CyberProof®
A UST Company

Microsoft

4 Fantastic Superpowers of Cloud-Native XDR

Contents

Everything everywhere all at once

Cyber threats are adapting as rapidly as the technologies we use to ward them off. Enterprises are taking note.

As edge environments expand and IoT devices multiply, the cost of protecting your business has likely grown. IDG found that the average annual security budget is nearly $9 million.1 Despite the recurring investment in security infrastructure, Security Operation Center (SOC) teams, and cybersecurity insurance, bad actors still penetrate company networks 9 times out of 10.[1]

ANNUAL SECURITY BUDGETS[2]

$3.7 M

< 10K Employees

$8.7 M

Average Budget

$19.7 M

Larger Enterprises

To address gaps in traditional cybersecurity practices, reduce alert fatigue, and shorten the time to detect and respond to threats, future-focused businesses are turning to cloud-native extended detection and response (XDR) solutions. Whereas on-premises threat detection systems (on-prem SIEMs, EDR, etc.) run into storage challenges and data disparity, cloud-native XDR can aggregate security information from your entire environment to help teams isolate and respond to threats faster.

Achieve greater confidence in your security posture and protect your assets as you migrate to the cloud by ensuring your XDR solution features these four “fantastic” superpowers: extended visibility, data optimization, automation, and security as code.

Extended visibility

In cybersecurity, vigilance is the name of the game. Without eyes and ears everywhere, no detection and response system can be effective.

When migrating security operations to the cloud, only cloud-native XDRs can maximize your visibility and context around threat intelligence. They do this by filtering massive volumes of events to obtain high-context alerts.

Learn more about the difference between on-premises, cloud-based, and cloud-native detection and response.

VIEW INFOGRAPHIC →

Whereas typical endpoint detection and response covers you across emails, applications, and devices, XDR extends protection across identities and cloud environments. Moreover, powerful cloud-native SIEMs use machine learning to proactively find anomalies hidden within acceptable user behavior, reducing false positive and false negative alerts.

XDR also helps you maintain end-to-end visibility of the data itself as it is migrated from cloud to on-prem, or vice versa. Security teams can identify where data was encrypted and if there was any exfiltration. It's like x-ray vision for your most important assets.

With a comprehensive view of your data across multi-cloud, or even multi-country environments, security teams can report to incident response managers faster and with higher quality information. This improved communication compounds the value of your security teams by informing better decision making and allocation of resources.

Data optimization

With transformation projects underway, multiple cloud migrations, and widespread remote work environments, C-Suite security officers are under more stress about their data connectivity.

And that's not considering the new regulations and government standards that have emerged as more and more business takes place in cyberspace.

CISOs are designing their data strategies to ensure long-term resilience and adaptability. Among the hurdles standing in their way are log collection bottlenecks, data search capacities, and federated org structures.

Companies need supercomputing abilities to navigate the swarm of information they collect. Cloud-native XDR can be customized with features that enhance:

- Log collection
- Parsing
- Tagging
- Filtering of security data

By storing lower value data in a cloud data lake while routing high valued data into detection systems, the SIEM and XDR work together to clean and route large volumes of information.

Even with this technology, data collection from non-cloud-native sources will always be a thorn in the paw. To prevent blind spots that allow attackers to hide in the network undetected, security teams need to establish a continuous process for collecting new formats of data. These activities are essential to collect all relevant security information, but they require the time of data scientists with valuable experience in software and data engineering.

Azure Data Explorer (ADX) works as a data translator, helping you scale activities like hunting and reporting.

CyberProof Log Collector (CLC) provides a wider lens for your security teams and helps speed up threat detection by augmenting the Microsoft security stack.

Automation

An immediate advantage to deploying cloud-native XDR is the ability to automate processes that bog security teams down.

On any given day, SOC analysts:

- Patch and test enterprise systems
- Deploy infrastructure improvements
- Address support tickets from the organization's employees
- Report on the company's security posture to management

Up to 80% of common tasks can be automated and orchestrated with built-in AI and ML.[2]

In larger and more complex environments, SOC teams get spread thin and can develop myopia around daily alert verifications and short-term recovery strategies. By removing tier 1 and tier 2 activities from their workload, security teams can spend more time analyzing and reacting to potential threats. To that end, automation brings about greater speed to insight, helping teams react quickly and with strong consensus.

Modern SIEMs, like Microsoft Sentinel, act as a single security analytics platform for multiple cloud environments. Within the SIEM, artificial intelligence works to connect and master data streams, ingest and verify alerts across the entire enterprise, and report to security analysts with actionable information. Cloud-native XDR helps SOCs hunt queries, run playbooks, and even deploy infrastructure as code.

Security Operations Center Activity Tiers

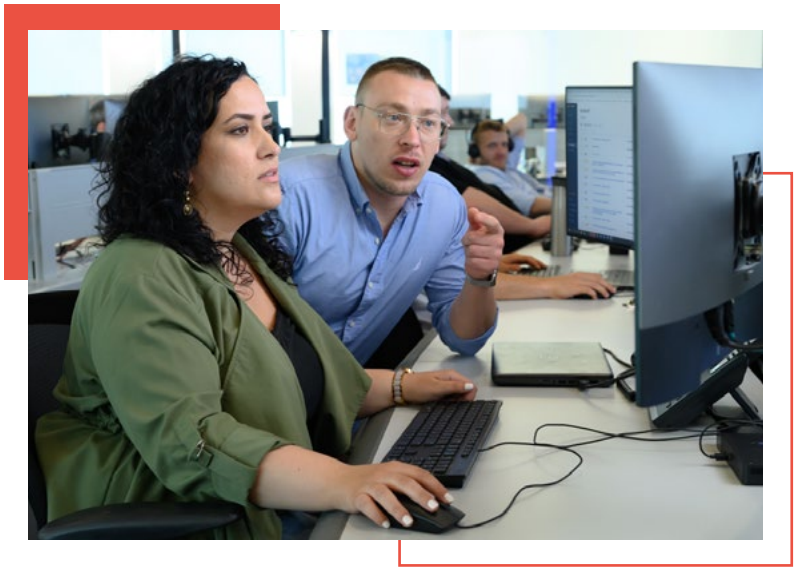
TIER 1
Review daily alerts, verify genuine incidents, configure monitoring tools.

TIER 2
Evaluate alerts flagged in tier 1, address real security incidents, pinpoint affected systems and run diagnostics, gauge size threat level of attack, create strategy for containment and recovery.

TIER 3
Manage critical incidents, carry out vulnerability assessments and penetration tests, assess resilience of the organization, isolate weaknesses.

Security as code

Perhaps the most powerful feature of cloud-native XDR is the ability to transcend typical infrastructure hurdles by deploying Infrastructure as Code (IaC).



Now, security teams can use DevOps environments and Continuous Integration/Continuous Deployment (CI/CD) pipelines to update content such as detection rules, playbooks, reports, automation rules, and hunting queries across multiple workspaces.

In other words, analysts can make major infrastructure and security modifications in real time.

Deploying new security capabilities and updates through scripts, rather than having to deploy new virtual machines or new hardware, provides greater speed to insight and flexibility. With security as code, your infrastructure is adaptable; it can be modified at any time with a click. Security teams can make the same updates to every workspace.

This exciting capability also requires a cultural shift. A 'security as code' methodology asks security teams to get in the heads of developers, and for developers to reciprocate. To reduce friction, be sure to automate security scans and tests, build a continuous feedback loop, and validate test scripts so they can be replicated across different projects. Engage your most experienced cloud security professionals to catalog best practices so that you can preserve hard-won wisdom and experience.

Microsoft Azure provides native support for IaC via the Azure Resource Manager.

CyberProof experts can define declarative templates that specify the infrastructure required to deploy their solutions.

Don't go it alone

The greatest obstacle that SOC managers face in modernizing their detection and response strategy is allocating the time and resources required to manage cloud-native security monitoring.

For those who have been in the trenches of a poorly planned migration, the idea of transformation can conjure fears of data loss and corruption, long periods of downtime, or endless unforeseen costs. For healthcare companies, financial services firms, utilities companies, or any business that collects personnel data, risk is not an option.

Only 30% of organizations in a recent study feel they can effectively keep up with the evolving cybersecurity threat landscape.[1]

Even companies with established security operations centers and a deep bench will seek a third party to help them optimize their XDR strategy. Managed Detection and Response (MDR) providers bring advanced best practices, ranks of experienced security analysts, and special tools to unlock the full security potential of the cloud.

Choose an MDR provider if you are:

1. Experiencing difficulty finding and retaining cybersecurity talent
2. Lacking resources to monitor security at all hours
3. Unsure of best tools and processes for your organization
4. Unable to verify whether alerts are real threats
5. Not responding quickly enough to security incidents

MDR checklist

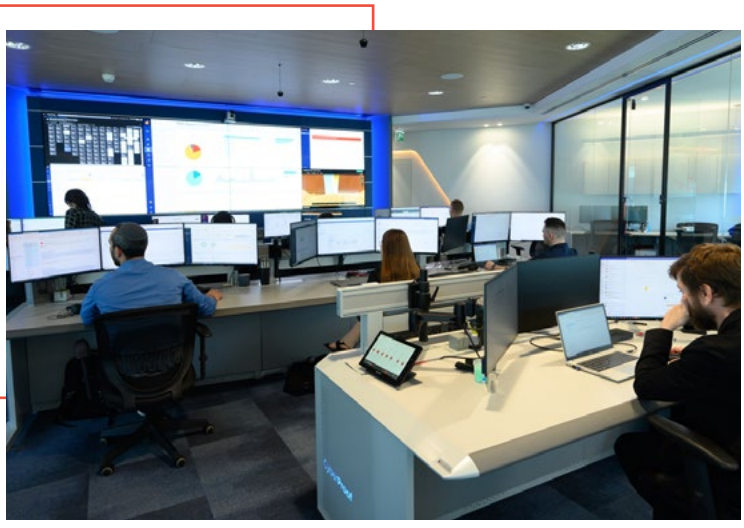
Your Managed Detection and Response provider will be on your front lines.

Ensure they have these capabilities to protect your assets:

- ☐ Extensive experience deploying large scale cloud-native SIEM & XDR solutions
- ☐ Use Case Kits that enable fast onboarding and visibility of cloud threats
- ☐ Alignment to the MITRE ATT&CK Matrix
- ☐ Customized monitoring of tailored queries, detection rules, etc.
- ☐ Rapid alert prioritization and communication channels
- ☐ Automated DevOps approach to deploying security stack infrastructure
- ☐ Transparent processes and clear KPI reporting
- ☐ Hybrid SOC model that can act as an extension of your team
- ☐ Proprietary tools and cost management techniques
- ☐ Expertise in navigating cloud security monitoring costs

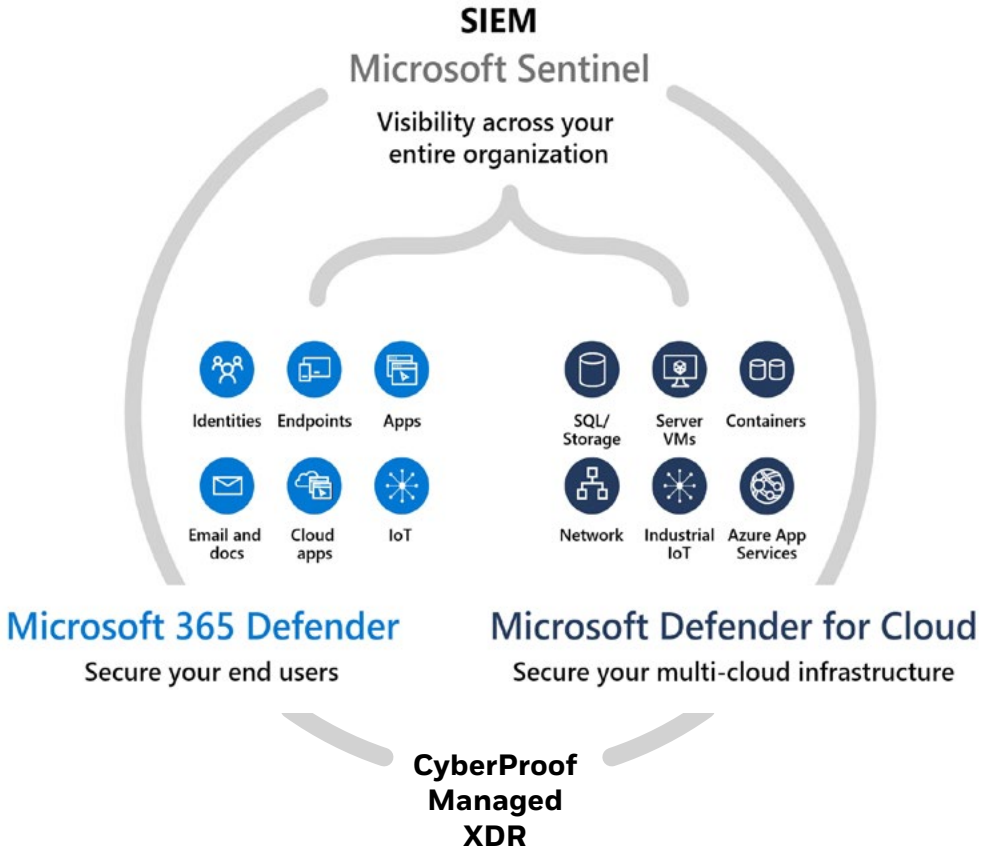
MITRE ATT&CK MATRIX

The MITRE ATT&CK Matrix is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. CyberProof uses the matrix to eliminate client-specific threat gaps throughout the service lifecycle.



The most secure cloud

CyberProof trusts Microsoft Azure to deliver the highest level of security in the cloud. Here's how Microsoft SIEM and XDR work together to fortify your enterprise.



MICROSOFT 365 DEFENDER

Protect identities, endpoints, apps, email, data, and cloud apps with XDR capabilities.

MICROSOFT SENTINEL

Get a bird's eye view across your entire enterprise with cloud-native security information and event management.

MICROSOFT DEFENDER FOR CLOUD

Protect multi-cloud and hybrid cloud workloads, secure servers, storage, databases, and containers, and focus on what matters most with prioritized alerts.

Protect your assets as you move to the cloud

Learn how CyberProof can augment your SOC with proprietary tools, deep expertise, and rapid threat detection and response services.

LEARN MORE →

CONTACT SALES →

CyberProof®
A UST Company

References:

1. Barker, Ian. Cybercriminals can penetrate 93 percent of company networks. Web. 2022.
2. Microsoft. SIEM Shift: How the Cloud is Transforming Security Operations. 2021.
3. Ponemon Institute. 2022 Global Study on Closing the IT Security Gaps Ponemon Institute Report. 2022.