Microsoft

Security in Azure

Combine native Azure features with Managed Security Services to secure your cloud environment today!

Through 2020, 95% of cloud security failures will be the customer's fault

Gartner

Source: Gartner Revels Top Predictions for IT Organizations and Users for 2016 and Beyond, October 2015

Insecure misconfiguration & lack of controls #1 cause to cloud based data centers breaches

Forbes

"Through 2020, **80%** of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities"

"A historic **424%** jump in breaches related to misconfigured cloud infrastructure, largely due to human error."

Source: https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-one-cloud-security-metric-every-ciso-should-know/#3ff8c87e5375 , Author: Josh Stella, Forbes council

Cloud security is a shared responsibility

Shared responsibility model for cloud security

Microsoft's commitment

Secure foundation

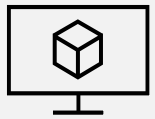
Physical assets

Datacenter operations

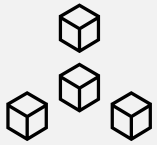
Cloud infrastructure and fabric

Joint responsibility

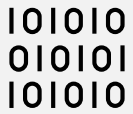
Microsoft provides built-in controls



Virtual machines and networks



Apps and workloads



Data

Nova Quantum

How does your company understand the quality of their security posture against security controls that are possible to configure within Azure?

Azure Security Center Secure Score

- Secure Score measures what you have done to secure your environment compared to what you can do
- Your secure score will change depending on what resources are deployed in a subscription
- Two organizations can only have the same secure score if they have the same resources deployed with the same security configuration
- Secure Score will change as new security configuration options become available over time

Nova Quantum

Comprehensive security for hybrid environments

with built-in Azure services

 Identity & access management	 App and Data protection	 Network security	 Threat protection	 Security management
Azure Active Directory	Encryption (Disks, Storage, SQL)	VNET, VPN, NSG	Azure Security Center	
Multi-Factor Authentication	Azure Key Vault	Application Gateway (WAF), Azure Firewall	Azure Sentinel	
Role Based Access Control	Confidential Computing	DDoS Protection Standard	Microsoft Antimalware for Azure	Azure Log Analytics
Azure Active Directory (Identity Protection)		ExpressRoute		

A lot of data available for manual remediation: we can managed it for you!

Nova Quantum

How does your company understand and resolve its most urgent cloud security issues?

Resource Security Hygiene

Compute and Apps:

VMs and Computers, VM Scale Sets, Cloud Services, App Services, Containers, Compute resources

Networking:

Network map, Adaptive Network Hardening, Virtual Networks

IoT Hubs & Resources

IoT resources

Data & storage

SQL, Storage accounts, Data Lake Analytics, Data Lake Store

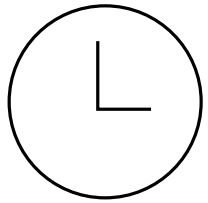
Identity & access

Account security, key vaults

Nova Quantum

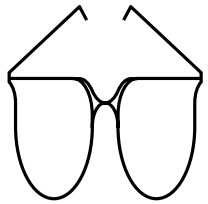
How does your company ensure that administrative tasks are only performed by authorized users?

Privileged Identity Management

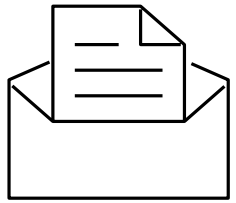


Privileged role membership only granted for a limited amount of time

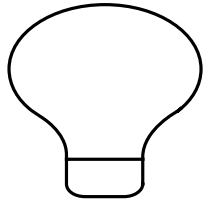
Roles can be configured to require staff to perform MFA prior to elevation of privilege



Roles can be granted automatically or after review by one or more approvers



All role requests for and role approvals are automatically recorded in logs or by email



Almost all roles should be managed by PIM, with a “break glass” permanent account for critical roles just in case

Nova Quantum

How can your company ensure that only certain IaaS VMs can access a specific storage account?

Locking Down Service Endpoints

- Virtual network service endpoints enable you to limit network access to some Azure service resources to a virtual network subnet
  - (Storage / KeyVault / Service Bus / etc)
- Can also remove internet access to the resources

Nova Quantum

How can your company improve the security of Azure SQL instances?

Azure SQL Server Advanced Threat Protection

- Vulnerability to SQL Injection
- Potential SQL injection
- Access from unusual location
- Access from unusual data center
- Access from unfamiliar principal
- Access from potentially harmful application
- Brute force SQL Credentials

Nova Quantum

How does your company understand the quality of their security posture against industry recognized security standards?

Security and Compliance

Many organizations security needs are driven by compliance requirements. Azure Security Center can measures compliance against the following:

Standard	Author	Description
Azure CIS 1.1.0	Center for Internet Security	Set of security controls published by the Center for Internet Security
PCI DSS 3.2.1	Payment Card Industry Standards Council	Standards required for organizations that manage payment card data
ISO 27001	International Standards Organization	Set of security controls for information security systems. Standard 27017 is cloud computing specific.
NIST 800-53	National Institute of Standards and Technology	Security and Privacy Controls for Federal Information Systems and Organizations.

By default, most of the environments are NOT compliant with any security standards!

Nova Quantum

Our Proposal: let us manage your Azure security!

While the auditing of your environment using previously mentioned standards is easy to enable on your own (albeit not for all controls), the actual **remediation** tasks of the non-compliant resources is time consuming and complicated.

We provide managed Azure Security services:

- Perform an initial assessment of the existing infrastructure and identify the critical components
- Enable auditing of the environment against one(or more) of the following regulatory standards: Azure CIS 1.1.0, NIST 800-53, PCI DSS 3.2, ISO 27001, and SOC TSP.
- Provide continuous monitoring and **remediation** *(certain exclusions apply)* of policy violations
- Provide monthly/weekly reports of the compliance status
- Provide advanced alerting *(integration with ServiceNow)* for policy violations
- Create best-of-breed, enterprise-level-tested, alerts for all the essential Azure services used in a particular environment
- Create custom operational dashboards for monitoring critical Azure components

Nova Quantum