UNIT4

In business for people

Defining your cloud security strategy

The ultimate objectives for a security organization don’t change when you migrate to cloud. But how those objectives are achieved will change.

Modernizing your security strategy

How the cloud is changing security

Shifting to the cloud for security is more than a simple technology change, it’s a generational shift – akin to moving from mainframes to desktops and onto enterprise servers. Successfully navigating this change requires fundamental shifts in expectations and mindset by security teams.

While these could be part of any security modernization plan, the rapid pace of change in the cloud makes adopting them an urgent priority. Security teams must partner closely with business and IT teams to establish shared goals around productivity, reliability, and security and work collectively with those partners to achieve them.

Security teams must learn the business and IT objectives and why each is important and how they are thinking about achieving them as they transform and share why security is important in the context of those business goals and risks, what other teams can do to meet security goals, and how they should do it.

While the size and number of changes can initially seem daunting, the modernization of your security strategy allows you shed some of the burdens associated with legacy approaches as you consider the more dynamic approach required by cloud. More mature cloud platforms, like Microsoft Azure, are actually built with these considerations in mind.

5 reasons with Microsoft security solutions to protect your business:

- In 2020, Microsoft had **2.5 billion cloud-based detections** that blocked almost 6 billion threats
- More than **30 billion authentications** are processed across 425 million users through Azure Active Directory
- **30 billion email threats** were blocked by Microsoft 365 Defender in 2020
- Compliance solutions process more than **5 billion document classifications** each month
- Azure Sentinel analyzes over **4 petabytes of data** each month from Azure, Amazon Web Services, on-premises, and more

Microsoft real-time security stats

40M+
lines of data reviewed per day

85%
of cyberattacks detected after three months of learning feedback

Incorporates analyst feedback daily in order to adapt to threats in real time

5x
fewer false positives than machine-only systems

100-200
suspicious events flagged for human anaysis per day

Cyber crime continues to flourish

424%
increase in cyberattacks aimed at small businesses in 2020

43%
Business that question whether they can identify and report a breach within 72 hours

$149K
The average cost of a data breach for a small to medium sized company

Monitor and protect at cloud-scale

Security teams must take an agile approach to modernizing security, and rapidly modernize the most critical aspects of the strategy with a mindset of continuous improvement - especially as your cloud estate and exposure scales, and more devices than ever are connecting to your platforms.

Security of the cloud and from the cloud

As your organization adopts cloud services, security teams will work toward two main objectives:

- **Security of the cloud:** applying security principles to cloud assets to ensure they are properly protected across all endpoints and do not leave back-doors into other systems.
- **Security from the cloud:** applying security tools and approaches hosted in or facilitated by the cloud – which can allow your teams to achieve security postures infeasible with only on-prem infrastructure, like more rapid scaling of your security functions and greater visibility of individual assets.

The right level of security friction

Security naturally creates friction that slows down processes, it's critical to identifying which elements are healthy in your DevOps and IT processes and which are not.

Healthy friction is that which strengthens systems by forcing critical thinking at the right time and helps your teams to identify and remediate vulnerabilities (e.g. via threat modelling.)

Unhealthy friction impedes more value than it protects. This often happens when security bugs generated by tools have a high false positive rate or when the effort to discover or fix security issues far exceeds the risk and likely impact of an attack.

Standalone and integrated responsibilities

Security teams' jobs consist of both "pure" security functions (like vulnerability management and security ops), or security functions integrated into other functions (like app development and threat modelling.)

Performing these functions will require security teams to modernize their tools, technologies, and processes.

Managing expectations of transformation

Conflict and misaligned expectations can both derail critical projects and incentivize teams to bypass security risk mitigation – leading to **increased security risk** (particularly when teams get frustrated by security and bypass normal processes or when outdated security approaches are easily bypassed by attackers) and **reduced operational effectiveness** (often when security processes hold up key business initiatives).

Patience, empathy, and education will help your teams better navigate this period, driving good security outcomes for the organization.

Cybersecurity resilience

Many organizations have begun their cloud journeys because they have been managing the steady rise in volume and sophistication of attacks in recent years in the hopes of adopting a more resilient strategy. The functions of the **NIST cybersecurity framework** serve as a useful guide on how to balance investments between the complementary activities of identify, protect, detect, respond, and recover in a resilient strategy.

Adopting the shared responsibility model

Hosting IT services in the cloud splits the operational and security responsibilities for workloads between the cloud provider and the customer tenant, creating a de facto partnership with shared responsibilities. All security teams must study and understand this shared responsibility model to adapt their processes, tools, and skill sets to the new world. For our solutions, responsibility is split between Unit4, the Customer, and Microsoft Azure. Learn more about the details in **this video.**

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	□	□	□	□
Client & end-point protection	□	□	□	□
Identity & access management	□	□	□ ■	□ ▨ ■
Application level controls	□	□	□ ■	■ ▨
Network controls	□	□ ■	■	■ ▨
Host infrastructure	□	□ ■	■	■ ▨
Physical security	□	■	■	■

□ Cloud Customer ▨ Unit4 ■ Azure

Building security initiatives

This diagram illustrates the three primary security initiatives that most security programs should follow to adjust their security strategy and security program goals for the cloud, according to Microsoft:

Responsibility	SaaS	PaaS	IaaS	On-prem	
Information and data	■	■	■	■	Established a modern perimeter
Devices (Mobile and PC)	■	■	■	■	
Accounts and identities	■	■	■	■	
Identity and directory infrastructure	◥	◥	■	■	Established a modern perimeter
Applications	□	◥	■	■	
Network controls	□	◥	■	■	
Operating system	□	□	■	■	
Physical hosts	□	□	□	■	“Trust but verify” each cloud provider
Physical network	□	□	□	■	
Physical datacenter	□	□	□	■	

□ Microsoft ■ Customer

Building a resilient security posture in the cloud requires several parallel complementary approaches:

- **Trust but verify:** Evaluate the security practices of cloud providers and the security controls they offer to ensure they meet your needs.
- **Modernize infrastructure and application security:** Prioritize modernizing security tooling and associated skill sets to minimize coverage gaps for securing resources in the cloud.
- **Establish a modern perimeter:** of consistent, centrally managed identity controls to protect yout data, devices, and accounts.

Managing risk

Your move to the cloud isn't entirely without risk, and your strategy should include appropriate mitigations, including:

Business continuity and disaster recovery: Is the cloud provider financially healthy with a business model that's likely to survive and thrive during your organization's use of the service?

Security: Does your vendor partner follow industry best practices for security? Has this been validated by independent regulatory bodies?

Business competitor: Is the cloud provider a significant business competitor in your industry? Do you have sufficient protections in the cloud services contract or other means to protect your business against potentially hostile actions?

Multicloud: Many organizations have a de facto or intentional multicloud strategy. Regardless of the reason, this strategy can introduce potential risks and costs that have to be addressed and incorporated into your security approach.

Ready to learn more?

To discover more about how to prepare for your organization's journey to cloud visit **this page.**

For more information go to:

unit4.com

UNIT4
In business for people

UNIT4

In business for people