Contents

Identity and access management

4/5/2019 • 2 minutes to read • Edit Online

Learn more about identity annd access management technologies in Windows 10 and Windows 10 Mobile.

SECTION	DESCRIPTION
Access control	Describes access control in Windows, which is the process of authorizing users, groups, and computers to access objects on the network or computer. Key concepts that make up access control are permissions, ownership of objects, inheritance of permissions, user rights, and object auditing.
Configure S/MIME for Windows 10 and Windows 10 Mobile	In Windows 10, S/MIME lets users encrypt outgoing messages and attachments so that only intended recipients who have a digital identification (ID), also known as a certificate, can read them. Users can digitally sign a message, which provides the recipients with a way to verify the identity of the sender and that the message hasn't been tampered with.
Install digital certificates on Windows 10 Mobile	Digital certificates bind the identity of a user or computer to a pair of keys that can be used to encrypt and sign digital information. Certificates are issued by a certification authority (CA) that vouches for the identity of the certificate holder, and they enable secure client communications with websites and services.
Protect derived domain credentials with Credential Guard	Introduced in Windows 10 Enterprise, Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Credential Guard helps prevent these attacks by protecting NTLM password hashes and Kerberos Ticket Granting Tickets.
Protect Remote Desktop credentials with Remote Credential Guard	Remote Credential Guard helps you protect your credentials over a Remote Desktop connection by redirecting the Kerberos requests back to the device that's requesting the connection.
User Account Control	Provides information about User Account Control (UAC), which helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. UAC can help block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.
Virtual Smart Cards	Provides information about deploying and managing virtual smart cards, which are functionally similar to physical smart cards and appear in Windows as smart cards that are always-inserted. Virtual smart cards use the Trusted Platform Module (TPM) chip that is available on computers in many organizations, rather than requiring the use of a separate physical smart card and reader.

SECTION	DESCRIPTION
VPN technical guide	Virtual private networks (VPN) let you give your users secure remote access to your company network. Windows 10 adds useful new VPN profile options to help you manage how users connect.
Smart Cards	Provides a collection of references topics about smart cards, which are tamper-resistant portable storage devices that can enhance the security of tasks such as authenticating clients, signing code, securing e-mail, and signing in with a Windows domain account.
Windows Hello for Business	In Windows 10, Windows Hello replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and a biometric or PIN.
Windows 10 Credential Theft Mitigation Guide Abstract	Learn more about credential theft mitigation in Windows 10.

Information protection

4/5/2019 • 2 minutes to read • Edit Online

Learn more about how to secure documents and other data across your organization.

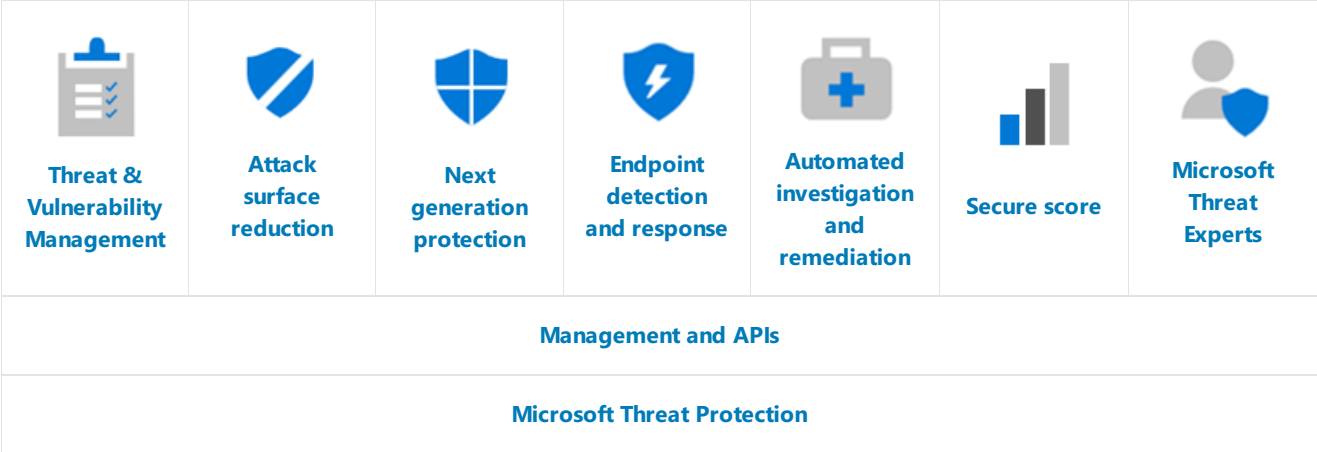
SECTION	DESCRIPTION
BitLocker	Provides information about BitLocker, which is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
Encrypted Hard Drive	Encrypted Hard Drive uses the rapid encryption that is provided by BitLocker Drive Encryption to enhance data security and management.
Kernel DMA Protection for Thunderbolt™ 3	Kernel DMA Protection protects PCs against drive-by Direct Memory Access (DMA) attacks using PCI hot plug devices connected to Thunderbolt™ 3 ports.
Protect your enterprise data using Windows Information Protection (WIP)	Provides info about how to create a Windows Information Protection policy that can help protect against potential corporate data leakage.
Secure the Windows 10 boot process	Windows 10 supports features to help prevent rootkits and bootkits from loading during the startup process.
Trusted Platform Module	Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that helps you with actions such as generating, storing, and limiting the use of cryptographic keys.

Threat Protection

5/31/2019 • 2 minutes to read • Edit Online

Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) is a unified platform for preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender ATP protects endpoints from cyber threats; detects advanced attacks and data breaches, automates security incidents and improves security posture.

Microsoft Defender ATP



Threat & Vulnerability Management

This built-in capability uses a game-changing risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.

- Risk-based Threat & Vulnerability Management
- What's in the dashboard and what it means for my organization
- Configuration score
- Scenarios

Attack surface reduction

The attack surface reduction set of capabilities provide the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, these set of capabilities resist attacks and exploitations.

- Hardware based isolation
- Application control
- Device control
- Exploit protection
- Network protection
- Controlled folder access
- Network firewall
- Attack surface reduction controls

Next generation protection

To further reinforce the security perimeter of your network, Microsoft Defender ATP uses next generation protection designed to catch all types of emerging threats.

- Behavior monitoring
- Cloud-based protection
- Machine learning
- URL Protection
- Automated sandbox service

Endpoint detection and response

Endpoint detection and response capabilities are put in place to detect, investigate, and respond to advanced threats that may have made it past the first two security pillars.

- Alerts
- Historical endpoint data
- Response orchestration
- Forensic collection
- Threat intelligence
- Advanced detonation and analysis service
- Advanced hunting
  - Custom detection
  - Realtime and historical hunting

Automated investigation and remediation

In conjunction with being able to quickly respond to advanced attacks, Microsoft Defender ATP offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

- Automated investigation and remediation
- Threat remediation
- Manage automated investigations
- Analyze automated investigation

Secure score

Microsoft Defender ATP includes a secure score to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization.

- Asset inventory
- Recommended improvement actions
- Secure score
- Threat analytics

Microsoft Threat Experts

Microsoft Defender ATP's new managed threat hunting service provides proactive hunting, prioritization and additional context and insights that further empower Security Operation Centers (SOCs) to identify and respond to threats quickly and accurately.

- Targeted attack notification
- Experts-on-demand
- Configure your Microsoft Threat Protection managed hunting service

Management and APIs

Integrate Microsoft Defender Advanced Threat Protection into your existing workflows.

- Onboarding
- API and SIEM integration

- Exposed APIs
- Role-based access control (RBAC)
- Reporting and trends

Microsoft Threat Protection

Microsoft Defender ATP is part of the Microsoft Threat Protection solution that helps implement end-to-end security across possible attack surfaces in the modern workplace. Bring the power of Microsoft threat protection to your organization.

- Conditional access
- O365 ATP
- Azure ATP
- Azure Security Center
- Skype for Business
- Microsoft Cloud App Security