million due to GDPR violations<sup>2</sup> is another example of the direct impact of compliance failures.**

When organizations undergo cloud transformation, they must maintain the same standards in terms of data security and privacy measures. This is of particular importance in highly regulated industries. Where Security Incident and Event Management (SIEM) is used, for example, the effectiveness of detection rules, playbooks, and other sources must be established.

<sup>1</sup> Top 10: Fines Issued for Data Protection Violations

<sup>2</sup> Amazon Gets Record \$888 Million EU Fine Over Data Violations

## Protecting data in the cloud

When migrating data and critical assets to the cloud environment, the protection of sensitive data, privacy, and intellectual property is a concern. Possible misconfigurations and overexposure of data are not unusual, and research from IBM shows that this **accounts for 15% of breaches** in the cloud.

Building a full-scale cybersecurity framework helps to mitigate the risk of misconfigurations, vulnerabilities, and human error by leveraging detection and response. Automation and optimization techniques help to drive rapid response capabilities, eliminating threats and mitigating exposures before any significant harm can be done.



## Key takeaways: Partnering for success

Ensuring successful cloud security transformation requires a collaborative approach between many stakeholders. Some of the benefits of this kind of partnership include:



**Adopting a holistic approach** – Partnering with a managed cloud security provider allows you to tap into deep experience and develop a comprehensive security strategy that addresses specific concerns and requirements. This strategy should encompass various aspects, including cost reduction, data management, and collaboration.



**Reducing security costs** – A well-managed data collection and data lake solution can optimize the expense of log data ingestion and storage – allowing you to extract actionable security intelligence from big data.



**Accessing the right expertise at the right time** – Managed cloud service providers help organizations overcome challenges in staffing specialized skill sets. A cyber threat intelligence (CTI) team helps enterprises stay ahead of new and emerging threats. This is augmented by advanced threat hunting, which proactively seeks out malicious actors that may have slipped past defenses.



**Collaboration and transparency** – Managed cloud security providers who adopt a flexible and collaborative approach can act as an extension of your SOC team – meeting the needs of your organization by fostering a strong partnership throughout the cloud security transformation journey.



## 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.

Visit us at [www.cyberproof.com](http://www.cyberproof.com).

## About UST

For more than 23 years, UST has worked side by side with the world's best companies to make a real impact through transformation. Powered by technology, inspired by people, and led by our purpose, we partner with our clients from design to operation. Through our nimble approach, we identify their core challenges, and craft disruptive solutions that bring their vision to life. With deep domain expertise and a future-proof philosophy, we embed innovation and agility into our clients' organizations—delivering measurable value and lasting change across industries, and around the world. Together, with over 30,000 employees in 30+ countries, we build for boundless impact—touching billions of lives in the process.

Visit us at [www.UST.com](http://www.UST.com)