Common attacks and Microsoft capabilities that protect your organization

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.

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.

Any employee clicks on a link and enters their credentials.

Azure Identity Protection detects users with leaked credentials, sign-ins from anonymous IP addresses, impossible travel to atypical locations, sign-ins from IP addresses with suspicious activity, sign-ins from unfamiliar locations.

Azure Advanced Threat Protection helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber identity attacks and insider threats.

Threat Actor replaces firmware with malware with Firmware bootkits or Threat Actor places bootkits to start malware before Windows starts

Secure boot makes sure that a device boots using only software that is trusted by the OEM. When the PC starts, the firmware checks the signature of UEFI firmware drivers, EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system.

Threat Actor installs system or driver rootkits to start kernel-level malware while Windows is starting, before Windows Defender and antimalware solutions can start.

Trusted Boot with Early Launch Antimalware(ELAM) evaluates the boot time device/application drivers for malicious code.

Virtualization based Security is a hardware virtualization feature that isolates a secure region of memory from the normal operating system.

Device Guard: Kernel Mode Code Integrity restricts devices to only run authorized apps while also hardening the OS against kernel memory attacks

Threat Actor installs user-level malware and exploits a vulnerability in the system or an application, and owns the device after Windows starts

OS Improved Features such as protected Process
Device Guard: User Model Code Integrity restricts devices to only run authorized apps

Enter

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.

Attacker uses stolen privileged credentials to gain access to the corporate resources.

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

- Tier Model – minimizes the chances of privileged credentials being found on devices with Internet risky connections (email and browsing)
- LAPS – Randomizes the local administrator password for the device and stores it in AD
- ESAE/Admin Forest – Isolate privilege credentials from the user and application forest. This allows the capability to implement stronger security configuration for the users and workstations.
- PAM – Enable Just-in-Time (privilege rights provided upon request and in a timed manner)
- PAW – hardened Windows 10 workstation for privileged users (Credential Guard, Firewall, limited applications, Kerberos only and others)

Attacker uses stolen service account credentials to gain access to the corporate resources.

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

- Tier Model – minimizes the chances of privileged credentials being found on devices with Internet risky connections (email and browsing)

Traverse

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 on-premises and hybrid cloud environments.

Azure Advanced Threat Protection helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber identity attacks and insider threats.

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

Securing Privileged Access Roadmap is guidance to mitigate lateral traversal and credential theft techniques for your on-premises and hybrid cloud environments

- Tier Model – minimizes the chances of privileged credentials being found on devices with Internet risky connections (email and browsing)
- ESAE/Admin Forest – Isolate privilege credentials from the user and application forest. This allows the capability to implement stronger security configuration for the users and workstations.
- PAM – Enable Just-in-Time (privilege rights provided upon request and in a timed manner)
- PAW – hardened Windows 10 workstation for privileged users (Credential Guard, Firewall, limited applications, Kerberos only and others).

SecInfo Tools isolation from Production if production is compromised, the attacker would not be able to use the systems to compromise the cloud.

Azure AD Privileged Identity Management provides just in time administrator access

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 non-business 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.

SharePoint Online and OneDrive for Business store deleted files in the recycle bin where they can be restored. Files encrypted by ransom attackers can be rolled back to previous versions.

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.

Microsoft

Common attacks and Microsoft capabilities that protect your organization

Begin attack

Brute-force attack
Attacker tries a large list of possible passwords for a given account or set of accounts.

Azure Advanced Threat Protection helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber Identity attacks and insider threats.

Azure Security Center can determine baseline login activity for virtual machines and use machine learning to define what is outside of normal login activity.

Weak passwords are systematically identified.

Azure Identity Protection detects users with leaked credentials, sign-ins from anonymous IP addresses, impossible travel to atypical locations, sign-ins from IP addresses with suspicious activity, sign-ins from unfamiliar locations.

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.

Windows for Business is a two-factor authentication: one factor being a key or certificate that's bound to the device, and the second a PIN or biometric authentication stored locally on the device.

Other similar attacks:
Watering hole attacks, leaked passwords.

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

Windows Defender App Guard opens the site in an isolated Hyper-V-enabled container, which is separate from the host operating system

Threat Actor installs bootkit, rootkit or other malware, exploits a vulnerability in the system or an application, and owns the device.

Windows 10 Protections slowing attackers by addressing modern security threats with advancements to strengthen identity protection and access control, information protection, and threat resistance: Windows Defender Exploit Guard, Application Guard, Windows Defender ATP, Windows Defender Antivirus, Windows Hello, Device Guard, Credential Guard, BitLocker, SmartScreen, Firewall and others.

Windows Defender Advanced Threat Protection protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and remediate the device by auto-cleaning configuration changes made by the attacker.

Enter

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.

Attacker uses stolen credentials to gain access to the user's files or to account and group management tools or access to a privileged service such as InfoSec systems like key management, configuration management, monitoring, backups, virtualization and others.

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

- Tier Model – minimizes the chances of privileged credentials being found on devices with Internet risky connections (email and browsing)
- LAPS – Randomizes the local administrator password for the device and stores it in AD
- ESAE/Admin Forest – Isolate privilege credentials from the user and application forest. This allows the capability to implement stronger security configuration for the users and workstations.
- PAM – Enable Just-in-Time (privilege rights provided upon request and in a timed manner)
- PAW – hardened Windows 10 workstation for privileged users (Credential Guard, Firewall, limited applications, Kerberos only and others)

Windows Defender Advanced Threat Protection alerts and integrate with other tools like SIEM, Azure Security Center, Azure AD Conditional Access to make decisions to block access.

Traverse

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 on-premises and hybrid cloud environments.

Azure Advanced Threat Protection helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber attacks and insider threats.

Attacker uses credentials to quickly spread through the environment including creating backdoor accounts, adding them to privileged groups, changing GPOs, installing malware or changing system configuration using compromised InfoSec systems or even compromising key and certificate servers.

Azure Security Center bring information from Microsoft and third party partner tools together and provide automated correlation to alert about the threats. Supports Win Devices and Linux both on-prem or any IaaS Cloud

Windows Defender Advanced Threat Protection alerts about abnormal behavior.

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

Azure AD Cloud IaaS Forest provides isolation for high valuable assets. Follows the DIAD recommended structure, uses the latest Windows Server capabilities and removes legacy functionality. Since Privilege user accounts are limited (PAM integration) and Tier 2 systems and users are in a separate forest, it is easier to maintain Tier-1 focus configuration and updates.

Azure SaaS and PaaS Applications make it more difficult for legacy configurations and threats like pass-the-hash to have much effect.

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 non-business 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.

SharePoint Online and OneDrive for Business store deleted files in the recycle bin where they can be restored. Files encrypted by ransom attackers can be rolled back to previous versions.

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.

Microsoft

Common attacks and Microsoft capabilities that protect your organization

Begin attack

Lost or stolen device → Possession is unknown. → Attacker gains access into the device. → Attacker moves laterally, gaining access to cloud services and resources in the environment. → Attacker removes data from the environment.

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

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

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

Trusted Platform Module (TPM) provides hardware-based, security-related functions.

Device Health Attestation validates the TPM and PCR logs for a device and issues a DHA report. Integrates with MDM

Intune (MDM) manages mobile devices, mobile apps, protect your organization information by helping to control the way your workforce accesses and shares it.

Windows Defender Advanced Threat Protection helps detect, investigate, and remediate the device by auto-cleaning configuration changes made by the attacker.

→ Malicious files and viruses are introduced into the environment. → Any employee clicks on a malicious link or opens a malicious file shared by the compromised user.

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.

Trusted Platform Module (TPM) provides hardware-based, security-related functions.

Device Health Attestation validates the TPM and PCR logs for a device and issues a DHA report. Integrates with MDM

Intune (MDM) manages mobile devices, mobile apps, protect your organization information by helping to control the way your workforce accesses and shares it.

Conditional Access enforces controls on the access to apps in your environment based on specific conditions from a central location.

Enter

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.

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

Any employee clicks on a malicious link or opens a malicious file shared by the compromised user.

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

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.

Windows Defender Advanced Threat Protection protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and remediate the device by auto-cleaning configuration changes made by the attacker

Traverse

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

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 remediate the device by auto-cleaning configuration changes made by the attacker.

Windows 10 Credential Guard makes it more difficult for attackers gaining access to other resources in the organization through Pass-the-Hash or Pass-the-Ticket attacks.

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

Azure Advanced Threat Protection helps protect your enterprise hybrid environments from multiple types of advanced targeted cyber attacks and insider threats.

Exfiltrate data

Attacker removes data from the environment.

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 non-business documents, unauthorized apps, and unapproved locations.

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

SharePoint Online and OneDrive for Business store deleted files in the recycle bin where they can be restored. Files encrypted by ransom attackers can be rolled back to previous versions.

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.

Zero Day and Polymorphic malware is introduced in the environment → Malware changes signatures in a random timeframe using real company compromised code sign certificates → Malware perform different type of behaviors in order to confuse the defensive systems. → Malware self replicate through the environment

Windows Defender Advanced Threat Protection protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and remediate the device by auto-cleaning configuration changes made by the attacker

Intelligent Security Graph real-time threat protection provided by many Microsoft products and services. This protection is powered by artificial intelligence predictive calculations made from the analysis of behavior observed and information gathered from all the different services interconnected in the environment as well to the security graph. This includes both Microsoft and Third party partners.

Azure Security Center bring information from Microsoft and third party partner tools together and provide automated correlation to alert about the threats. Supports Win Devices and Linux both on-prem or any IaaS Cloud

Microsoft

Common attacks and Microsoft capabilities that protect your organization

Begin attack

Attack start in the IT-Supply chain → Master file table is encrypted or the boot record is replaced with malicious code

Secure boot makes sure that a device boots using only software that is trusted by the OEM. When the PC starts, the firmware checks the signature of UEFI firmware drivers, EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system.

Virtualization based Security is a hardware virtualization feature that isolates a secure region of memory from the normal operating system.

Device Guard: Kernel Mode Code Integrity restricts devices to only run authorized apps while also hardening the OS against kernel memory attacks

Users access to the Corporate resources from non-secure devices and threat actor tricks them to run a link from email → The malware attempts to make external connections and creates the service to continue infection

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.

Windows 10 slowing attackers by addressing modern security threats with advancements to strengthen identity protection and access control, information protection, and threat resistance: Windows Defender Exploit Guard, Application Guard, Windows Defender ATP, Windows Defender Antivirus, Windows Hello, Device Guard, Credential Guard, BitLocker, SmartScreen, Firewall and others.

Enter

Automatic propagation that leave little time to react → A dropper Trojan attempts to exploit the SMB CVE-2017-0145 vulnerability in other computers

Windows Defender Advanced Threat Protection protects endpoints from cyber threats; detects advanced attacks and data breaches, protects the organization by blocking access until the system is remediated and automates the resolution of security incidents and response. For blocking access, Intune and Azure AD are required to drive the policies.

Windows Defender Advanced Threat Protection protects endpoints from cyber threats; detects advanced attacks and data breaches, protects the organization by blocking access until the system is remediated and automates the resolution of security incidents and response. For blocking access, Intune and Azure AD are required to drive the policies.

Traverse

Use multiple traversal techniques to try to fool protection systems → Uses the network to spread through SMB exploit when an unpatched computer is available from the infected machines

Windows Defender Advanced Threat Protection protects endpoints from cyber threats; detects advanced attacks and data breaches, protects the organization by blocking access until the system is remediated and automates the resolution of security incidents and response. For blocking access, Intune and Azure AD are required to drive the policies.

Windows Firewall protects against unauthorized access by blocking legacy protocols and others.

Azure AD Cloud IaaS Forest provides isolation for high valuable assets. Follows the DIAD recommended structure, uses the latest Windows Server capabilities and removes legacy functionality. Since Privilege user accounts are limited (PAM integration) and Tier 2 systems and users are in a separate forest, it is easier to maintain Tier-1 focus configuration and updates.

Exfiltrate data

Asset data is destroyed → Ransomware takes over the infected machines

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

SharePoint Online and OneDrive for Business store deleted files in the recycle bin where they can be restored. Files encrypted by ransom attackers can be rolled back to previous versions.

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.

Azure SaaS and PaaS Applications makes it more difficult for ransomware.

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

SharePoint Online and OneDrive for Business store deleted files in the recycle bin where they can be restored. Files encrypted by ransom attackers can be rolled back to previous versions.

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.

Azure SaaS and PaaS Applications makes it more difficult for ransomware.

Microsoft

Begin attack

User uses an USB Device to copy data
or
User uses a cloud service to exfiltrate information
or
User uses wrong application to open or save documents at (IE: Partner app instead of Organization's)
or
Personal Device was enrolled into the organization's environment. After saving lots of data in the device, the user leaves the organization

Azure AD single identity for all cloud applications can help report and audit all user access.

Intune manages the device and apply Mobile Application Management (MAM) policies

Enter

Control of Data location is lost

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

Cloud App Security detects and ale rts 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.

Exfiltrate data

Data gets published in the internet or sold to competitors

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

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