Microsoft Cloud Security

A complete solution for protecting M365 and Azure environments.

A comprehensive solution for securing Microsoft 365 and Azure environments.

The Microsoft Cloud Security package developed by Moresi.com - Microsoft Solutions Partner - meets the renewed security needs of organizations in a scenario of hybrid and remote working and in a context where attack techniques have rapidly evolved, and new criminals have a greater ability and maturity to identify critical targets and strike at companies' business.

Moresi.com supports organizations in their security journey for Microsoft 365 and Microsoft Azure with a strategic coaching approach, enabling an assessment of the solutions required based on actual needs. The goal is to build tailor-made solutions with a view to constant and fruitful collaboration.

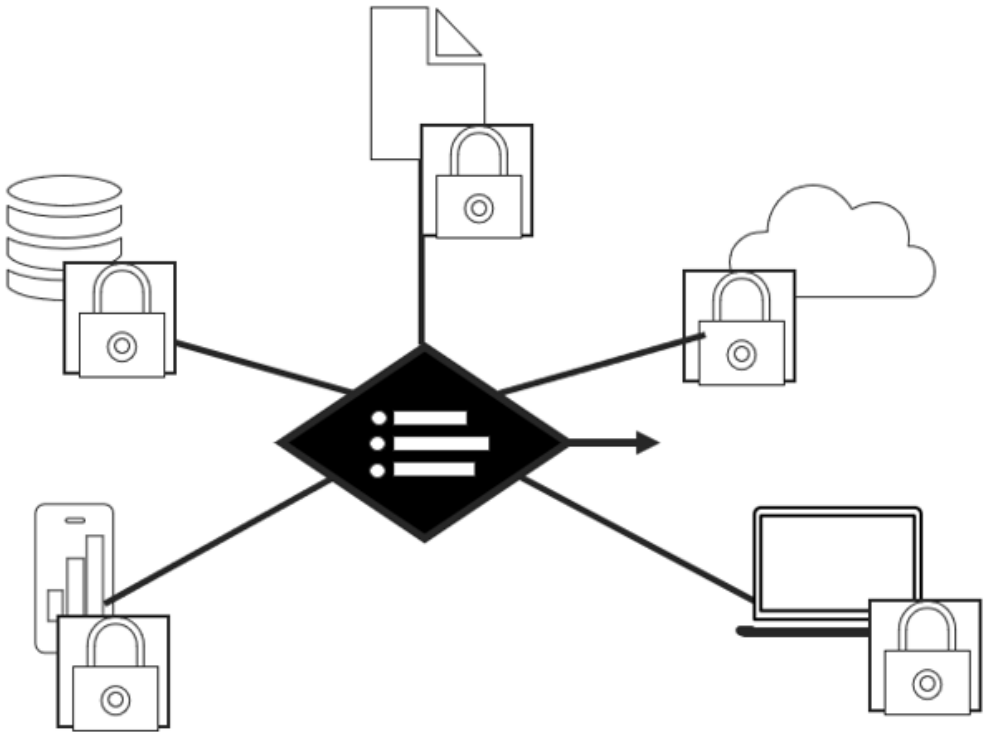
The Zero Trust Security Model

The proliferation of data and devices, the growth of hybrid work and increasingly sophisticated attacks reduce the effectiveness of perimeter-based IT security.

IT professionals manage a huge variety of technologies. Companies typically use a mix of cloud and on-premise infrastructure, platforms and software. They may have multiple vendors and cloud systems. Employees work on personal devices and can easily access cloud applications and services. Data are in more places than ever before, making them more valuable and vulnerable.

For these reasons, the Security solution proposed by Moresi.com focuses on three main aspects:

- Identity protection
- Device protection
- Infrastructure protection



Protecting identities

Cloud applications and the growth of hybrid work have redefined the security perimeter. Enterprise applications and data are also moving from on-premises to hybrid and cloud environments. However, many organisations rely on old-fashioned identity and access management systems built for a world with a clear line between what is inside and what is outside the network.

These systems make accessing the applications and data they need difficult and create security gaps by granting excessive privileges to trusted users. A Zero Trust framework, which incorporates cloud-based identity solutions such as multi-factor authentication and single sign-on (SSO) throughout the environment, is better suited to the modern workplace.

Protecting devices

The modern company has an incredible variety of endpoints accessing data. Still, not all endpoints are managed or even owned by the organisation, resulting in different device configurations and software patch levels.

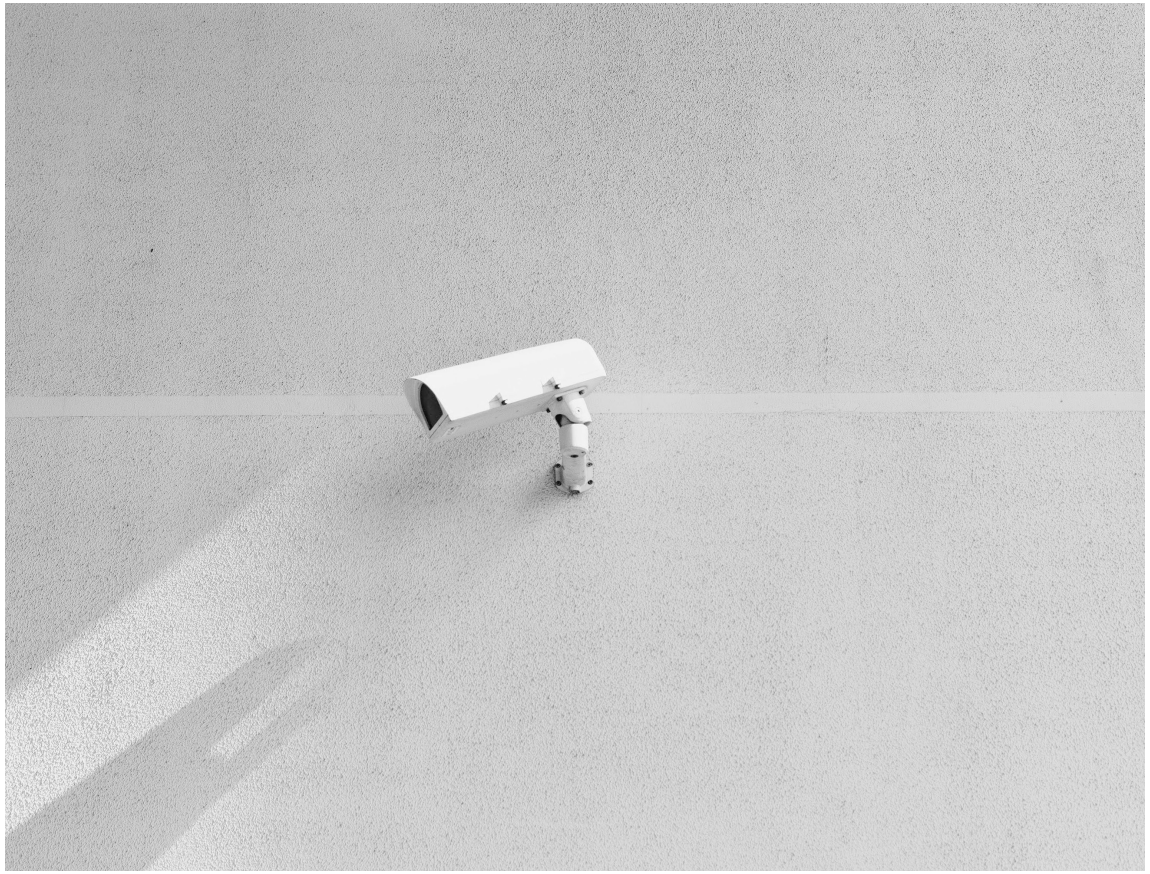
This creates a huge attack surface. An end-to-end Zero Trust framework can help you improve endpoint security to enable more secure hybrid working and leverage device-dependent strategies such as IoT and edge computing.

Protecting the infrastructure

Many organisations struggle to secure this environment because they manually manage permissions between environments and do not have effective configuration management of virtual machines and servers. Implementing an end-to-end Zero Trust framework makes it easier to:

- Ensure software and services are up-to-date.
- Manage configurations.
- Prevent, detect and mitigate attacks.
- Identify and block risky behaviour.

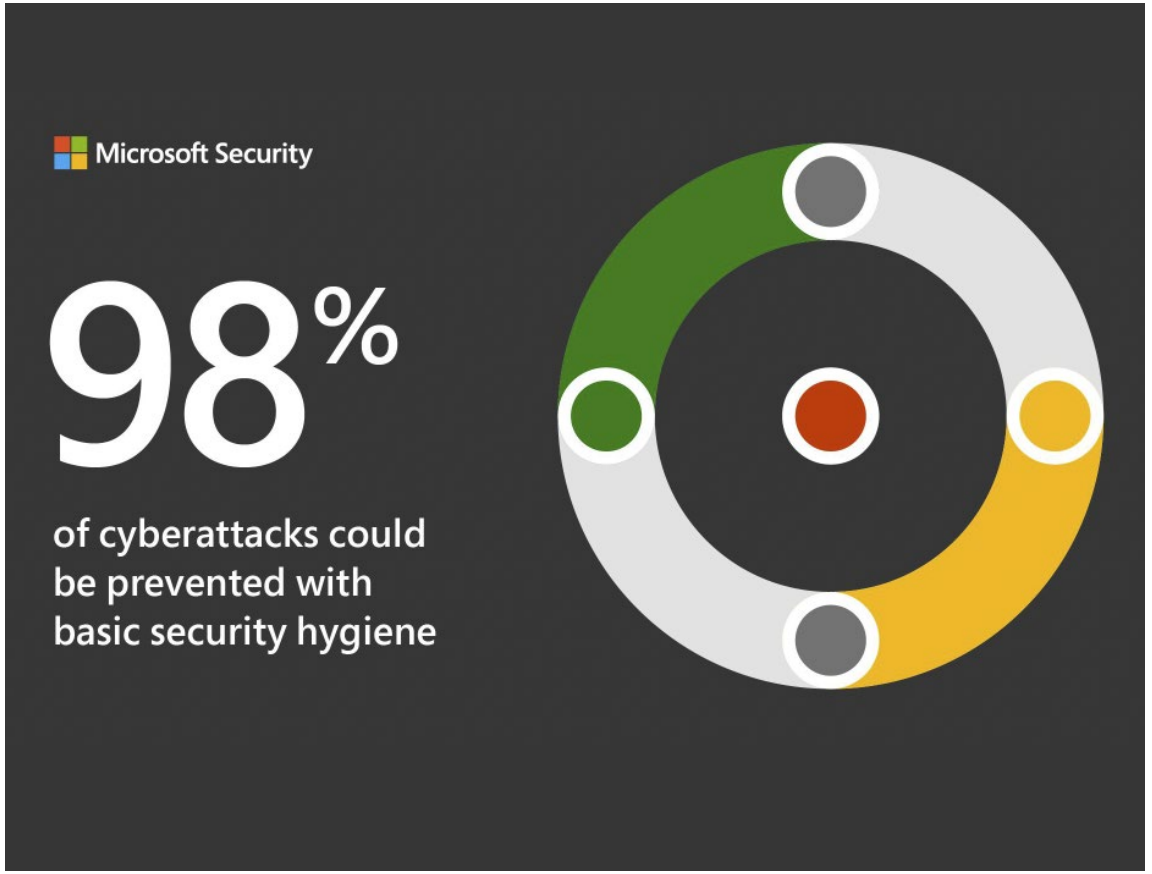
As networks are subject to continuous and increasingly sophisticated attacks, it is particularly important to protect the network infrastructure with security solutions that intelligently recognise known and unknown threats and adapt to prevent them in real-time.



Customisation of default security settings

The default security settings of Microsoft 365 and Azure tenants are designed to fit most small to medium-sized organisations. However, like any cloud service, the default settings do not always fit everyone's needs. Therefore, reviewing them to conform to business and organisational requirements and evaluating them regularly is always advisable.

With Moresi.com's solution, you can improve your Tenant's default security configurations by implementing some basic security hygiene practices. Indeed, good security hygiene can protect your systems from 98% of cyber attacks.



Security Workshop

WORKSHOP	CAN DO	HAVE DONE	CUSTOMERS
Defend Against Threats with SIEM Plus XDR	Yes	Yes	Datamars
Mitigate Compliance and Privacy Risks	No		
Protect and Govern Sensitive Data	Yes		
Secure Identities and Access	Yes	Yes	Mikron, Migros, Sintetica, Bally
Secure Multi-Cloud Environments	Yes		

SECURITY SERVICES	BASIC	SILVER	GOLD	PLATINUM
Basic security hygene	•	•	•	•
Privileged users management	•	•	•	•
Logging Configuration	•	•	•	•
Break glass accounts configuration	•	•	•	•
Hardening of the Azure AD, Exchange and Teams default settings		•	•	•
Conditional Access Policies		•	•	•
Defender for Office 365		•	•	•
Intune client security baselines & Compliance policies		•	•	•
Defender for Endpoint configuration		•	•	•
Azure AD Password Protection		•	•	•
Passwordless Authentication			•	•
Azure AD Privileged Identity Management			•	•
Azure AD Identity Protection			•	•
Enterprise Application Analysis			•	•
Access Reviews for privileged roles			•	•
Access to cloud resources from compliant devices only			•	•
Azure Information protection Labelling			•	•
Cloud App Security			•	•
Connection of services to Sentinel				•
Customer Lockbox				•
Insider risk management				•
Azure AD Entitlement Management				•
Data Loss Prevention (DLP)				•
Data Retention Policies				•
Server Protection with Defender for Cloud				•
Update management for Servers				•