Cloud Security

Protect your company, services, and products

In today's fluid, fast-evolving threat environment, companies face increasingly difficult challenges to adequately protect their assets while maintaining an accessible and transparent user experience. Our team can help identify gaps in your security architecture, reduce at-risk surface area, improve the accuracy of threat alerting, automate manually intensive security tasks, and reduce cost.

Urgent Priorities for Cloud Security

- Development of a cohesive end-to-end cybersecurity reference architecture — a holistic best-practices blueprint is essential to establishing flexible, adaptive governance
- Deployment of a best-in-class SIEM and SOAR solution such as Microsoft Sentinel — a complete automation solution capable of unifying point solutions and disjointed coverage
- Performing a cloud readiness cybersecurity assessment for on-prem systems workloads — ensuring all necessary prerequesites are in place before cloud migration

The Value

- Important insights into your current cybersecurity systems
- Improve your team's awareness of the newest tools and tech
- Plan your next-gen security strategy and how to deliver it

The Proof

- Our team has helped dozens of firms improve cybersecurity
- False positives can be reduced by 60-70% with Sentinel
- By 2023, 90% of SIEM solutions will have capabilities that are only delivered via the cloud

The Outcomes

- Critical workloads can be cloudmigrated safely and securely
- Cutting-edge monitoring and lerting automation frees up staff for faster threat response
- Reduced security costs

Take Action

Tactical Solutions: A structured two-hour creative problem solving workshop. Start with the problem that needs to be solved, not the end solution.

Governance Assessment: A three-day process to analyse your existing cybersecurity framework and map out the benefits of a SIEM/SOAR implementation.

Cloud Security Blueprint: Identify strengths and weaknesses in your existing security architecture and create an achievable, cloud-ready reference architecture.

Roadmap Your Future: Create an actionable transition plan to move forward in defined stages to remediate deficiencies, close gaps, and enhance existing threat detection.

Our Solution

Our cloud security experts will work with your infrastructure team to analyse your current state security framework. Most importantly, we'll work with your team to develop a standards-based security blueprint and compliance roadmap to ensure your cybersecurity and governance is cloud-ready.

Know Where to Start

What are my Cloud Security priorities?

First, create a cybersecurity reference architecture to provide a blueprint for securing and monitoring all critical workloads, whether on-prem or cloud. Second, fully utilise SIEM and SOAR technology for improved SecOps. Third, consolidate and eliminate legacy point solutions using more efficient, lower-cost cloud platform solutions.

What security solutions are my competitors implementing?

Security Information and Event Management (SIEM) technology is now widely deployed to provide threat detection, compliance, and security incident management. Larger firms are utilising Security Orchestration, Automation and Response (SOAR) technology to automate the management of high alert volumes.

What cloud security features do my business users need most?

Look for these features from your cloud provider: Advanced Perimeter Firewall, Active Directory Integration, Intrusion Detection Systems with Event Logging, Unmanaged Client Cybersecurity, Hybrid Cloud SecOps, and Encryption for Data-at-Rest.

My security architecture is too expensive

Monitoring and alert escalation are often the most expensive components of SecOps because they require a significant allocation of SecAdmin time. To reduce cost, look at newer SOAR technologies that can automate a substantial amount of this work.

We experience too many false positives

False positives are the bane of SecOps. But machine learning and AI can dramatically reduce false positives. These features are typically found in advanced SIEM solutions.

My security team is not currently working with Microsoft Azure

Few SecOps teams can cover all the bases in the fast-evolving world of Azure cybersecurity. That's why it's important to partner with a cybersecurity specialist that can help keep your team up to date and focused on the most important priorities.

The Business Problem

"I need a better, more defined approach to stay on top of fastevolving security challenges."

The Opportunities

Identify Cloud-Related Risks
Run an assessment of your current security architecture to identify gaps and exposures that need fixes.

Train Your Team
Update team skills with briefings on key Azure security components.

Develop Cloud Security Guidelines
Create a blueprint for implementing cybersecurity and identify best practices across your enterprise.

Train Your Tools
Configure machine learning and AI tools to improve alert pattern detection and reduce false positives.

Establish Good Governance
Prioritise governance objectives and create automated KPIs to help monitor security and compliance.

Partner With the Best
Design your security architecture with a strategic Microsoft partner

74%
of corporations use SIEM products to automate cybersecurity alerting

2-3 days
to perform an initial cybersecurity SIEM (Sentinel) implementation

43%
of all cyber attacks are aimed at small businesses