
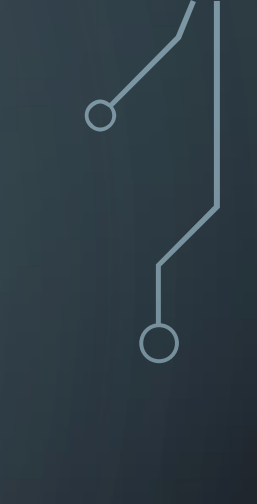
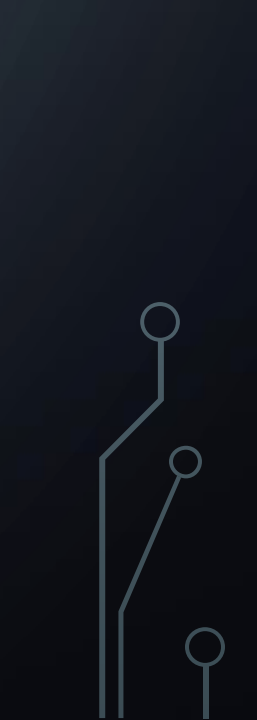


An abstract graphic on the left side of the slide, consisting of a network of thin, light-blue lines and small circles, resembling a circuit board or a neural network. The lines are vertical and horizontal, with some diagonal connections, and the circles are small and white, acting as nodes or junctions.

WINDOWS IN THE ENTERPRISE



OBJECTIVES

- Explain why Windows is heavily focused in the enterprise
 - Discuss some key metrics
 - Discuss what Windows is good at and why you might want to use Windows in an enterprise environment
- 
- 
- 

MICROSOFT

- Microsoft started in 1975 with Paul Allen and Bill Gates
- 114k employees today
- Owns major brands such as Office, Xbox, Skype, Office 365, Nokia, MSN, 343 studios
- 80% of Fortune 500 run on Microsoft Cloud
- Worth about \$450-\$500B

FUN MICROSOFT FACTS

- The generic silhouette outline placeholder picture in Microsoft Outlook 2010 is actually Bill Gates' mug shot, when he was arrested for a driving offense.
- DirectX's original name was 'The Manhattan Project' because it was Microsoft's initiative to destroy Japanese dominance of the gaming industry.
- Microsoft included Solitaire in Windows, in part, to familiarize people with drag and drop operations. In 1990, many users were still unfamiliar with graphical user interfaces.
- The guy who snagged windows2000.com happened to be named Bob and Microsoft just happened to own Bob.com. They came to an agreement to trade one for the other.
- In 1997, Microsoft invested \$150 million in Apple to help revitalize the then failing company.

WINDOWS BY THE NUMBERS

- Microsoft started in 1975 with Paul Allen and Bill Gates
- 1985 – Windows 1.0 came out
- Latest OS is Windows 10
- 400 million devices running Windows 10 alone
- 192 countries run Microsoft Windows

WHY LEARN ABOUT WINDOWS

- Enterprises run on windows, both on workstations and servers
- UCCS is roughly 70% Windows for desktops, 50% servers
- Virtualization
 - Hyper-V 35%
 - VMware – 65%
- Some reports say 95% of companies use Windows Active Directory for user management

WHAT WINDOWS DOES BEST

- Enterprise operating systems – Windows 7,8,10 etc.
- User management – Active Directory
- Authentication – ADFS, Kerberos

WINDOWS AS A DESKTOP OS

- Ease of management
- Built for enterprises
- Antivirus baked in
- Gaming
- Security features
- Xbox app!
- Encryption

CONCLUSION


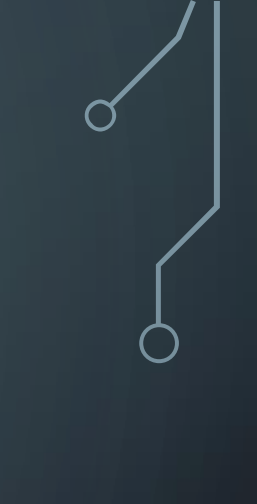
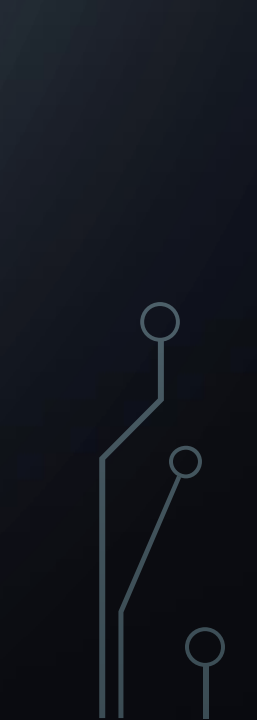
- Windows is robust and has many components that can be configured to suit nearly any enterprise needs
- Planning for a Windows environment also takes time and effort

An abstract graphic on the left side of the slide, consisting of a network of thin, light-blue lines and small circles, resembling a circuit board or a neural network. The lines are vertical and horizontal, with some diagonal connections, and the circles are small and white, acting as nodes or junctions.

WHAT IS AUTHORIZATION



OBJECTIVES

- Discuss what authorization is
 - Explain scenarios where authorization is important
 - Discuss why it's important to Windows specifically
- 
- 
- 

AUTHORIZATION

- Authorization is allowing or denying permissions based on who or what you are
- Extremely important in practical business world

SCENARIO

- You invited me to your place
- Once I am there, I knock the door
- You open the door, greet me, and invite me to come inside...
- What does prevent me to grab a coke (or three!) from your refrigerator, or destroying your TV?

You ***authenticated*** me (biometrics – facial recognition). What did you **authorize** me to do?



AUTHORIZATION AND PERMISSIONS

When we provide access to our information systems, computers, and networks to others:

- We cannot afford the luxury of making assumptions about their code of ethics
- Instead, we must develop *access control systems* that prevent unwanted behaviors
- Regardless of code of ethics, what happens in the case of accidental exposure or destruction of data?



WINDOWS USERS AND AUTHORIZATION

- Enterprise users have access to many tools and data
 - Organizational data security must remain intact
 - Comprehensive authorization models must be developed to ensure that business data remains secure
- 
- 

USERS

- A organization cannot rely on users to keep their data secure
- Comprehensive access control plan helps ensure data remains safe
- The biggest threat to organizational data is users
- Due to the way Windows authenticates users – more specifically Kerberos, access control is essential to protect data

CONCLUSION



- Next few lessons will focus on how we protect data within Windows
- Users are an issue. If we didn't have users, then data may be secure! — But if we didn't have users, we wouldn't have jobs

An abstract graphic on the left side of the slide, consisting of a series of vertical and diagonal lines of varying lengths, some ending in small circles, resembling a circuit board or a stylized tree structure.

BUILT IN SECURITY CONTROLS



OBJECTIVES

- Discuss many security features that are configurable on Windows
 - Explain how users might use the security features to protect Windows systems
 - Discuss how the technology might affect the end user experience
- 
- 

DEFENDER

- Technology: Antimalware that is built into Windows. Provides both administrators and end users to scan files and processes, checking for malware
- How it's configured: Built in, however, domain admins have control if needed
- How user's might use the technology to protect themselves: Scanning files and processes
- How administrators use it: automatically scanning devices, one-off system scanning to ensure system is safe
- User Experience: End-users won't even know it's running unless they receive an alert or a system administrator starts a scan

FIREWALL

- Technology: Standard GUI and CLI based firewall that allows or denies actions based on port, service, protocol or application
- How it's configured: Users or Administrators
- How user's might use the technology to protect themselves: May let software through that needs to communicate out to receive updates
- How administrators use it: block certain activity such as gaming
- User Experience: User only notices if program requests access to add settings to firewall

SECURE BOOT/UEFI

- Technology: Verifies bootloader so rootkit infected OS cannot run
- How it's configured: Must be configured upon installation of OS
- How user's might use the technology to protect themselves: Not configured for end user
- How administrators use it: Protect against systems that have been infected at the operating system level. Guarantee software is genuine
- User Experience: Not configured for end user

VBS

- Technology: Virtualization-based security runs sensitive processes inside of a protected environment, strengthening security
- How it's configured: Built into operating system, but with caveats
- How user's might use the technology to protect themselves: Happens automatically
- How administrators use it: Very strict set of requirements to run, however provides great protection
- User Experience: Happens automatically

DEVICE GUARD AND CREDENTIAL GUARD

- Technology: Uses virtualization-based security to protect devices and credentials by running them through virtual subsystems
- How it's configured: Generally administrators
- How user's might use the technology to protect themselves: Happens automatically
- How administrators use it: Requires VBS, but allows protection of OS through devices, protects credentials from being stolen
- User Experience: Happens automatically

DEP

- Technology: Data Execution Prevention prevents malware from executing in spaces designed for OS execution
- How it's configured: Either through user or through Administrator
- How user's might use the technology to protect themselves: Protects certain programs, configurable by the user to not execute code outside the application memory
- How administrators use it: Same as users
- User Experience: Can be cumbersome if users have a lot of applications

CONCLUSION


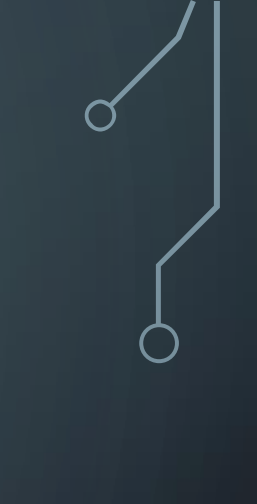
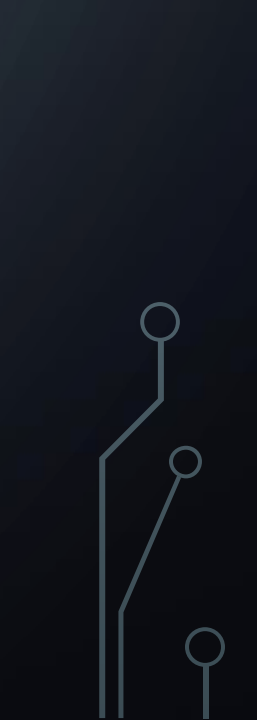
- Windows has many more features than the ones listed
- The features discussed will help with overall attack surface, but end-users still need to be vigilant about security
- Windows provides security to protect end users, however they are only effective when users and administrators run them properly

A decorative graphic on the left side of the slide, consisting of a series of vertical and diagonal lines of varying lengths, some ending in small circles, resembling a circuit board or a stylized tree structure.

SECURITY CONSIDERATIONS FOR WINDOWS





OBJECTIVE

- Discuss concepts where it may not be so obvious to secure our infrastructure
 - Explain why it's a good idea to build a layered security approach
 - Discuss points in which my experience has told me goes further than completely relying on technology
- 
- 
- 



CONSIDERATION 1 – ASSESSING YOUR ENVIRONMENT

- Windows cannot protect you from everything
 - Even with enhancements over the years, security is still a problem
 - Completed security checklist for systems and audit regularly
 - Example: Patches - finding missing updates
- 
- 

CONSIDERATION 2 - MONITOR

- Event logs can be boring to read through, however essential to a well running environment
- Security and system logs are important to understand
- Use another system to monitor critical infrastructure
- Example: How do you know something is working or not working?

CONSIDERATION 3 – USE A LAYERED APPROACH TO SECURITY

- A firewall can't protect everything just like antivirus can't protect you from everything either
- Careful consideration and due diligence are important steps in planning for a secure environment
- Firewalls, antimalware, DEP, least privilege are all steps in protecting systems, however, without understanding how users are using the system, layered security might be too restrictive
- Example: Password security policies may have opposite effect you want

CONSIDERATION 4 – YOUR END USERS NEED YOUR HELP

- Not everything is intuitive like Microsoft thinks it is
- Users need training as to why or why not technology put in place is there to protect them
- You have to support your users in the end
- Example: Moving to the cloud

CONCLUSION

- While some decisions seem obvious to you, they always aren't to everyone else
- Explanations on security decisions go a long way to ensure stability and continuity and less data breaches