Common attacks and Microsoft capabilities that protect your organization

Enter

Begin attack

Phishing Attacker targets

employees by email or other unsafe links or websites.

Spear-phishing

Attacker uses information specifically about a user to construct a more plausible phishing attack.

Brute-force attack —

Attacker tries a large list of possible passwords for a given account or set of accounts.

Other similar attacks: Watering hole attacks, leaked passwords.

Devices compromise

Malware is installed on the device. This can include viruses, spyware, ransomware, and other unwanted software that installs without consent.

Lost or stolen device -

Any employee clicks on a link and enters their credentials.

Exchange Online Protection blocks malicious hyperlinks in a message.

Office 365 Advanced Threat Protection protects against links in mail and files that are redirected to unsafe sites. Protection continues dynamically after mail is delivered.

Windows Defender SmartScreen checks sites against a dynamic list of reported phishing sites and warns users.

Weak passwords are systematically identified.

Azure AD password protections enforce minimum requirements for passwords, dynamically ban commonly used passwords, and force reset of leaked passwords.

Azure AD Smart Account Lockout temporarily locks out accounts with high-risk login activity.

For on-premises networks, Advanced Threat Analytics detects brute-force activity targeted to the domain.

Malicious files and viruses are introduced into the environment.

Exchange Online Protection scans for and blocks known malware and viruses.

Office 365 Advanced Threat Protection tests incoming files for unknown malware and viruses before they are delivered.

Windows and Office updates protect against new threats to this software.

Windows Defender Application Guard for Microsoft Edge protects against advanced attacks coming from the Internet.

Windows 10 Device Guard only allows trusted applications (defined by you) to run.

Possession is unknown.

Intune device configuration policy enforces password and/or pin requirements and wipes the device after a specified number of failed login attempts.

Traverse

Attacker uses stolen credentials to gain access to the user's mail and files.

Multi-factor authentication prevents password-only access to cloud services, including Exchange Online mailboxes and OneDrive for Business files.

Azure AD conditional access rules block access from unmanaged PCs.

Azure AD Smart Account Lockout temporarily locks out accounts with high-risk login activity.

Risk-based conditional access protect apps and critical data in real time using machine learning and the Microsoft Intelligent Security Graph to block access when risk is detected.

Any employee clicks on a malicious link or opens a malicious file.

Windows Defender Antivirus scans for malware, viruses, and security threats.

Windows Defender SmartScreen checks to see if new apps lack reputation or are known to be malicious, and responds accordingly.

Windows Firewall protects against unauthorized access.

Securing Privileged Access Roadmap provides guidance for protecting workstations used for privileged access.

Attacker gains access into the device.

Windows 10 UEFI Secure Boot helps protect the boot process and firmware against tampering, such as from a physically present attacker.

Windows 10 BitLocker protects files from access without the user credentials.

Attacker moves laterally, gaining access to cloud services and resources in the environment.

Azure AD conditional access rules can protect all SaaS apps in your environment.

Cloud App Security detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Securing Privileged Access Roadmap is guidance to mitigate lateral traversal and credential theft techniques for your onpremises and hybrid cloud environments.

For on-premises networks, Advanced Threat Analytics identifies abnormal activity by using behavioral analytics and leveraging Machine Learning.

Attacker moves laterally, gaining access to cloud services and resources in the environment.

Intune device compliance policies define criteria for healthy and compliant devices.

Azure AD conditional access rules block access from noncompliant devices and enforce multi-factor authentication for access to cloud services.

Cloud App Security detects and alerts on anomalous activity.

Windows Defender Advanced Threat Protection is a service that helps detect, investigate, and respond to advanced attacks on your networks.

Windows 10 Credential Guard prevents attackers from gaining access to other resources in the organization through Pass-the-Hash or Pass-the-Ticket attacks.

Exfiltrate data

Attacker removes data from the environment.

Cloud App Security detects and alerts on anomalous activity, such as download activity, and can suspend user accounts.

Intune Mobile Application Management rules prevents business data from leaving approved business apps on mobile devices.

Windows Information Protection (WIP) protects business content on devices with file level encryption that helps prevent accidental data leaks to nonbusiness documents, unauthorized apps, and unapproved locations.

Office 365 Exchange mail flow rules prevent auto-forwarding of mail to external domains.

Office 365 data loss prevention (**DLP**) rules prevent sensitive data from leaving the environment.

Azure Information Protection and Azure **Rights Management** encrypts and permissions sensitive files. Protection travels with the files.

Azure technologies provide encryption for disks and storage, SQL Encryption, and Key vault.

SQL Database dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

SQL Threat Detection alerts on suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns.

Azure Backup is a service you can use to back up and restore your data in the Microsoft cloud. This service includes capabilities to protect your backups from ransomware.