span security

AZURE SECURITY HARDENING

Enhance the security of your cloud environment to make it less vulnerable to cyber attacks

Security benchmarks and standards are comprehensive and complex. It can be challenging and an exhaustive exercise for organizations to map respective security controls to their cloud deployments through appropriate configuration settings and security services.

66%
organizations leave back doors open to attackers through misconfigured cloud services

630%
increase in cloud-based attacks between January and April 2020 alone

51%
of organizations marked failure in properly setting their cloud services configuration as a reason for data loss

With our security hardening services based on Azure Security Benchmark, we provide effortless adjustment of cloud security settings for customers with Azure IaaS, PaaS or SaaS deployments.

Azure Security Benchmark is focused on various control areas, consistent with well-known CIS and NIST security frameworks (Center for Internet Security Controls Version 7.1, National Institute of Standards and Technology SP 800-53).

Span experts will take care of the multi-layered protection for your Cloud deployment to various attack vectors.

Get all required security controls properly implemented for your Azure environment:

Network Security

Establish controls to **secure and protect Azure networks**, including securing virtual networks, establishing private connections, preventing and mitigating external attacks, and securing DNS.

Identity Management

Establish a secure identity and access controls using Azure Active Directory, including the use of **single sign-on, strong authentications, managed identities** (and service principals) for applications, conditional access, and account anomalies monitoring.

Privileged Access

Establish controls to protect **privileged access** to your Azure tenant and resources, including a range of controls to protect your administrative model, administrative accounts, and privileged access workstations against deliberate and inadvertent risk.

Data Protection

Establish controls of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, and logging in Azure.

Asset Management

Establish controls to ensure **security visibility and governance** over Azure resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for services and resources (inventory, track, and correct).

Logging & Threat Detection

Establish controls for detecting threats on Azure and **enabling, collecting, and storing audit logs** for Azure services, including enabling detection, investigation, and remediation processes with controls to generate high-quality alerts with native threat detection in Azure services; it also includes collecting logs with Azure Monitor, centralizing security analysis with Azure Sentinel, time synchronization, and log retention.

Incident Response

Establish controls in **incident response life cycle** - preparation, detection and analysis, containment, and post-incident activities, including using Azure services such as Azure Security Center and Sentinel to automate the incident response process.

Posture & Vulnerability Management

Establish controls for **assessing and improving Azure security** posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting, and correction in Azure resources.

Endpoint Security

Establish controls in **endpoint detection and response**, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Backup & Recovery

Establish controls to ensure that **data and configuration backups** at different service tiers are performed, validated, and protected.

BENEFITS

ZERO-TOUCH IMPLEMENTATION

Rely on Span expertise, experience and proven track record of successful cloud security implementations to quickly and efficiently increase resilience for your cloud services, too.

REDUCED RISK

We apply multi-layered protection to decrease the surface attack area that can be exploited, consistent with well-known security frameworks.

COMPLIANCE READINESS

We take care to implement controls for your Azure environment that will satisfy your regulatory requirements.

WHY SPAN?

Span has been present on the market for more than 25 years, achieving excellence in a wide variety of technologies and solutions. IT Security Solutions is one of our strategic businesses, in which we continuously invest to be able to provide our customers with leading edge defense solutions, ranging from security assessment and proactive protection to security incident detection and response.

Contact us at:

info@span.eu

span