Microsoft Azure

Securing Your Migration

Contents

Introduction 03

Chapter 1
Securing your entire IT landscape 04

Chapter 2
Enabling innovation in the cloud with unified and comprehensive security 06

Chapter 3
Customer stories on cloud security 08

Conclusion
Azure runs on trust 14

Introduction

In today's landscape, cyberattacks seem inevitable—but the reality is less bleak than it appears. The Microsoft Digital Defense Report found that basic security hygiene protects against 99% of attacks.[1] As more organizations strategize how they'll use AI and cloud-native services to drive innovation, embracing those basic cloud security practices can help them address their top security concerns.

The race to innovate with AI and cloud technology comes with several challenges. Organizations face rising costs, changing regulations, IT sprawl, and expanding security threats. Without the right tools, these realities can easily decelerate plans for innovation and growth.

Organizations need comprehensive security solutions that use the cloud to increase scalability, reduce IT sprawl, maximize team skill sets, and optimize costs and resources to thrive in today's fast-paced market. Migrating to the cloud provides a secure platform for innovating with AI while simultaneously maximizing ROI and ensuring high performance for both first-party and third-party workloads.

This e-book outlines the strategies and tools you need to secure your IT infrastructure in the cloud as part of a responsible AI framework.

Fundamentals of cyber hygiene

Migrating to the cloud makes it easier to implement fundamental security standards. The following security standards help protect organizations against over 99% of attacks:[1]

- Multifactor authentication
- Zero Trust design principles
- Extended detection and response (XDR) and antimalware
- Updating firmware, OS, and applications
- Protecting data

[1]Microsoft Digital Defense Report, October 2023.

Chapter 1

Securing and managing your entire IT landscape to enable responsible AI

Organizations need a cohesive multicloud cybersecurity strategy

With around 87% of businesses embracing multicloud environments and 72% taking a hybrid approach, security and compliance teams are grappling with how to provide a proper security posture to protect their cloud platforms against increasingly sophisticated and frequent cyberattacks.

Security is a top cloud challenge for all organizations.

For enterprises and SMBs, security is the second most pressing challenge just after managing cloud spend.[2]

Organizations face several challenges in securing cloud workloads.

Some of the biggest challenges reported by organizations include a lack of skilled cybersecurity staff (43%), ensuring compliance (37%), and visibility into infrastructure security (32%).[3]

Misconfigurations are the leading cause of cloud-related security incidents.

Recently, 24% of organizations experienced a public cloud-related incident, with the leading causes being misconfiguration, followed by account compromise and exploited vulnerabilities.[3]

Despite these ongoing challenges, the cloud holds immense value for companies looking to sharpen their competitive edge through innovation strategies. First, they must establish a simple, secure, and well-managed IT infrastructure that protects against growing threats without requiring extensive IT expertise or multitudes of additional resources.

[2] Flexera 2023 State of the Cloud Report, Flexera, 2023.

[3] 2023 Cloud Security Report, Cybersecurity Insiders, 2023.

Three critical components of a secure IT landscape

1. Threat intelligence

Reduce the time and effort required to prevent and resolve attacks.

Threat intelligence involves gathering and analyzing data about potential cyber threats so businesses can defend against them. It shifts security teams from a reactive stance to a more proactive one by providing data-driven security insights. These insights help shed light on unknown threats, allowing teams to understand the attackers' motives better and anticipate tactics, techniques, and procedures (TTPs) behind attacks.

For resource-strapped businesses, threat intelligence offers a level of security that might otherwise be unattainable. Meanwhile, enterprises incorporate external threat intelligence to help optimize costs and enhance the effectiveness of their security teams.

2. Simplified compliance

Keep infrastructure compliant with daily regulatory updates.

Regulatory compliance is a frequently cited challenge for many organizations. As technology advances, more rules and standards regulate how that technology—and the data involved—can be used. Given the increasingly complex regulatory landscape, simplifying compliance is crucial for businesses looking to bolster security in their multicloud and hybrid environments.

Several factors help simplify compliance, including centralized control, data risk visibility, and automated response orchestration. Additionally, daily regulatory updates help businesses keep track of the most recent rules and regulations that impact their jurisdiction. With these factors in place, organizations can better comply with regulations as they innovate with the latest technologies.

3. Tool consolidation

Secure cloud environments and platforms with an integrated set of tools.

When it comes to security and management tools, more isn't necessarily better. IT sprawl is common for security solutions, with IT environments consisting of different server and data setups across locations. For several reasons, reducing the variety of security tools and systems used to safeguard an IT landscape is crucial for enhancing security. Minimizing complexity improves the integration and communication between different security tools, enhancing visibility, detection, and response capabilities. It also helps eliminate overlapping and redundant security functions, leading to more sustainable and scalable operations.

Chapter 2

Enabling innovation in the cloud with unified and comprehensive security

Migrating to Azure provides organizations with an optimized platform for taking advantage of the latest technologies. By providing comprehensive code-to-cloud security, Azure helps businesses use AI and cloud-native tools in a secure environment, allowing teams to focus on driving innovation instead of mitigating risks.

Migrating your SQL and Windows Servers to Azure gives you access to unified, comprehensive security for your cloud stack. Explore the solutions below to see how each contributes to a secure, AI-ready foundation in the cloud.

Solution: Microsoft Defender for Cloud

Purpose: Help protect multicloud and hybrid environments with comprehensive security across the full app lifecycle, from code to cloud.

Plans and capabilities:

- **Cloud Security Posture Management:** Gain full visibility, contextual insights, and built-in workflows to remediate the most critical risks across clouds with Defender CSPM.
- **Server security:** Get comprehensive server protection for on-premises and multi-cloud servers (Azure, AWS, and GCP) with agent and agentless scanning.
- **Storage security:** Help protect Azure Blob Storage, Azure Files, and Azure Data Lake Storage from threats like malware with near-real time detections and response.
- **Container security:** Secure your container estate with industry-leading threat detection and response powered by Defender for Cloud and Defender XDR integration.
- **API security:** Strengthen security posture and protect APIs with full visibility, OWASP API Top 10 mapping, and risk mitigation for Azure API Management APIs and unmanaged APIs in Azure App Services.
- **AI security:** Proactively improve your AI security posture and protect AI applications from threats such as jailbreak attacks, credential theft, and wallet abuse.
- **Scenario:** ElringKlinger's small security team protects around 9,000 employees with a productivity-first umbrella that connects every aspect of cybersecurity, lowering security incidents overall and speeding response time.
  Learn more >

Comprehensive security across environments

Together, these tools provide multilayered environmental protection so you can adopt new technologies while protecting your most valuable digital assets.

- Detect and respond to threats with integrated threat protection
  - 30% reduction in time to remediate threats with Defender for Cloud[4]
- Keep your infrastructure compliant
  - 15% reduction in audit compliance overhead and lower reliance on auditing services
- Consolidate your tools for simplified management and cost savings
  - 10% percent license savings compared to legacy security infrastructure tools[3]

Securing hybrid environments

Not all infrastructure can be migrated to the cloud. Sometimes, regulations require that certain assets remain on-premises or within a certain geographic location, forcing companies to adopt a hybrid approach. Unfortunately, using both the cloud and on-premises servers creates complexity regarding control and governance. That's where Azure Arc comes in.

Azure Arc extends the Azure platform—and its security capabilities—to multicloud and on-premises environments. This creates a unified platform for managing and securing resources, whether in the cloud, in data centers, or on the edge. It offers built-in security and compliance for Azure Arc-enabled services, including Azure Kubernetes Service (AKS), app services, data services, and machine learning.

[4]The Total Economic Impact™ Of Microsoft Defender For Cloud, a commissioned study conducted by Forrester Consulting on behalf of Microsoft, January 2025

Chapter 3

Customer stories on cloud security

Discover how organizations are securing their cloud migrations and enabling AI innovation.

WTW consolidates security tools for elevated protection

Insurance

The company

Customers turn to WTW for actuarial and risk mitigation strategies that help them build resilience and make smarter decisions in a world of uncertainty. To help its clients achieve those goals, WTW relies on huge volumes of data and highly skilled analysts applying advanced data science techniques and contextual judgment to reveal opportunities.

Company details

120
countries of operation

55,000
workstation devices

300+
subscriptions

The challenge

Since its formation in 2016, WTW steadily built up a body of unconnected legacy solutions that were causing several security issues, including:

- Inflated licensing costs for multiple tools.
- Security data duplicated across solutions.
- Loss of agility as teams were pulled in different directions trying to manage varied technologies.

The goal

The company's vision for a more secure future involved several key goals:

- Consolidate its tools to streamline its security posture.
- Establish an agile, threat-led security team.
- Enhance visibility into its IT estate.

WTW

Solutions and outcomes

Microsoft Defender for Cloud

Deploying Microsoft Defender for Cloud provided greater protection for its cloud workloads and extended its detection and response (XDR) capability.

Microsoft Sentinel

Converting from a legacy SIEM system to Microsoft Sentinel allowed the team to aggregate threat data from Azure and its Oracle cloud.

Microsoft Purview

Rolling out Purview helped prioritize its data loss prevention (DLP) and information governance tools.

Outcomes in numbers

55,000
endpoints enabled with full-scale XDR capability

12 TB
less data going into the SIEM

$5–6M
USD saved in a year

[Read the full story](#) >

We need full visibility into our IT estate, especially as we embrace Zero Trust. The consistency in the Microsoft tooling delivers that visibility across endpoints, identities, and multicloud."

Paul Haywood, Chief Information Security Officer, WTW

World Bank centralizes security solutions in the cloud

Banking and capital markets

The company

The World Bank works tirelessly to end extreme poverty and boost prosperity on a livable planet by providing access to basic financial services. The organization offers lending services in developing countries worldwide in support of this mission.

Company details

189
developing countries served

170+
countries with employed workers

130+
operating locations

The challenge

The World Bank IT team was using multiple cloud providers and tools to manage the complex backend of the global institution. The security office used different software to monitor the risk security of all the company's servers, making it difficult to assess the database environment and get insights on their migration readiness.

- Decentralized tools couldn't monitor the entire SQL infrastructure (on-premises and cloud)
- Difficulty managing inventory of data workloads
- Inefficient maintenance processes for tasks like backups and patches

The goal

World Bank's IT and Information Security Office teams wanted a cloud-based solution to centralize monitoring, performance, resource consumption, and security management in a single package. The company's goals included:

- Deprecate duplicate licenses.
- Reduce operating costs.
- Centralize data storage.

World Bank

Solutions and outcomes

Compatibility played a big part in the World Bank's decision to partner with Azure. The company wanted a solution that could be used to manage both Azure and AWS servers and work with its Microsoft SQL Server stack.

Azure Arc

Implementing Azure Arc allowed the company to manage both clouds from a single dashboard and streamline its cloud migration journey.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides the company with comprehensive hybrid and multicloud security to help protect sensitive financial data.

Azure Monitor

The team uses Azure Monitor to gauge performance trends and identify potential anomalies.

Outcomes in numbers

300

SQL Servers enabled with Azure Arc (10 times more than the previously licensed tools could cover)

90%

cost savings by removing previously licensed tools

[Read the full story](#) >

"With Azure Arc, we can manage everything at the operating level and on the SQL Server side, all from a single pane of glass."

Chandra Kala Macha, Information Officer II, World Bank

Tecnicas Reunidas improves security across its expanding footprint

Energy

The company

A global engineering and energy leader, Tecnicas Reunidas is focused on carbon capture and storage, the circular economy, and hydrogen.

Company details

1000+
industrial plants managed

50+
countries with operations

900
on-premises and cloud servers

The challenge

With an extensive global footprint and complex operational, regulatory, and digital requirements, the company's growth began presenting several challenges. Over time, the IT team faced several limitations in managing security across its estates:

- Multiple security tools driving up costs
- Increasing IT complexity
- Growing number of threats adding pressure to manual processes

Tecnicas Reunidas launched an ongoing migration of some of its on-premises facilities and capabilities to Azure to overcome these challenges.

The goal

The IT team wanted to consolidate its on-premises and expand cloud environments so they could concentrate more on governance, rather than spending their time managing different services and tools.

- Establish centralized management for on-premises and cloud environments
- Integrate automation to reduce manual work
- Enhance visibility of the entire data IT infrastructure

Tecnicas Reunidas

Solutions and outcomes

Tecnicas Reunidas unified its growing hybrid environment to help establish optimal control over its security operations. The IT team primarily runs Windows Server in its environments and manages the entirety with Azure Arc, which it relies on to help handle security, governance, and compliance for its IT infrastructure.

Azure Arc

Using Azure Arc allowed the company to consolidate nearly 900 on-premises and cloud servers and automate many of the manual tasks associated with security.

Microsoft Defender for Cloud

The company uses Defender for Cloud to protect workloads running on-premises and in Azure.

Microsoft Sentinel

With Microsoft Sentinel, the team could aggregate data from across on-premises and Azure sources and use built-in AI for advanced threat protection.

Outcomes in numbers

~900

on-premises and cloud servers connected to Azure Arc

- Enhanced security capabilities, including management, security suite tools, compliance review, agent deployment, and security updates
- Teams can easily access company data for use in AI models

[Read the full story](#) >

Our work approach has changed with Azure. Now, we're putting more emphasis on governance instead of just loading up on services and tools. With Azure Arc, we can use automation to do less manual work and improve our security simultaneously."

Israel Pérez Jiménez, IT System and Cloud Architect, Tecnicas Reunidas

Conclusion

Azure runs on trust

Migrating your Windows Server and SQL Server to Azure provides the security, agility, and speed your organization needs to drive innovation with AI-powered and cloud-native tools. With best-in-class security solutions that are purpose-built for your entire IT estate, Azure helps your teams innovate freely in the cloud so you can drive business objectives further and faster. Plus, with Azure Arc, you can consolidate and manage your tools from a single dashboard, saving precious hours and costs that can be refocused on bringing groundbreaking ideas to life.

Migrate to innovate with built-in security from code to runtime

Azure provides unmatched speed, security, and cost savings compared to other cloud providers.

- Run up to 5x faster than AWS[5]
- Reduce costs by as much as 93% with Azure Hybrid Benefit[5]
- The most compliance certifications of any cloud provider

Azure relies on Microsoft Threat Intelligence to protect and defend a never-ending surge of security threats:[6]

- 84 trillion signals synthesized daily
- 30,000+ security and threat intelligence experts across the globe
- 600+ million daily identity attacks identified
- 1,500+ unique threat groups tracked

[5]Three Microsoft Azure SQL Managed Instance offered better SQL Server performance and value than their Amazon RDS counterparts in our tests, Principled Technologies, May 2022

[6]Microsoft Threat Intelligence

Take the next step to a secure migration

Assess your environment and build a migration business case with **Azure Migrate and Modernize**.

Contact Sales >