SECURE ENVIRONMENT ROADMAP

Hackers are always finding new ways to attack organizations. The path to secure your business data can frequently be unclear and never ending. In today's environment, it is imperative to understand what security measures you are currently taking to prevent attacks on your systems and to know what you should be doing to decrease your vulnerability. With so many different options being flooded in the market, it can be hard to know what products can help you with what.

Interlink Cloud Advisors solicited input from their clients on what security tools they had deployed and in what order. From that data, we developed a summary of the layered security offerings that are available to you from Microsoft. From basic security to advanced protection, you can now understand the layers necessary to ensure that your environment stays safe. We encourage our clients to always be adding new levels of protection to keep ahead of threats.

interlink®
CLOUD ADVISORS

Updated 8.22.23

Basics 101

1 in 3000 emails that pass through contain malware[1]

Endpoint Protection	Defender for Endpoint Plan 1
Up-to-Date Firewall with Monitoring	Windows Defender Firewall (managed by Intune)
Password Policies	AD Enforced, Azure AD Password Protection / Entra Password Protection
Automated Patching	Intune
Deep Email Scanning/Safe Link Rewrite	Defender for Office 365 Plan 1
Deprovisioning of Terminated Users	Policies, Automatic Deprovisioning with Azure AD SSO
Device Management	Intune
Multi-Factor Authentication for Cloud & Remote Access	Azure AD Premium Plan 1 / Entra ID Plan 1
End User Security Awareness Training	Threat Simulator (Defender for Office 365 Plan 2)
Mandatory Device Encryption	Bit Locker (Windows Enterprise + Intune)

Basics 201

80% of security incidents can be traced to a few missing elements that can be addressed through modern security approaches[2]

Enterprise Single Sign on for all Applications	Azure AD Premium Plan 1 / Entra ID Plan 1
Outbound Email Encryption	Microsoft 365 Message Encryption
Cloud Data Loss Prevention Scanning	Purview Data Loss Prevention
Endpoint Detection and Response (EDR)	Defender for Endpoint Plan 2 / Defender for Business
Shadow IT Detection	Defender for Cloud Apps
MFA for End User Logons	Windows Hello for Business
MFA for On-Premise Admin Accounts	Certificate Services / SmartCards

Intermediate 301

95% of all cyber security breaches are caused by human error[3]

Endpoint Data Loss Protection	E5 Compliance / Microsoft 365 E5
Regular Elevated Permissions Auditing	Azure AD Premium Plan 2 / Entra ID Plan 2
Risk Based Conditional Access	Azure AD Premium Plan 2 / Entra ID Plan 2
Intrusion Detection Inside the Network with Monitoring	Defender for Identity
Incident Response Procedures	Defender Threat Intelligence
Automated Data Classification and Sensitivity Labels	Purview Information Protection
Protect and Govern 3rd Party SaaS Applications	Defender for Cloud Apps
Application Control	AppLocker & Windows Defender Application Control
Access Management for Admin Accounts	Privileged Identity Management (PIM)
Security Information and Event Management (SIEM)	Sentinel
Security Orchestration, Automation and Response (SOAR)	Sentinel
Managed Detection and Response (SOC)	Red Canary
Vulnerability Management and Attack Surface Reduction	Defender for Endpoint Plan 2 / Defender for Business

Advanced 401

The volume of password attacks has risen to an estimated 921 attacks per second[4]

Threat Activity Monitoring & Alerting	Defender Threat Intelligence
Server Protection & JIT Server Admin	Defender for Cloud
Cloud Activity Monitoring & Alerting	Defender for Cloud
Protection for Storage, SQL Instances & Containers	Defender for Cloud
Define, Detect & Act on Insider Risk	Purview Insider Risk Management
Automated Access Reviews for Administration & Sensitive Data	Azure AD Premium Plan 2 / Entra ID Plan 2
Administrator Access Management	Privileged Access Management (PAM)
PII & Privacy Management	Priva

[1] https://safeatlast.co/blog/ransomware-statistics/

[2] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-state-of-cybercrime#viewactionableinsights1

[4] https://www.privacysharks.com/cybersecurity-statistics/

[3] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bcRe?culture=en-us&country=us