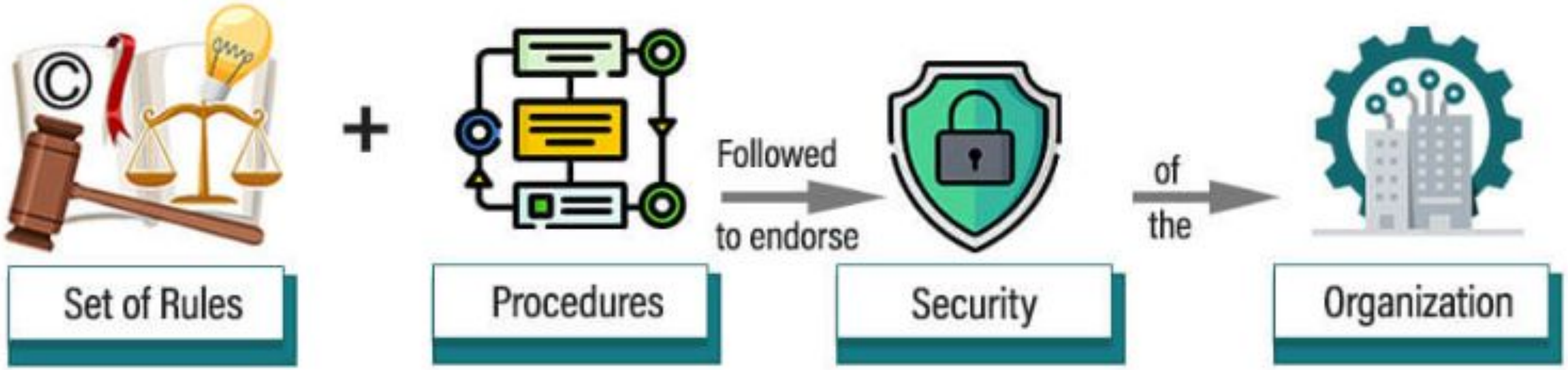
Unit 5: Security Policy



Reviewing Your Security Policy

- "Do you even have a security policy in place?“
- "Do you enforce this security policy ?“
- How often you review the policy?
- Whom the Security Policy is applicable?

Reviewing Your Security Policy

Security policies should include industry standards, procedures, and guidelines, which are necessary to support information risks in daily operations. These policies must also have a well-defined scope.

It is imperative that the applicability of the security policy states where it applies.

For example, if it applies to all data and systems, this must be clear to everyone reading it. Or Does this policy is applicable to contractors. Whether answer is Yes or No.. It must be stated in the scope section of the policy.

Reviewing Your Security Policy

- The foundation of the security policy should be based on the security triad (confidentiality, integrity, and availability).
- Ultimately, the users are required to protect and ensure the applicability of the security triad in the data and systems, which is independent of how that data was created, shared, or stored. Users must be aware of their responsibilities, and the consequences of violating these policies.
- Make sure that you also include a section that specifies the roles and responsibilities, since this is very important for accountability purposes.

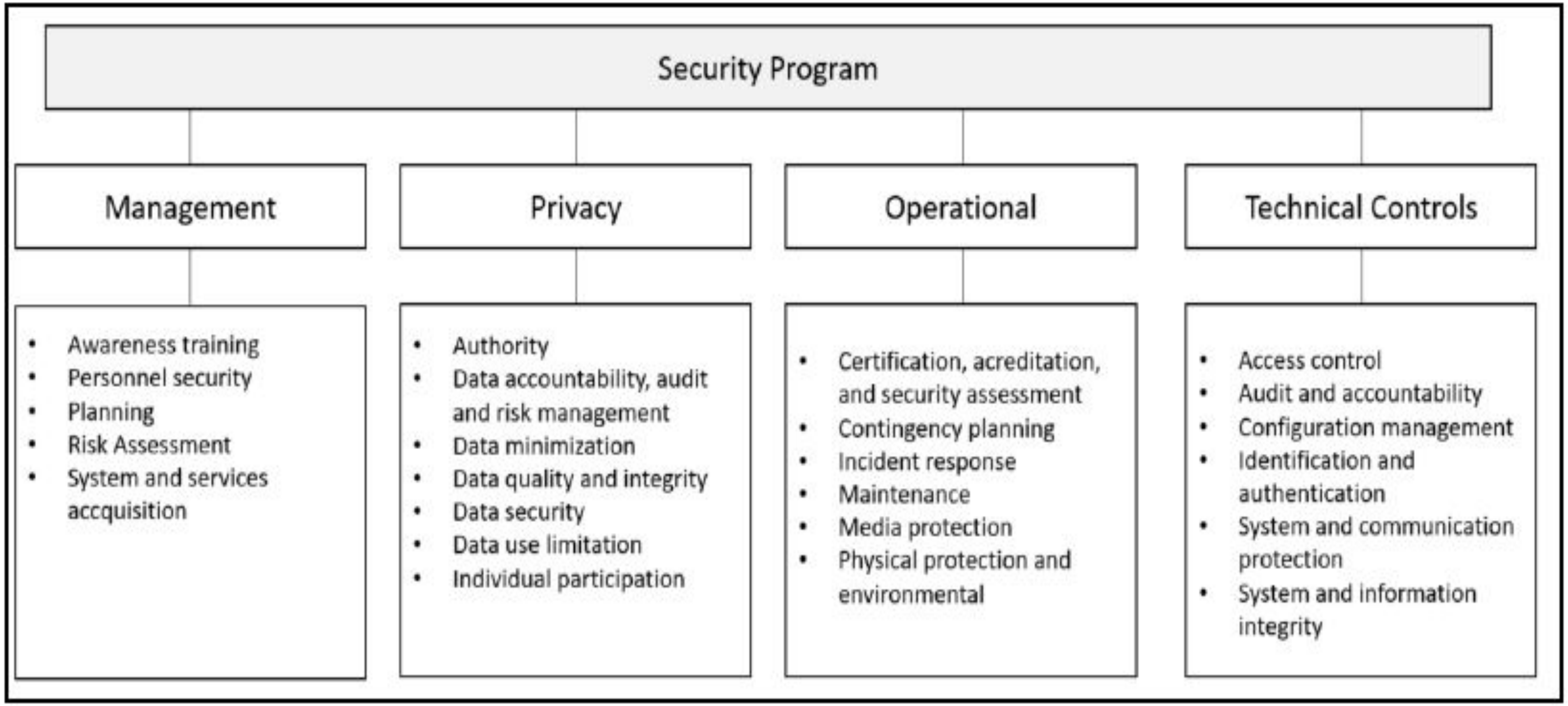
Policy: This is the basis of everything; it sets high-level expectations. It will also be used to guide decisions and achieve outcomes.

Procedure: As the name suggests, this is a document that has procedural steps that outline how something must be done.

Standard: This document establishes requirements that must be followed. In other words, everyone must comply with certain standards that were previously established.

Guidelines: Although many would argue that guidelines are optional, they are in fact more additional recommended guidance. Having said that, it is important to note that each company has the freedom to define whether the guidelines are optional, or if they are recommended.

Best practices: As the name says, these are best practices to be implemented by the entire company, or just some departments within the company. This can also be established per role—for example, all web servers should have security best practices from the vendor applied prior to being deployed in production.



Security Program

Management

- Awareness training
- Personnel security
- Planning
- Risk Assessment
- System and services accquisition

Privacy

- Authority
- Data accountability, audit and risk management
- Data minimization
- Data quality and integrity
- Data security
- Data use limitation
- Individual participation

Operational

- Certification, acreditation, and security assessment
- Contingency planning
- Incident response
- Maintenance
- Media protection
- Physical protection and environmental

Technical Controls

- Access control
- Audit and accountability
- Configuration management
- Identification and authentication
- System and communication protection
- System and information integrity

Educating End User

- End user's education is part of the management security control, under awareness training.
- Because a user who is uneducated in security practices can cause tremendous damage to your organization.
- According to ***Symantec Internet Security Threat Report Volume 22***, spam campaigns are the top cause of malware infestation, and although nowadays they rely on a great range of tactics, the largest malware spamming operations are still relying on social engineering techniques.

Educating End User

- In the Symantec report 2016, stated that, most common word used in malware campaigns was "invoice."
- This makes total sense, since the idea is to scare the user into thinking that he or she needs to pay something, otherwise something bad will happen.
- This is a typical approach: to scare in order to entice the user to click on the link that will compromise the system.
- Another platform that is being used to launch social engineering attacks is social media.
- In 2015, Symantec uncovered the diet spam operation on Twitter that used hundreds of thousands of fake accounts that were impersonating legitimate accounts to build a big follower base, and with that spread false propaganda about weight-loss solutions.
- The problem is that many users will be using their own device to access company information, also known as **bring your own device** (**BYOD**), and when they are participating in false social media campaigns like this, they are easy targets for hackers.

Social Media Security Guidelines for Users

- In an article titled Social Media Impact, published by ISSA Journal and written by Yuri Diogenes, many cases were examined where social media was the main tool for social engineering attack.
- The security program must be in line with HR and legal requirements regarding how much company should handle social media posts, and also give guidelines to employees on how they should handle their own social media presence.
- In October 2017, right after the mass shooting in Las Vegas, the CBS vice president made a comment implying that "Vegas victims didn't deserve sympathy because country music fans are often Republicans.“
- The result of this online comment was simple: She was fired for violating the company's standards of conduct.
- While it was important for CBS to apologize rapidly for her behavior and show policy enforcement by firing the employee, the company was still hurt by this person's comments.

Social Media Security Guidelines for Users

- With the political tensions in the world and the freedom that social media gives to individuals to externalize their thoughts, situations like this are arising every single day.

In August 2017, a Florida professor was fired for tweeting that Texas deserved Hurricane Harvey after voting for Trump.

- This is another example of an employee using his personal Twitter account to rant online and reaping bad consequences.
- Often, companies base their decision for firing an employee who misbehaved online on their code of conduct.
- For example, if you read the *Outside Communications* section in the Google Code of Conduct, you will see how Google makes recommendations regarding public disclosure of information.
- Another important guideline to include is how to deal with defamatory posts, as well as pornographic posts, proprietary issues, harassment, or posts that can create a hostile work environment.

Security Awareness Training

Security awareness training should be delivered to all employees, and it should be constantly updated to include new attack techniques and considerations.

Many companies are delivering such training online, via the company's intranet. If the training is well crafted, rich in visual capabilities, and contains a self-assessment at the end, it can be very effective.

Ideally, the security awareness training should contain:

Real-world examples: Users will more easily remember things if you show a real scenario. For example, talking about phishing emails without showing what a phishing email looks like, and how to visually identify one, won't be very effective.

Practice: Well-written text and rich visual elements are important attributes in training materials, but you must submit the user to some practical scenarios.

At the end of training, all users should acknowledge that they finalized the training and they are aware of security threats, countermeasures covered in the training, also about the consequences of not following company’s security policy.

Policy Enforcement

- Once you finish building your security policy, it is time to enforce it, and this enforcement will take place by using different technologies according to the company's needs.
- Ideally, you will have an architecture diagram of your network to understand fully what the endpoints are, what servers you have, how the information flows, where the information is stored, who has and who should have data access, and the different entry points to your network.
- Many companies fail to enforce policies fully because they only think of enforcing policies at endpoints and servers.
- What about network devices? That's why you need a holistic approach to tackle every single component that is active in the network, including switches, printers, and IoT devices.

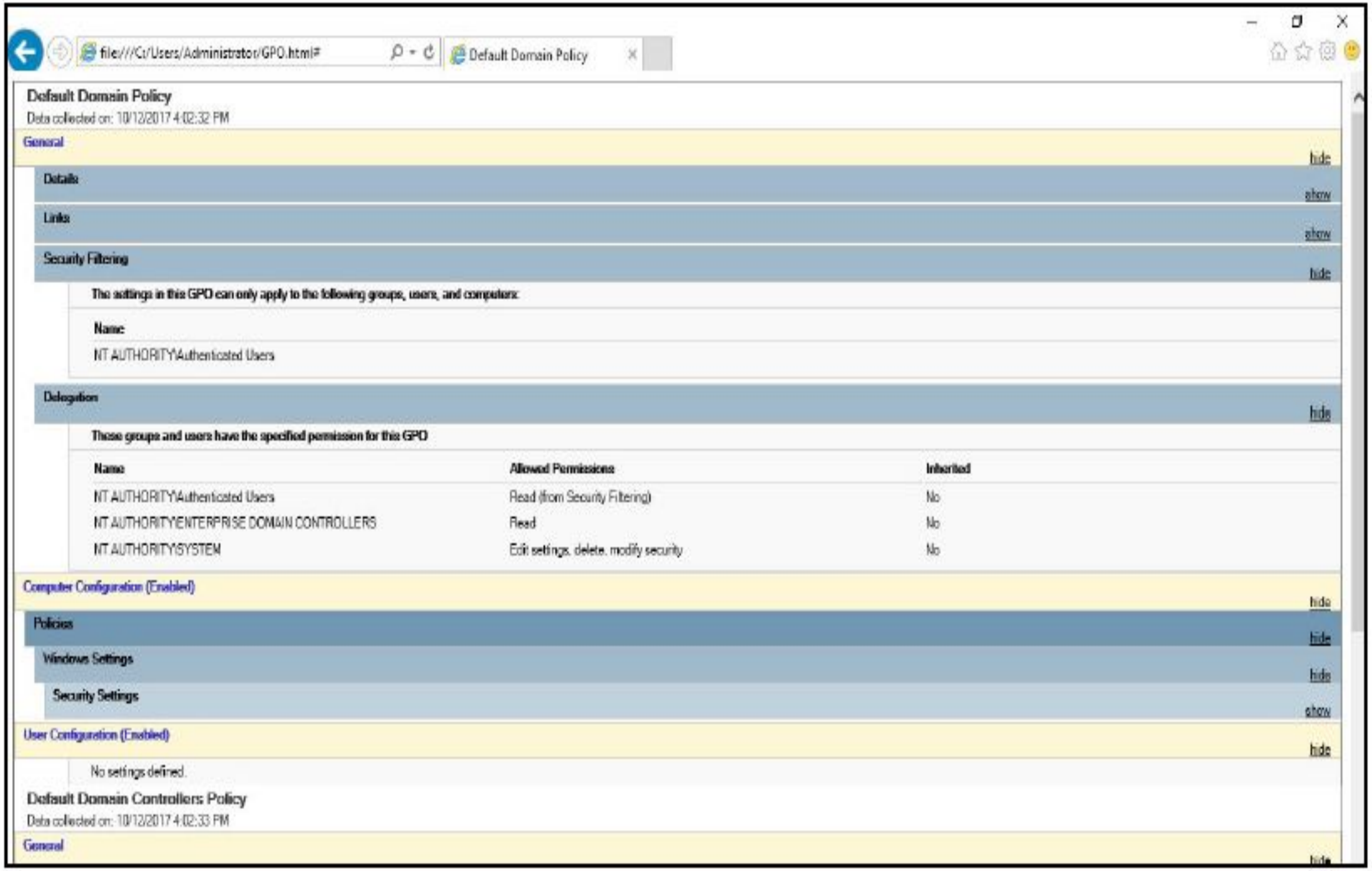
Policy Enforcement

- If your company has Microsoft Active Directory, you should leverage the **Group Policy Object** (**GPO**) to deploy your security policies.
- These policies should be deployed according to your company's security policy. If different departments have different needs, you can segment your deployment using **organizational units** (**OUs**), and assign policies per OU.
- For example, if the servers that belong to the HR department require a different set of policies, you should move these servers to the HR OU and assign a custom policy to this OU.
- If you are unsure about the current state of your security policies, you should perform an initial assessment using the PowerShell command Get-GPOReport to export all policies to an HTML file.
- Make sure that you run the following command from a domain controller:

```
PS C:> Import-Module GroupPolicy
PS C:> Get-GPOReport -All -ReportType HTML -Path .GPO.html
```

Policy Enforcement

The result of this command is shown here:



file:///C:/Users/Administrator/GPO.html#

Default Domain Policy

Default Domain Policy

Data collected on: 10/12/2017 4:02:32 PM

General — hide

Details — show

Links — show

Security Filtering — hide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation — hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled) — hide

Policies — hide

Windows Settings — hide

Security Settings — show

User Configuration (Enabled) — hide

No settings defined.

Default Domain Controllers Policy

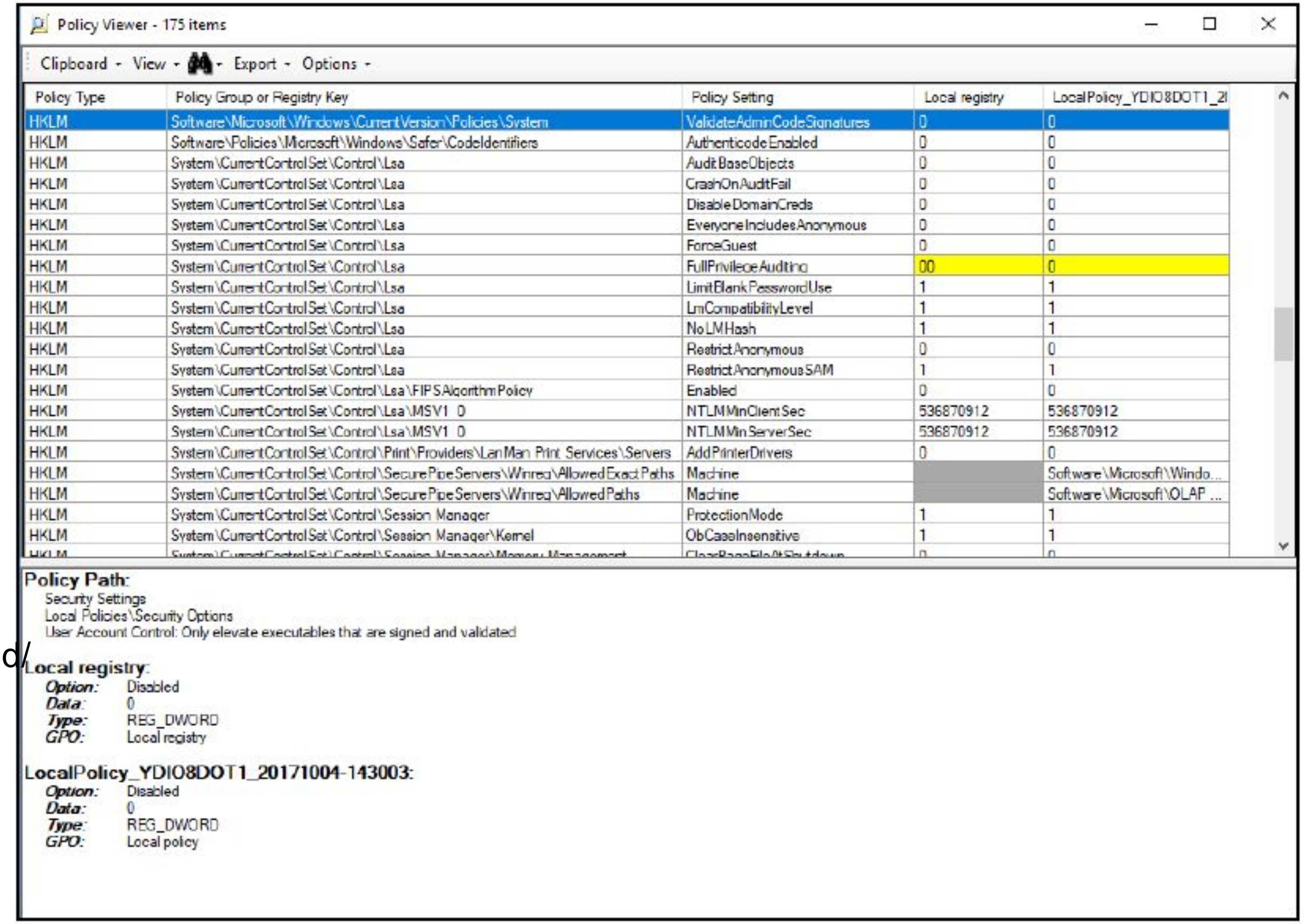
Data collected on: 10/12/2017 4:02:33 PM

General — hide

Policy Enforcement

It is also recommended that you perform a backup of the current configuration and make a copy of this report before making any change to the current group policies.

Another tool that you can also use to perform this assessment is the policy viewer, part of the Microsoft Security Compliance Toolkit, available at https:/ / www. microsoft. com/ en- us/ download/ details. aspx? id= 55319:



Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	LocalPolicy_YDIO8DOT1_2I
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ValidateAdminCodeSignatures	0	0
HKLM	Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	AuthenticodeEnabled	0	0
HKLM	System\CurrentControlSet\Control\Lsa	AuditBaseObjects	0	0
HKLM	System\CurrentControlSet\Control\Lsa	CrashOnAuditFail	0	0
HKLM	System\CurrentControlSet\Control\Lsa	DisableDomainCreds	0	0
HKLM	System\CurrentControlSet\Control\Lsa	EveryoneIncludesAnonymous	0	0
HKLM	System\CurrentControlSet\Control\Lsa	ForceGuest	0	0
HKLM	System\CurrentControlSet\Control\Lsa	FullPrivilegeAuditing	00	0
HKLM	System\CurrentControlSet\Control\Lsa	LimitBlankPasswordUse	1	1
HKLM	System\CurrentControlSet\Control\Lsa	LmCompatibilityLevel	1	1
HKLM	System\CurrentControlSet\Control\Lsa	NoLMHash	1	1
HKLM	System\CurrentControlSet\Control\Lsa	RestrictAnonymous	0	0
HKLM	System\CurrentControlSet\Control\Lsa	RestrictAnonymousSAM	1	1
HKLM	System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy	Enabled	0	0
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinClientSec	536870912	536870912
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinServerSec	536870912	536870912
HKLM	System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers	AddPrinterDrivers	0	0
HKLM	System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths	Machine		Software\Microsoft\Windo...
HKLM	System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths	Machine		Software\Microsoft\OLAP ...
HKLM	System\CurrentControlSet\Control\Session Manager	ProtectionMode	1	1
HKLM	System\CurrentControlSet\Control\Session Manager\Kernel	ObCaseInsensitive	1	1
HKLM	System\CurrentControlSet\Control\Session Manager\Memory Management	ClearPageFileAtShutdown	0	0

Policy Path:
Security Settings
Local Policies\Security Options
User Account Control: Only elevate executables that are signed and validated

Local registry:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local registry

LocalPolicy_YDIO8DOT1_20171004-143003:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local policy

Application Whitelisting

If your organization's security policy dictates that only licensed software is allowed to run in the user's computer, you need to prevent users from running unlicensed software, and also restrict the use of licensed software that is not authorized by IT. Policy enforcement ensures that only authorized applications will run on the system.

When planning policy enforcement for applications, you should create a list of all apps that are authorized to be used in the company. Based on this list, you should investigate the details about these apps by asking the following questions:

What's the installation path for each app?
What's the vendor's update policy for these apps?
What executable files are used by these apps?

Application Whitelisting

In AppLocker, there are three types of conditions to evaluate an app, which are:

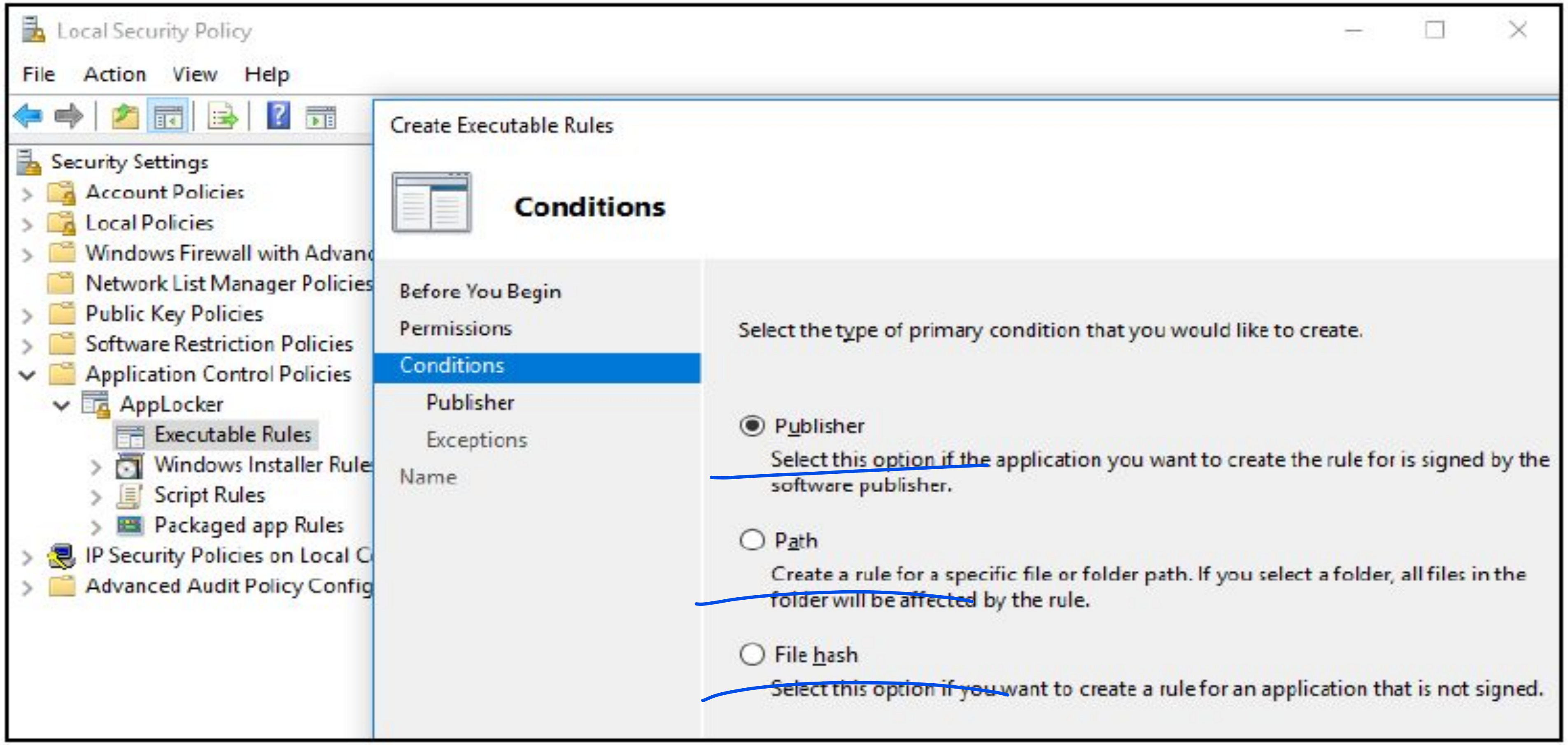
Publisher: This should be used if you want to create a rule that will evaluate an app that was signed by the software vendor.

Path: This should be used if you want to create a rule that will evaluate the application path

File hash: This should be used if you want to create a rule that will evaluate an app that is not signed by the software vendor

Application Whitelisting

These options will appear in the **Conditions** page when you run the create **Executable Rules** wizard:



Select the type of primary condition that you would like to create.

● Publisher

Select this option if the application you want to create the rule for is signed by the software publisher.

○ Path

Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

○ File hash

Select this option if you want to create a rule for an application that is not signed.

Application Whitelisting

Which option you would choose depends on your needs but these choices would cover the majority of the deployment scenarios. Keep in mind that, depending on which option you choose, a new set of questions will appear on the page that follows.

Make sure that you read the AppLocker documentation at https:/ / docs. microsoft. com/ en- us/ windows/ device- security/ applocker/ applocker- overview.

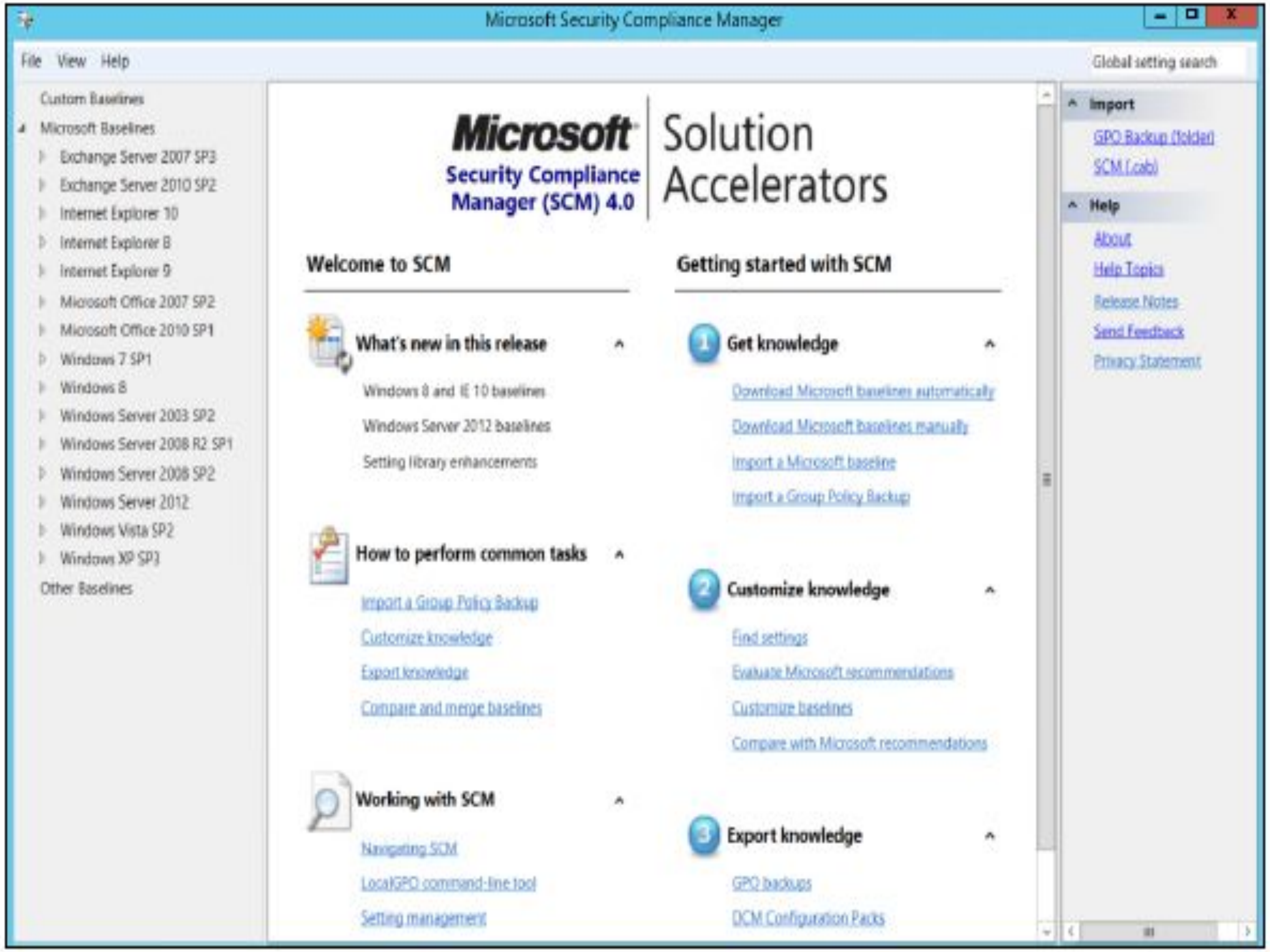
To whitelist apps in an Apple OS, you can use Gatekeeper (https:/ /support. apple. com/ en- us/ HT202491), and in a Linux OS you can use SELinux

Hardening

- As you start planning your policy deployment and addressing which setting should be changed to better protect the computers, you are basically hardening these to reduce the attack vector.
- You can apply **Common Configuration Enumeration (CCE)** guidelines to your computers.
- To optimize your deployment, you should also consider using security baselines. This can assist you in better managing not only the security aspect of the computer.

Hardening

- Hardening is a strategy that involves strengthening the security of a network component by reducing the vulnerability to attacks.
- As you start planning your policy deployment and addressing which setting should be changed to better protect the computers– Hardening process
- You can apply **Common Configuration Enumeration** (**CCE**) guidelines to your computers.



Microsoft Security Compliance Manager

File View Help

Global setting search

Custom Baselines

Microsoft Baselines

- Exchange Server 2007 SP3
- Exchange Server 2010 SP2
- Internet Explorer 10
- Internet Explorer 8
- Internet Explorer 9
- Microsoft Office 2007 SP2
- Microsoft Office 2010 SP1
- Windows 7 SP1
- Windows 8
- Windows Server 2003 SP2
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows Server 2012
- Windows Vista SP2
- Windows XP SP3

Other Baselines

Microsoft Security Compliance Manager (SCM) 4.0 | Solution Accelerators

Welcome to SCM

What's new in this release

- Windows 8 and IE 10 baselines
- Windows Server 2012 baselines
- Setting library enhancements

How to perform common tasks

- Import a Group Policy Backup
- Customize knowledge
- Export knowledge
- Compare and merge baselines

Working with SCM

- Navigating SCM
- LocalGPO command-line tool
- Setting management

Getting started with SCM

1 Get knowledge

- Download Microsoft baselines automatically
- Download Microsoft baselines manually
- Import a Microsoft baseline
- Import a Group Policy Backup

2 Customize knowledge

- Find settings
- Evaluate Microsoft recommendations
- Customize baselines
- Compare with Microsoft recommendations

3 Export knowledge

- GPO backups
- DCM Configuration Packs

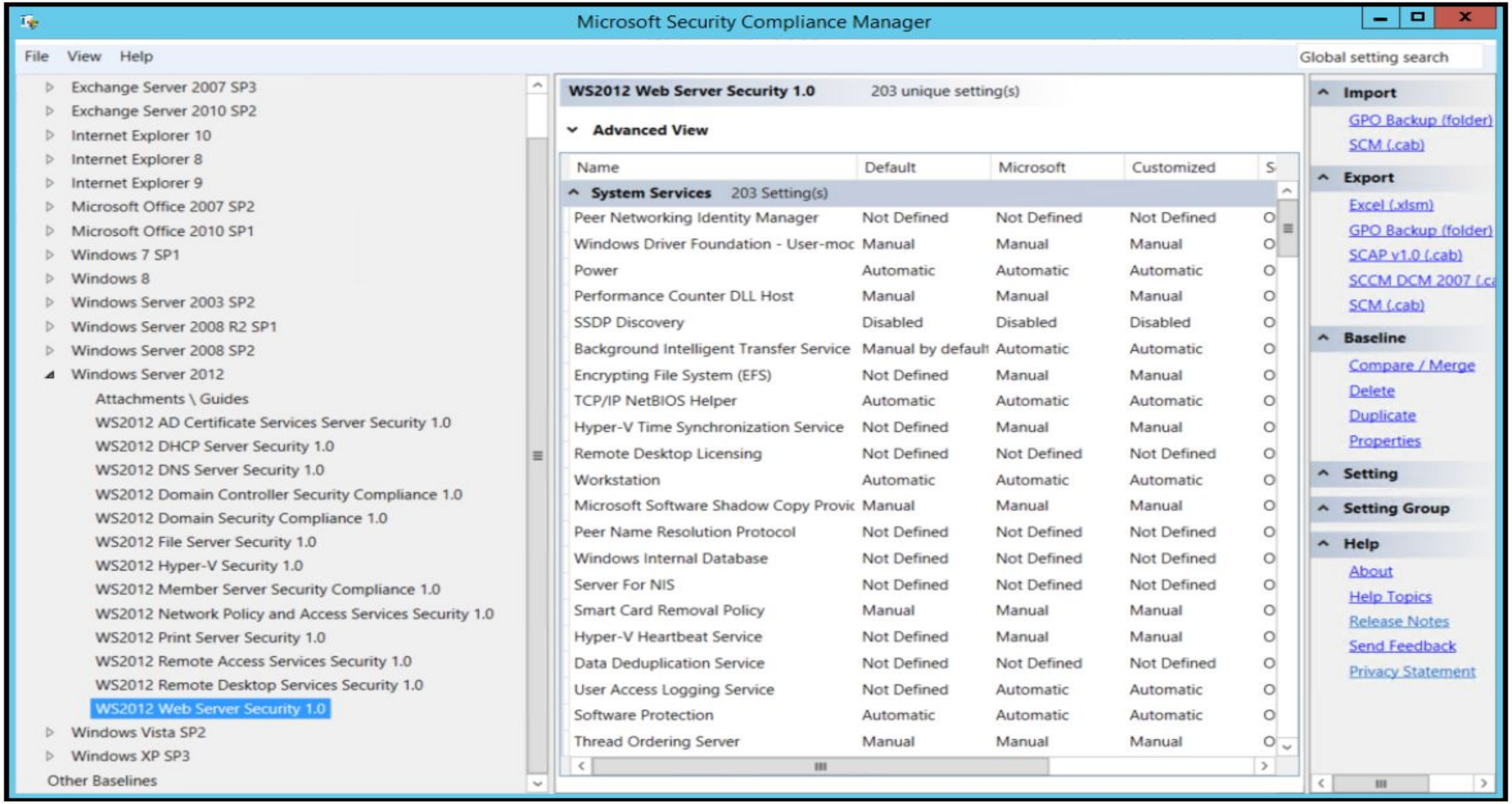
Import

- GPO Backup (folder)
- SCM (.cab)

Help

- About
- Help Topics
- Release Notes
- Send Feedback
- Privacy Statement

Hardening

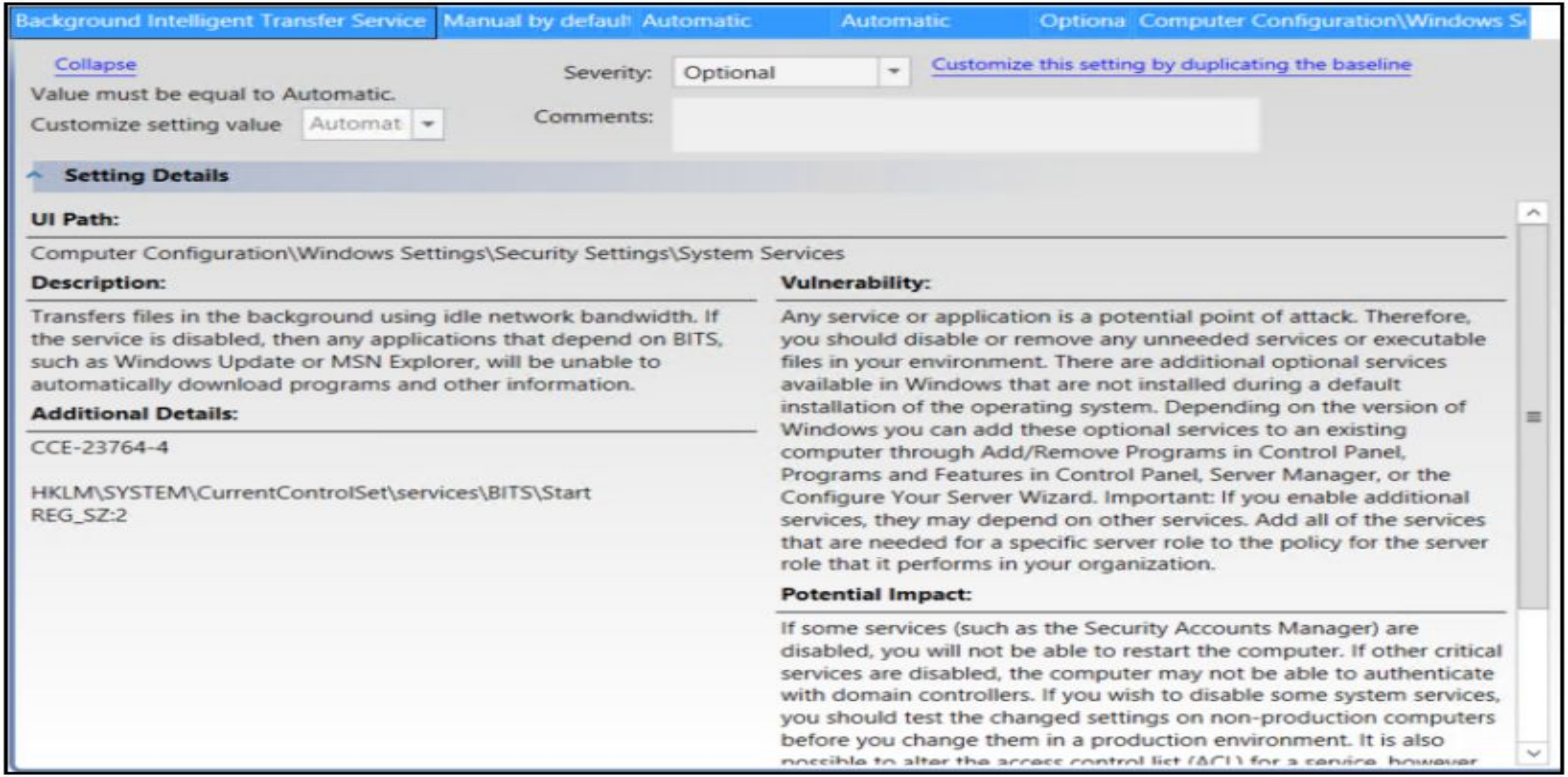

Microsoft Security Compliance Manager
File
View
Help
Global setting search
Exchange Server 2007 SP3
Exchange Server 2010 SP2
Internet Explorer 10
Internet Explorer 8
Internet Explorer 9
Microsoft Office 2007 SP2
Microsoft Office 2010 SP1
Windows 7 SP1
Windows 8
Windows Server 2003 SP2
Windows Server 2008 R2 SP1
Windows Server 2008 SP2
Windows Server 2012
Attachments \ Guides
WS2012 AD Certificate Services Server Security 1.0
WS2012 DHCP Server Security 1.0
WS2012 DNS Server Security 1.0
WS2012 Domain Controller Security Compliance 1.0
WS2012 Domain Security Compliance 1.0
WS2012 File Server Security 1.0
WS2012 Hyper-V Security 1.0
WS2012 Member Server Security Compliance 1.0
WS2012 Network Policy and Access Services Security 1.0
WS2012 Print Server Security 1.0
WS2012 Remote Access Services Security 1.0
WS2012 Remote Desktop Services Security 1.0
WS2012 Web Server Security 1.0
Windows Vista SP2
Windows XP SP3
Other Baselines
Import
GPO Backup (folder)
SCM (.cab)
Export
Excel (.xlsm)
GPO Backup (folder)
SCAP v1.0 (.cab)
SCCM DCM 2007 (.ca
SCM (.cab)
Baseline
Compare / Merge
Delete
Duplicate
Properties
Setting
Setting Group
Help
About
Help Topics
Release Notes
Send Feedback
Privacy Statement

WS2012 Web Server Security 1.0 203 unique setting(s)

Advanced View

Name	Default	Microsoft	Customized	S
System Services 203 Setting(s)				
Peer Networking Identity Manager	Not Defined	Not Defined	Not Defined	O
Windows Driver Foundation - User-moc	Manual	Manual	Manual	O
Power	Automatic	Automatic	Automatic	O
Performance Counter DLL Host	Manual	Manual	Manual	O
SSDP Discovery	Disabled	Disabled	Disabled	O
Background Intelligent Transfer Service	Manual by default	Automatic	Automatic	O
Encrypting File System (EFS)	Not Defined	Manual	Manual	O
TCP/IP NetBIOS Helper	Automatic	Automatic	Automatic	O
Hyper-V Time Synchronization Service	Not Defined	Manual	Manual	O
Remote Desktop Licensing	Not Defined	Not Defined	Not Defined	O
Workstation	Automatic	Automatic	Automatic	O
Microsoft Software Shadow Copy Provic	Manual	Manual	Manual	O
Peer Name Resolution Protocol	Not Defined	Not Defined	Not Defined	O
Windows Internal Database	Not Defined	Not Defined	Not Defined	O
Server For NIS	Not Defined	Not Defined	Not Defined	O
Smart Card Removal Policy	Manual	Manual	Manual	O
Hyper-V Heartbeat Service	Not Defined	Manual	Manual	O
Data Deduplication Service	Not Defined	Not Defined	Not Defined	O
User Access Logging Service	Not Defined	Automatic	Automatic	O
Software Protection	Automatic	Automatic	Automatic	O
Thread Ordering Server	Manual	Manual	Manual	O

Hardening



Background Intelligent Transfer Service	Manual by defaul	Automatic	Automatic	Optiona	Computer Configuration\Windows S

Value must be equal to Automatic.

Customize setting value: Automat

Severity: Optional

Comments:

Setting Details

UI Path:

Computer Configuration\Windows Settings\Security Settings\System Services

Description:

Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information.

Additional Details:

CCE-23764-4

HKLM\SYSTEM\CurrentControlSet\services\BITS\Start
REG_SZ:2

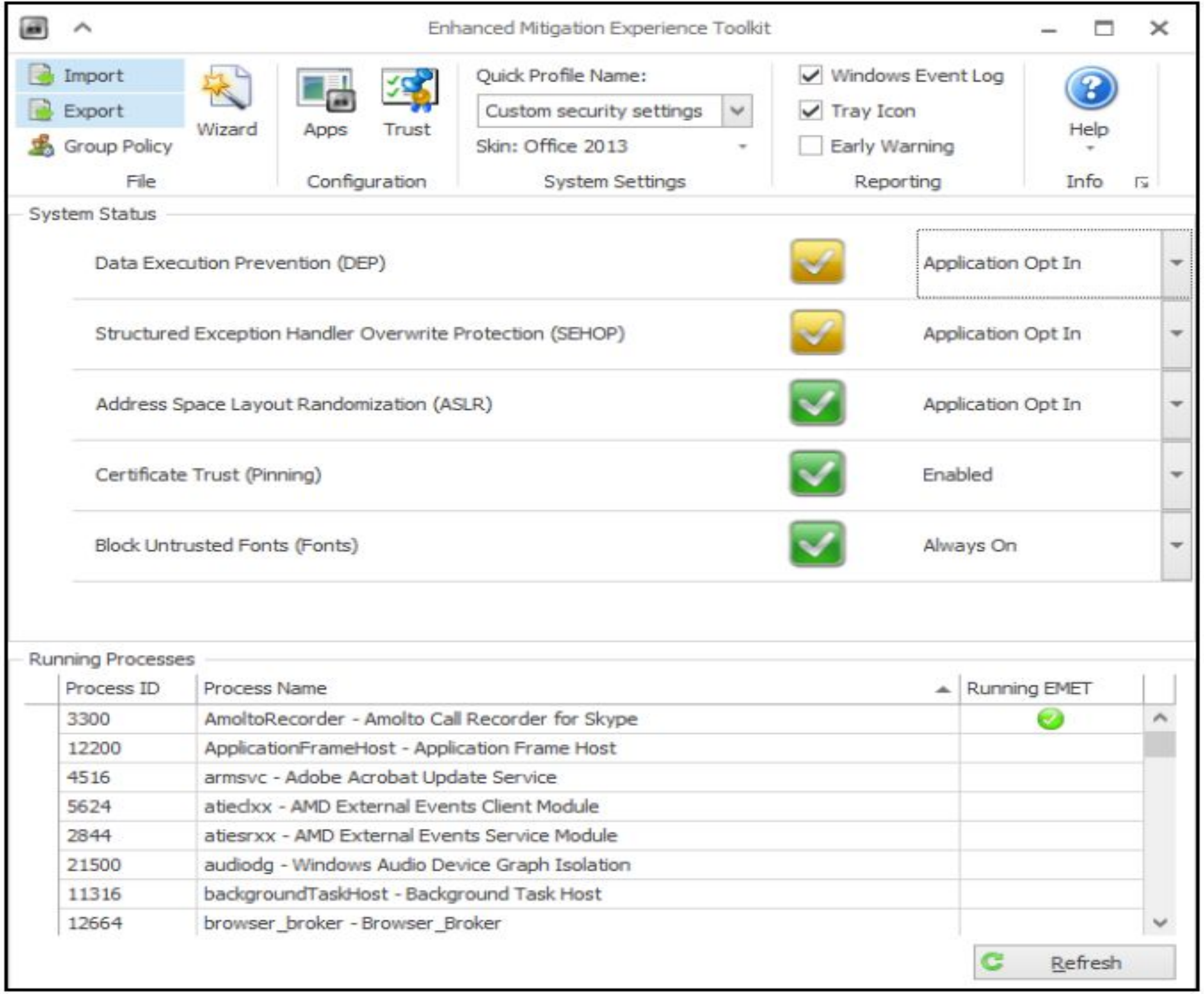
Vulnerability:

Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows that are not installed during a default installation of the operating system. Depending on the version of Windows you can add these optional services to an existing computer through Add/Remove Programs in Control Panel, Programs and Features in Control Panel, Server Manager, or the Configure Your Server Wizard. Important: If you enable additional services, they may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.

Potential Impact:

If some services (such as the Security Accounts Manager) are disabled, you will not be able to restart the computer. If other critical services are disabled, the computer may not be able to authenticate with domain controllers. If you wish to disable some system services, you should test the changed settings on non-production computers before you change them in a production environment. It is also possible to alter the access control list (ACL) for a service, however

Enhanced Mitigation Experience Toolkit (EMET). EMET helps to prevent attackers from gaining access to your computers by anticipating and preventing the most common techniques that attackers are using to exploit vulnerabilities in Windows-based systems.



Quick Profile Name: Custom security settings

Skin: Office 2013

☑ Windows Event Log
☑ Tray Icon
□ Early Warning

System Status

Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled
Block Untrusted Fonts (Fonts)	✓	Always On

Running Processes

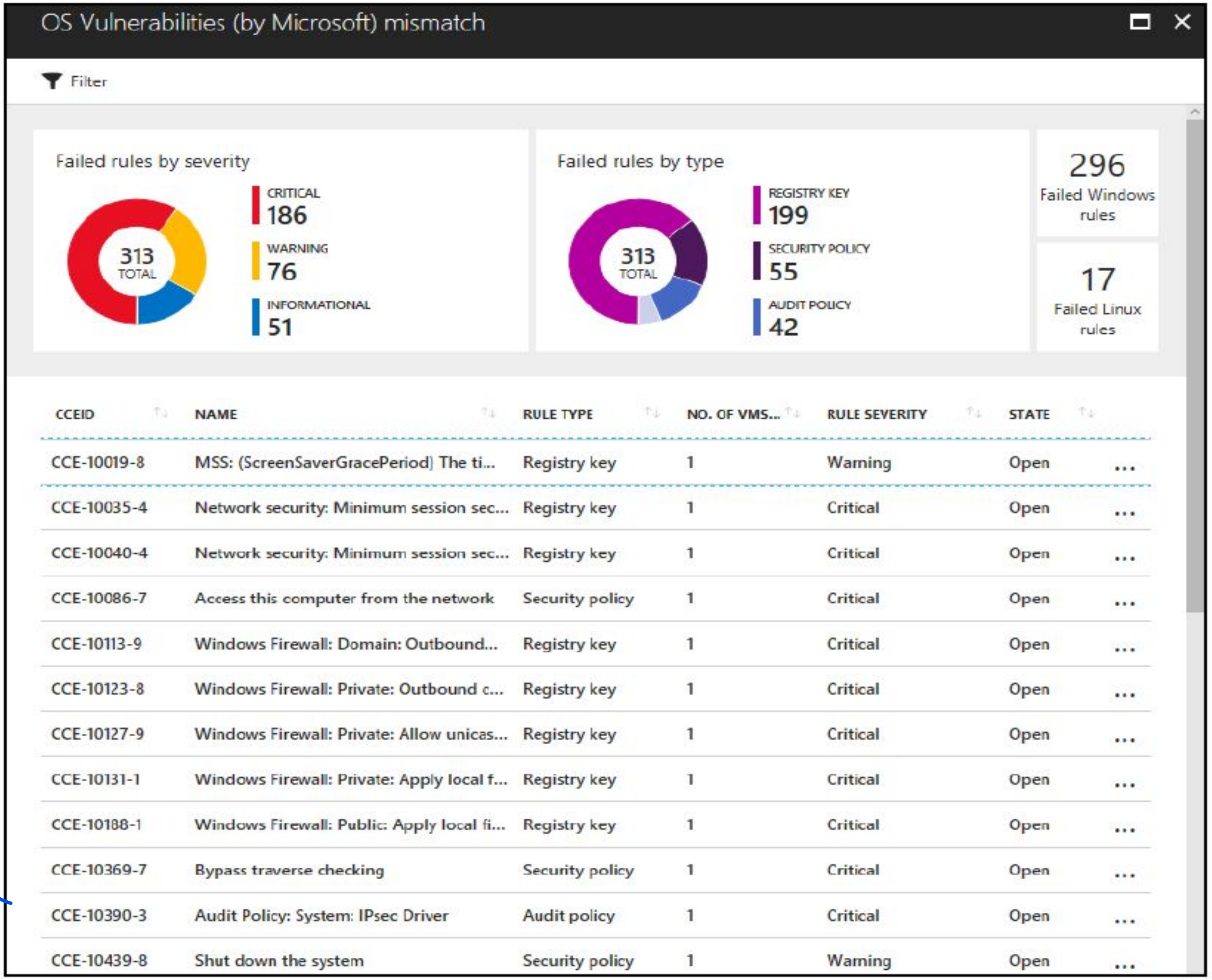
Process ID	Process Name	Running EMET
3300	AmoltoRecorder - Amolto Call Recorder for Skype	✓
12200	ApplicationFrameHost - Application Frame Host	
4516	armsvc - Adobe Acrobat Update Service	
5624	atiedxx - AMD External Events Client Module	
2844	atiesrxx - AMD External Events Service Module	
21500	audiodg - Windows Audio Device Graph Isolation	
11316	backgroundTaskHost - Background Task Host	
12664	browser_broker - Browser_Broker	

Monitoring for Compliance

- While enforcing policies is important to ensure that the upper management's decisions are translated into real actions towards optimizing the security state of your company, monitoring these policies for compliance is also indispensable.

- Policies that were defined based on CCE guidelines can be easily monitored using tools, such as Azure Security Center, which not only monitor Windows VMs and computers, but also those operating with Linux software:

Monitoring for Compliance



OS Vulnerabilities (by Microsoft) mismatch

Filter

Failed rules by severity

313 TOTAL

CRITICAL 186

WARNING 76

INFORMATIONAL 51

Failed rules by type

313 TOTAL

REGISTRY KEY 199

SECURITY POLICY 55

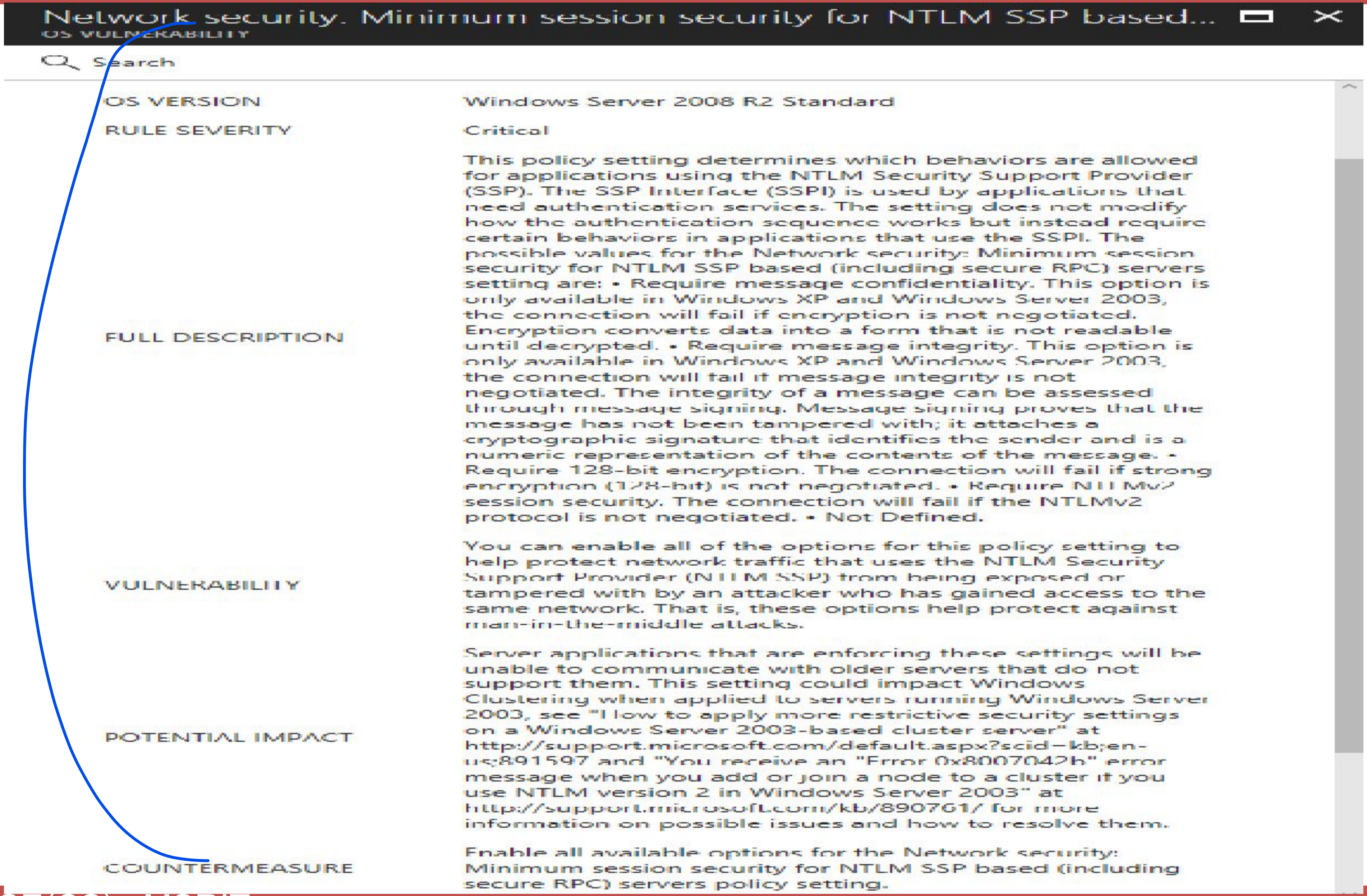
AUDIT POLICY 42

296 Failed Windows rules

17 Failed Linux rules

CCEID	NAME	RULE TYPE	NO. OF VMS...	RULE SEVERITY	STATE	
CCE-10019-8	MSS: (ScreenSaverGracePeriod) The ti...	Registry key	1	Warning	Open	...
CCE-10035-4	Network security: Minimum session sec...	Registry key	1	Critical	Open	...
CCE-10040-4	Network security: Minimum session sec...	Registry key	1	Critical	Open	...
CCE-10086-7	Access this computer from the network	Security policy	1	Critical	Open	...
CCE-10113-9	Windows Firewall: Domain: Outbound...	Registry key	1	Critical	Open	...
CCE-10123-8	Windows Firewall: Private: Outbound c...	Registry key	1	Critical	Open	...
CCE-10127-9	Windows Firewall: Private: Allow unicas...	Registry key	1	Critical	Open	...
CCE-10131-1	Windows Firewall: Private: Apply local f...	Registry key	1	Critical	Open	...
CCE-10188-1	Windows Firewall: Public: Apply local fi...	Registry key	1	Critical	Open	...
CCE-10369-7	Bypass traverse checking	Security policy	1	Critical	Open	...
CCE-10390-3	Audit Policy: System: IPsec Driver	Audit policy	1	Critical	Open	...
CCE-10439-8	Shut down the system	Security policy	1	Warning	Open	...

Monitoring for Compliance



Network security: Minimum session security for NTLM SSP based...

OS VULNERABILITY

OS VERSION	Windows Server 2008 R2 Standard
RULE SEVERITY	Critical
FULL DESCRIPTION	This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are: • Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. • Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. • Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. • Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. • Not Defined.
VULNERABILITY	You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.
POTENTIAL IMPACT	Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.
COUNTERMEASURE	Enable all available options for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers policy setting.

Network Segmentation

- Now it's time to continue with this vision by ensuring that the network infrastructure is secure, and the first step to doing that is to make sure the network is segmented, isolated and that it provides mechanisms to mitigate intrusion.

- The Blue Team must be fully aware of the different aspects of network segmentation, from the physical to the virtual, and remote access.

- Even if companies are not fully cloud-based, they still need to think about connectivity with the cloud in a hybrid scenario, which means that security controls must also be in place to enhance the overall security of the environment, and network infrastructure security is the foundation for that.

Defense in Depth Approach

Defense in depth means having multiple layers of protection and that each layer will have its own set of security controls, which will end up delaying the attack, and that the sensors available in each layer will alert you to whether or not something is happening.

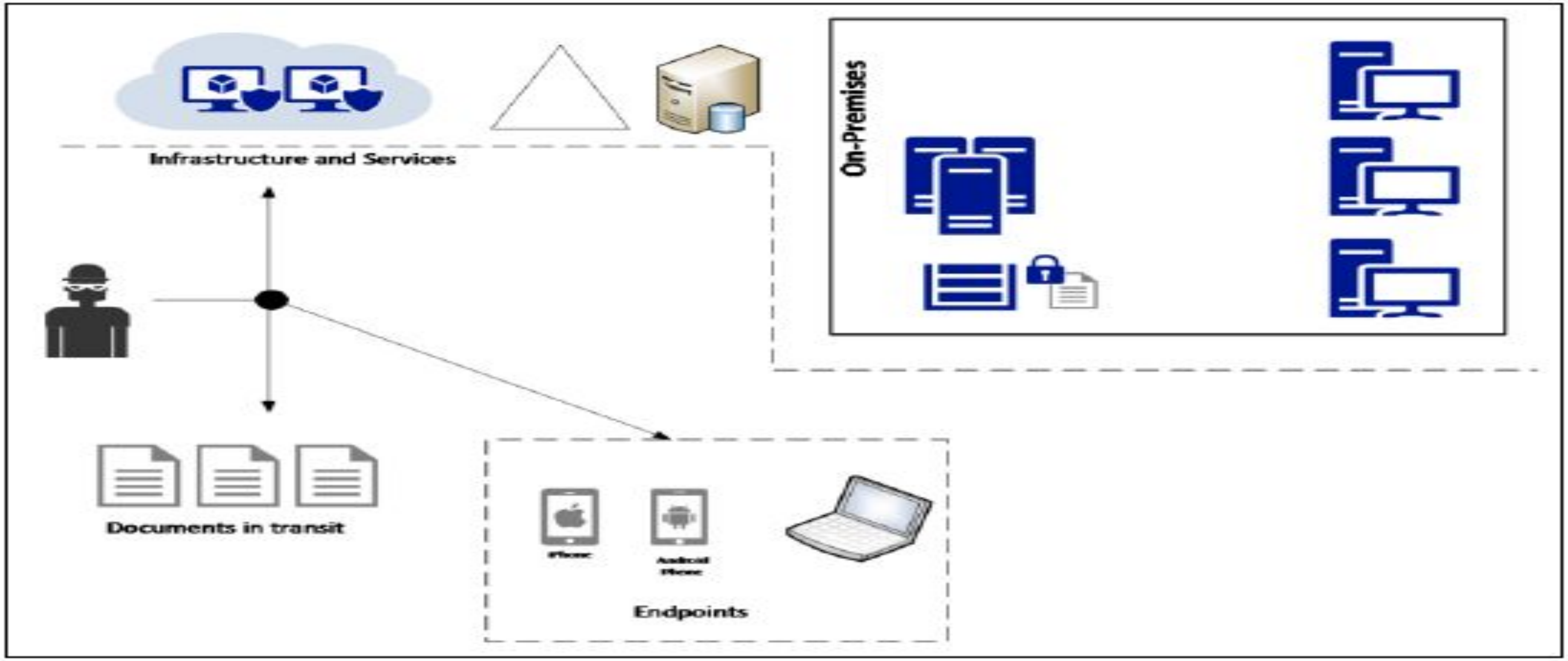


Fig : Defense in Depth

Infrastructure and Services

Attackers can disrupt your company's productivity by attacking its infrastructure and its services.

It is important to realize that even in an on-premises-only scenario, you still have services, but they are controlled by the local IT team.

Your database server is a service: it stores critical data consumed by users, and if it becomes unavailable, it will directly affect the user's productivity, which will have a negative financial impact on your organization.

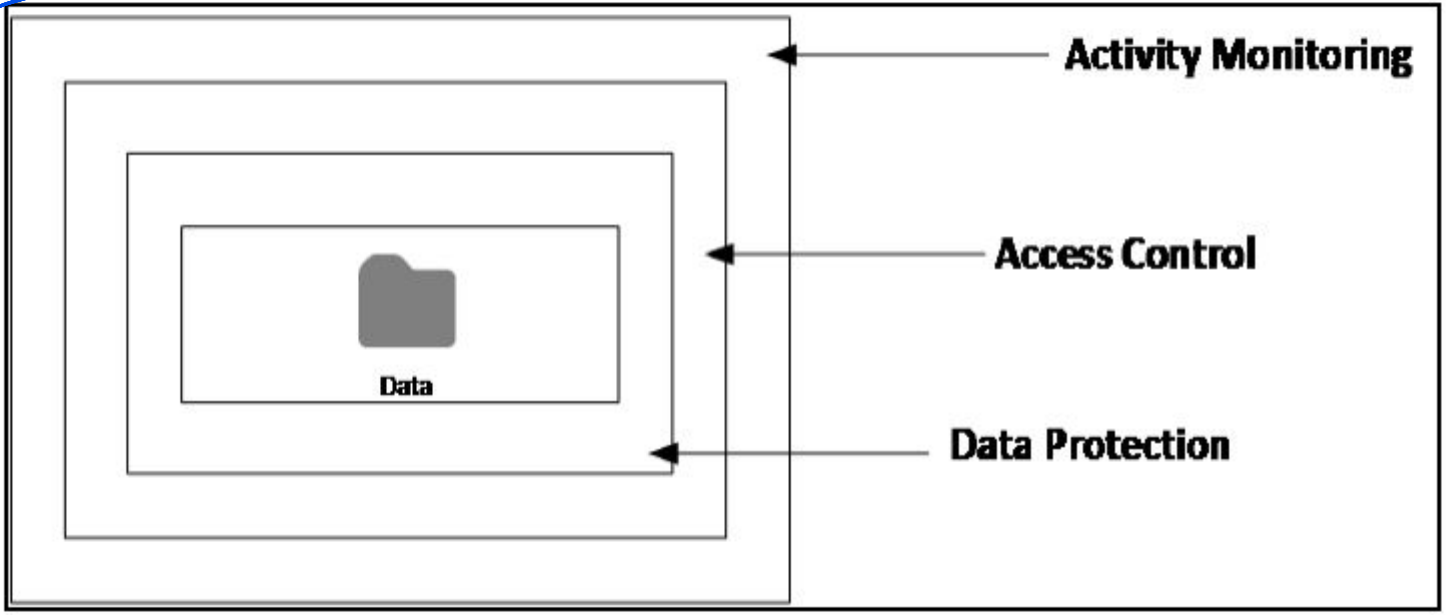
In this case, you need to enumerate all services that are offered by your organization to its end users and partners, and identify the possible attack vectors.

Once you identify the attack vectors, you need to add security controls that will mitigate these vulnerabilities—for example, enforce compliance via patch management, server protection via security policies, network isolation, backups, and so on.

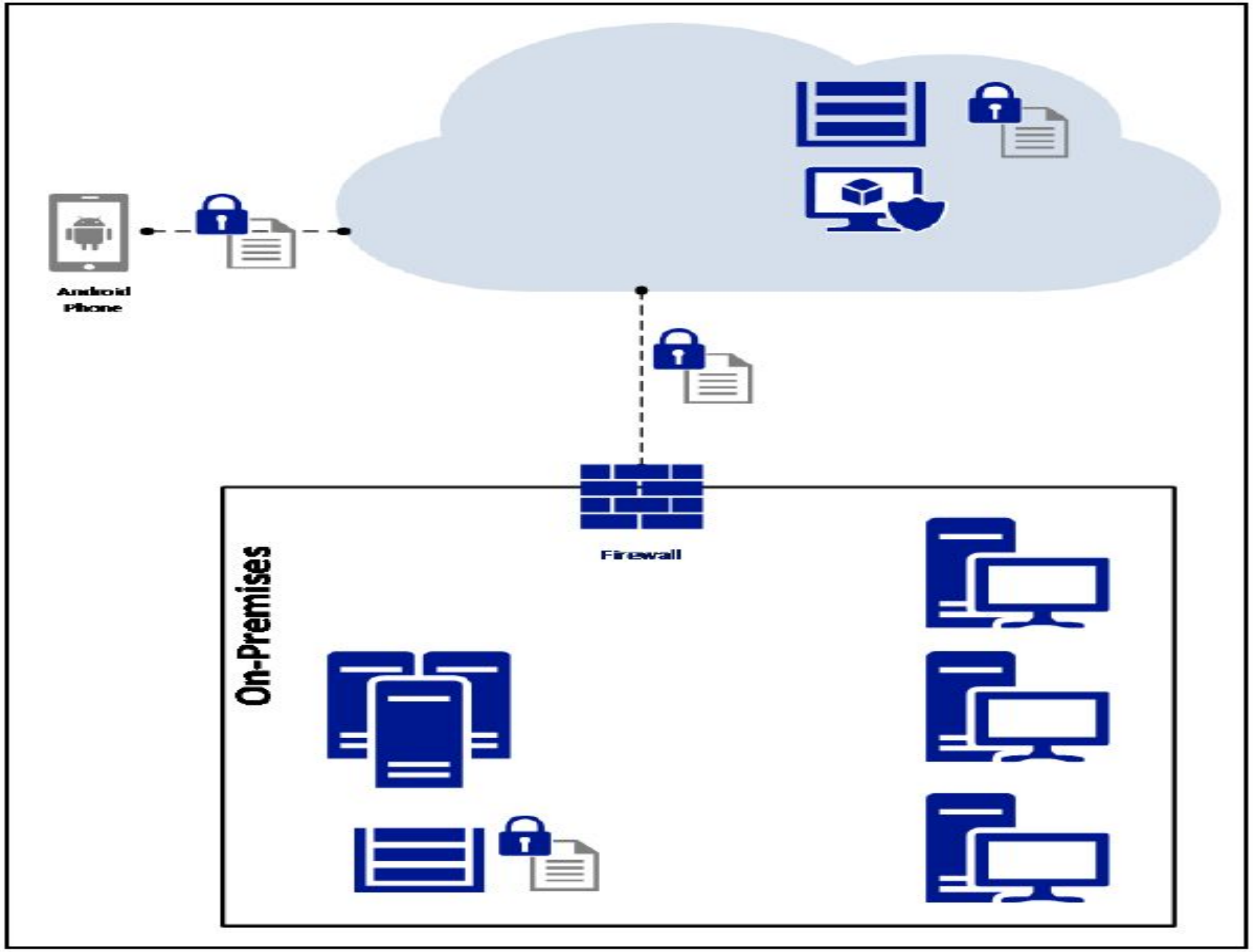
Documents in Transit

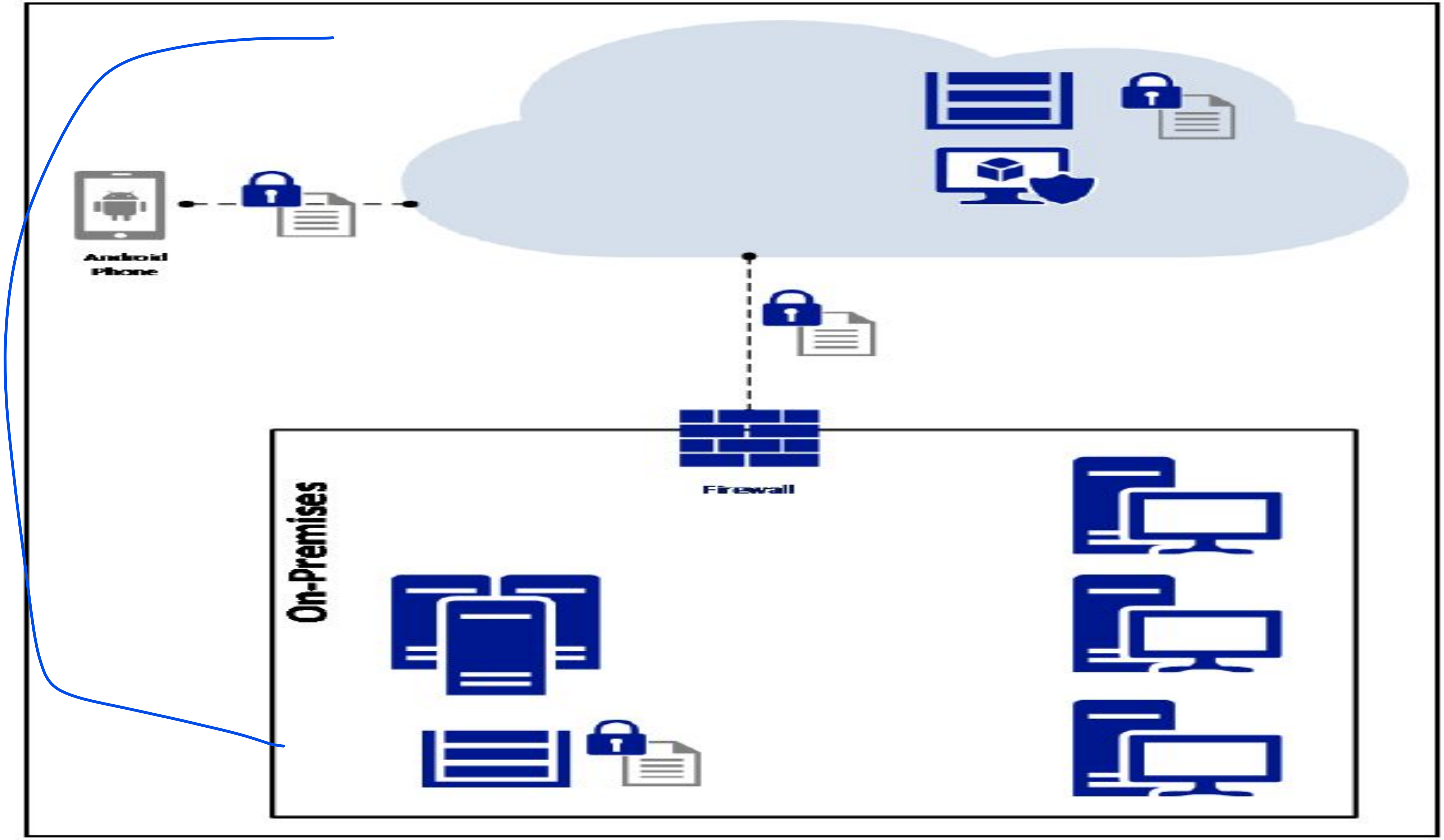
Data is usually vulnerable when it is in transit (from one location to another). Make sure that you leverage encryption to protect data in transit. Encryption in transit is something that should not only be done in public networks—it should also be implemented in internal networks.

Besides encryption, you must also add other security controls for monitoring and access control, as shown in the following diagram



This is an example of a document that was encrypted at rest in a server located on-premises; it traveled via the internet, the user was authenticated in the cloud, and the encryption was preserved all the way to the mobile device that also encrypted it at rest in the local storage:




Android Phone
Firewall
On-Premises

End Points

- When planning defense in depth for endpoints, you need to think beyond computers.
- Nowadays, an endpoint is basically any device that can consume data.
- The application dictates which devices will be supported, and as long as you are working in sync with your development team, you should know what devices are supported.
- In general, most applications will be available for mobile devices, as well as computers. Some other apps will go beyond this, and allow accessibility via wearable devices, such as Fitbit.
- Regardless of the form factor, you must perform threat modeling to uncover all attack vectors and plan mitigation efforts accordingly. Some of the countermeasures for endpoints include:

- Separation of corporate and personal data/apps (isolation)
- Use of TPM hardware protection
- OS hardening
- Storage encryption

Physical Network Segmentation

- Blue Team may face difficulty when dealing with network segmentation is getting an accurate view of what is currently implemented in the network.
- This happens because, most of the time, the network will grow according to the demand, and its security features are not revisited as the network expands.
- For large corporations, this means rethinking the entire network, and possibly rearchitecting the network from the ground up.

Physical Network Segmentation

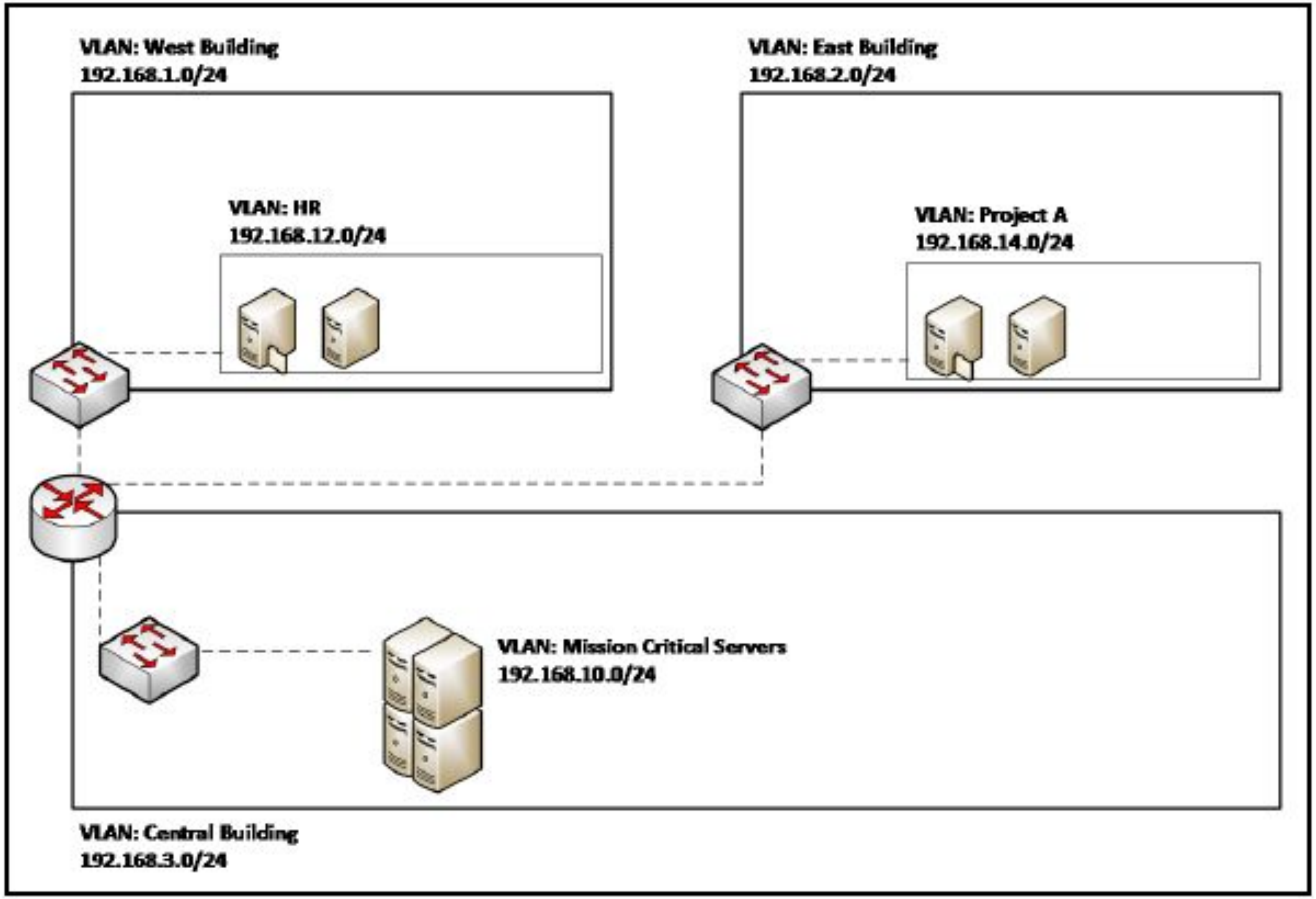
- The first step to establishing an appropriate physical network segmentation is to understand the logical distribution of resources according to your company's needs.

- You must analyze each network case by case, and plan your network segmentation according to the resource demand and logical access.

- For small-and medium-sized organizations, it might be easier to aggregate resources according to their departments—for example, resources that belong to the financial department, human resources, operations, and so on.

- If that's the case, you could create a **virtual local area network (VLAN)** per department and isolate the resources per department. This isolation would improve performance and overall security.

Physical Network Segmentation



Physical Network Segmentation

Some other ways to aggregate resources can be based on the following aspects:

- **Business objectives**: Using this approach, you can create VLANs that have resources based on common business objectives
- **Level of sensitivity**: Assuming that you have an up-to-date risk assessment of your resources, you can create VLANs based on the risk level (high, low, medium)
- **Location**: For large organizations, sometimes it is better to organize the resources based on location
- **Security zones**: Usually, this type of segmentation is combined with others for specific purposes, for example, one security zone for all servers that are accessed by partners

Physical Network Segmentation

In addition, best practices can be used as:

- Use SSH to manage your switches and routers
- Restrict access to the management interface
- Disable ports that are not used
- Leverage security capabilities to prevent MAC flooding attacks
- Leverage port-level security to prevent attacks, such as DHCP snooping
- Make sure that you update the switch's and router's firmware and operating systems

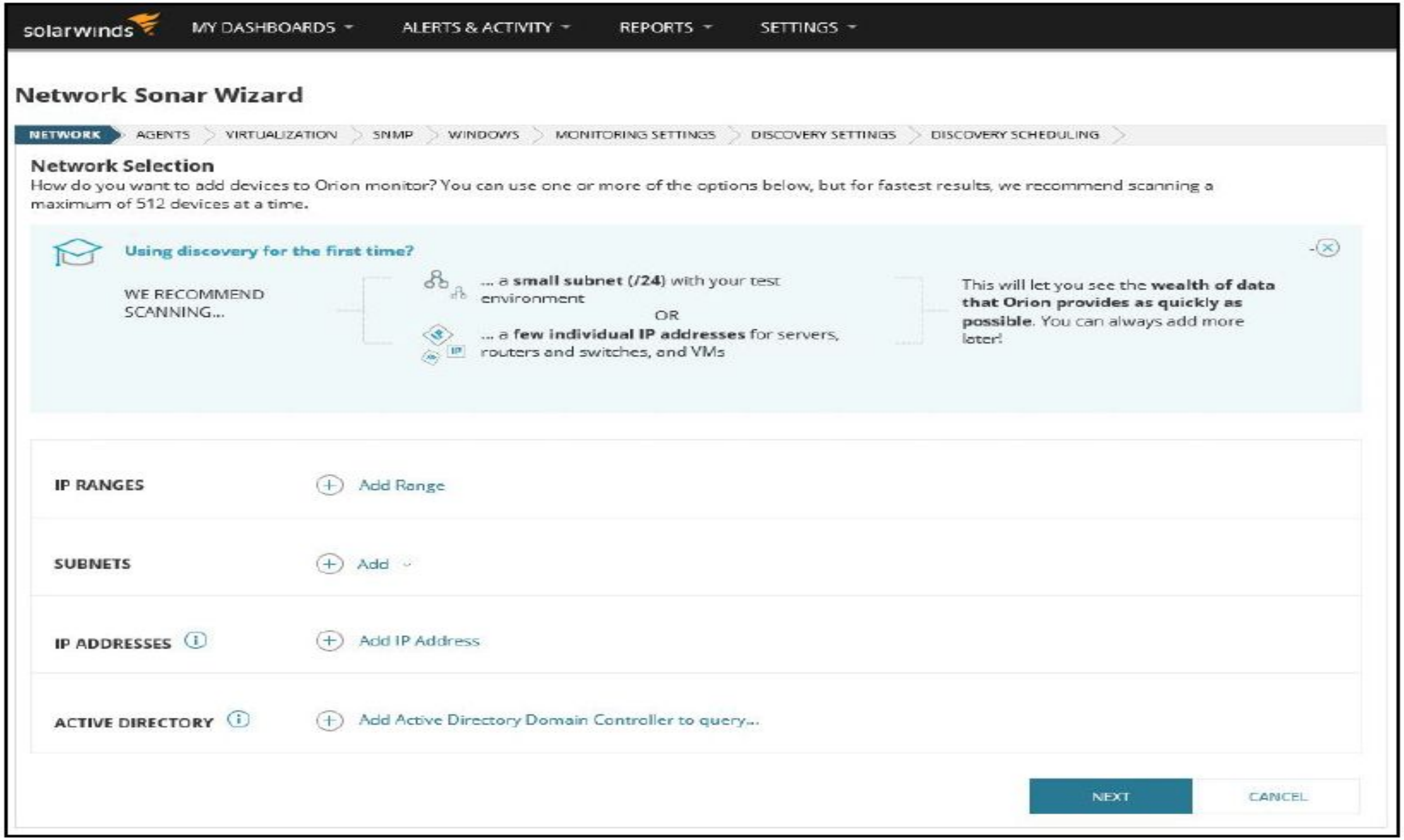
Discovering Your Network

- One challenge that the Blue Team might face when dealing with networks that are already in production is understanding the topology and critical paths, and how the network is organized.

- One way to address this issue is to use a networking map tool that can present the current network state.

- One tool that can help you with that is the **Network Performance Monitor Suite** from Solarwinds. After installing it, you need to launch the network discovery process from the **Network Sonar Wizard**

Discovering Your Network



Network Sonar Wizard

Network Selection

How do you want to add devices to Orion monitor? You can use one or more of the options below, but for fastest results, we recommend scanning a maximum of 512 devices at a time.

Using discovery for the first time?

WE RECOMMEND SCANNING...

... a **small subnet (/24)** with your test environment

OR

... a **few individual IP addresses** for servers, routers and switches, and VMs

This will let you see the **wealth of data that Orion provides as quickly as possible**. You can always add more later!

IP RANGES — Add Range

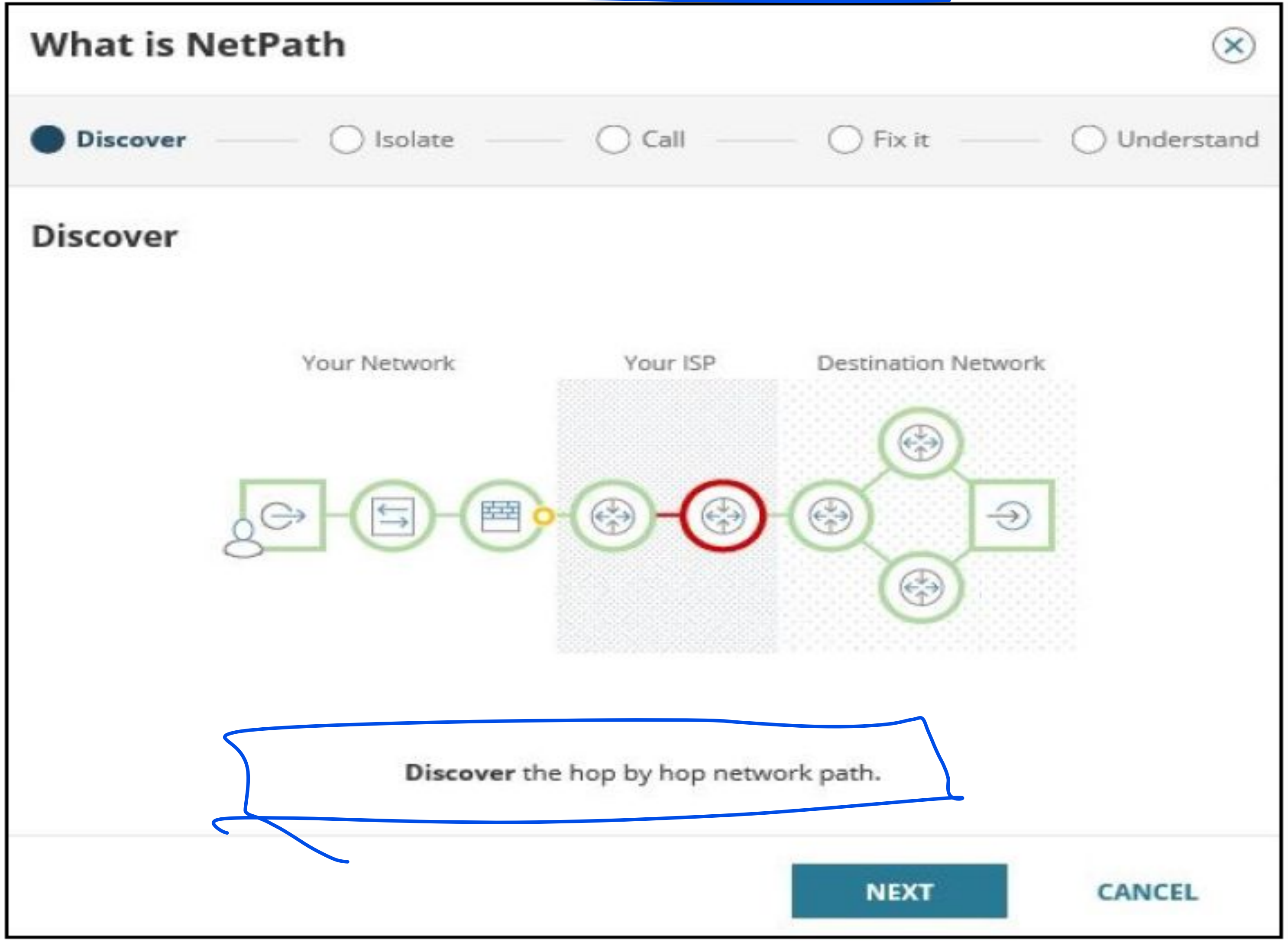
SUBNETS — Add

IP ADDRESSES — Add IP Address

ACTIVE DIRECTORY — Add Active Directory Domain Controller to query...

Discovering Your Network

You need to fill in all these fields before you click **NEXT**, and once you finish, it will start the discovery process. At the end, you can verify your NetPath, which shows the entire path between your host and the internet:



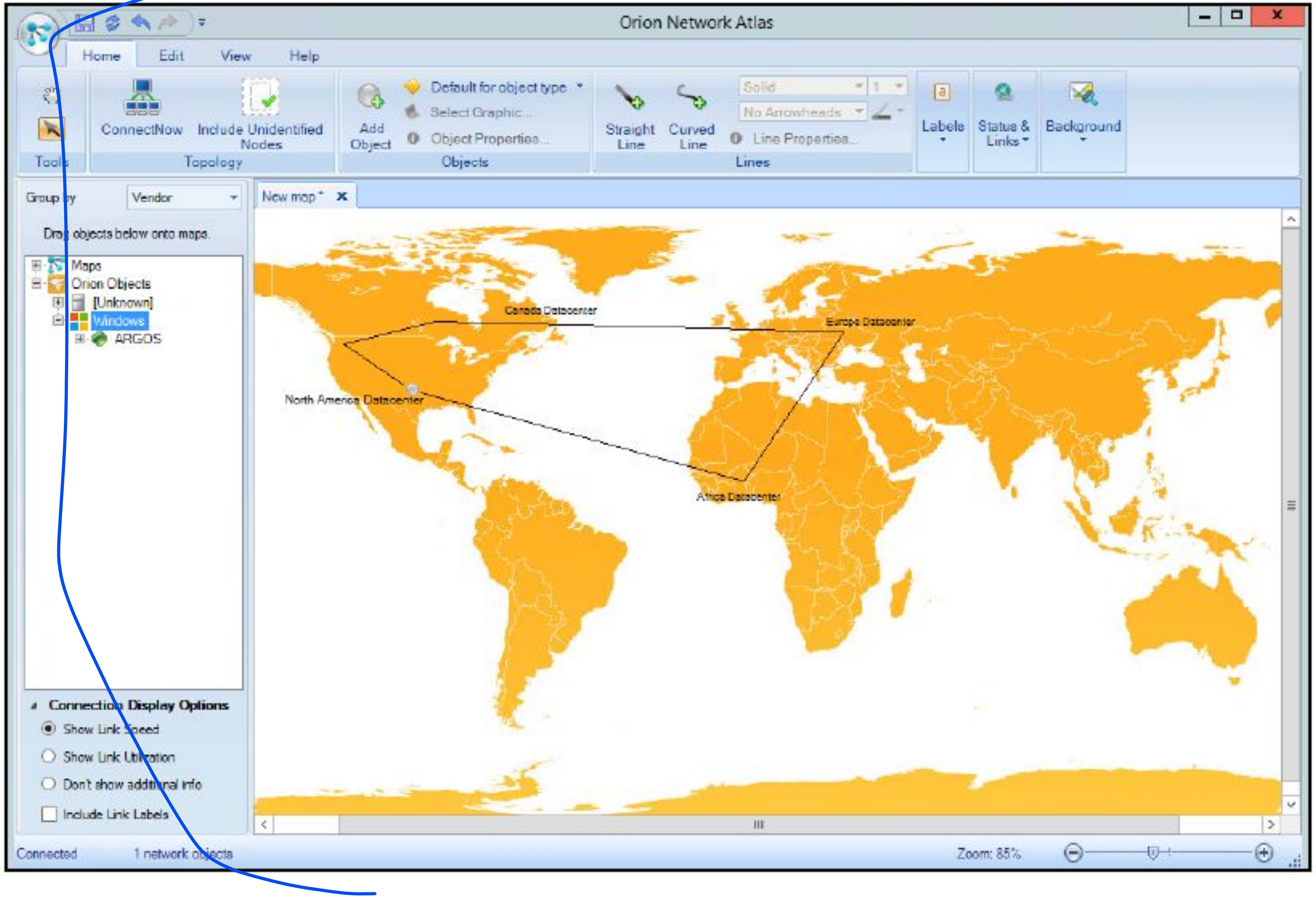
What is NetPath

● Discover ○ Isolate ○ Call ○ Fix it ○ Understand

Discover

Discover the hop by hop network path.

Discovering Your Network



Group by: Vendor

Connection Display Options

● Show Link Speed

○ Show Link Utilization

○ Don't show additional info

□ Include Link Labels

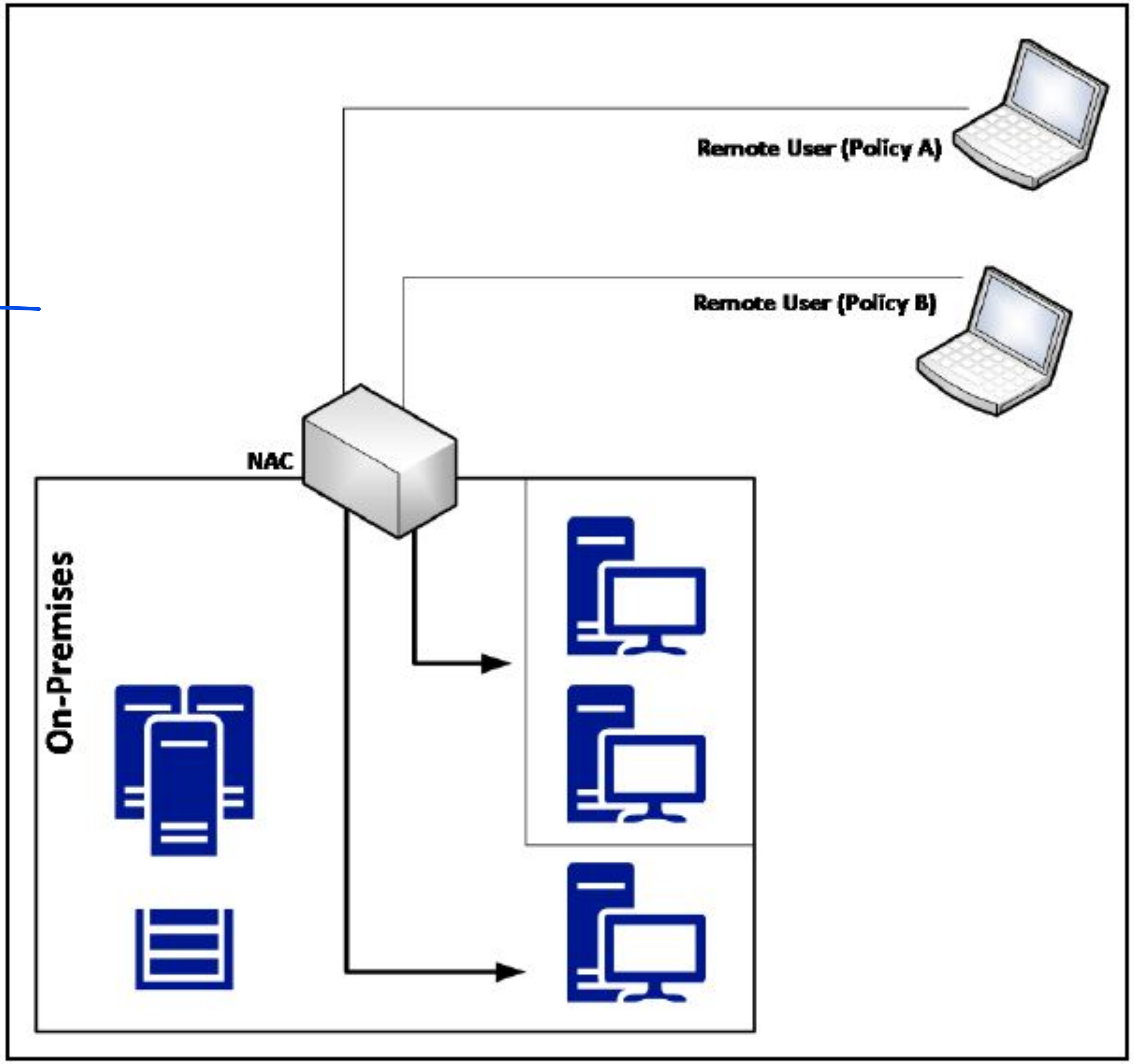
Securing Remote access to the Network

Securing Remote access to network evaluation includes following details

- That the remote system has the latest patches
- That the remote system has antivirus enabled
- That the remote system has a personal firewall enabled
- That the remote system is compliant with mandate security policies

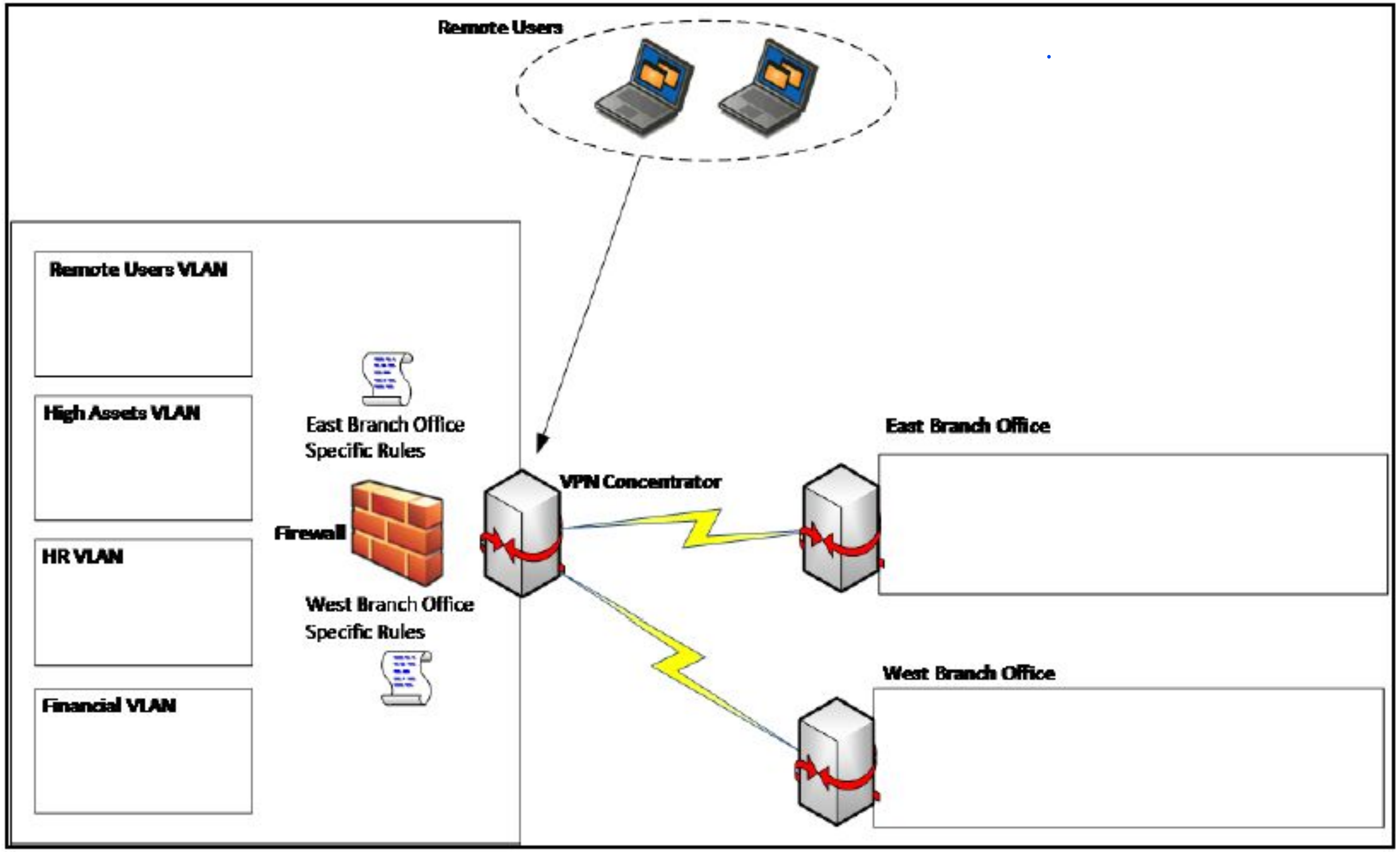
Securing Remote access to the Network

Network Access Control



Site to Site VPN

A site-to-site virtual private network (VPN) refers to a connection set up between multiple networks. This could be a corporate network where multiple offices work in conjunction with each other or a branch office network with a central office and multiple branch locations.



Site to Site VPN

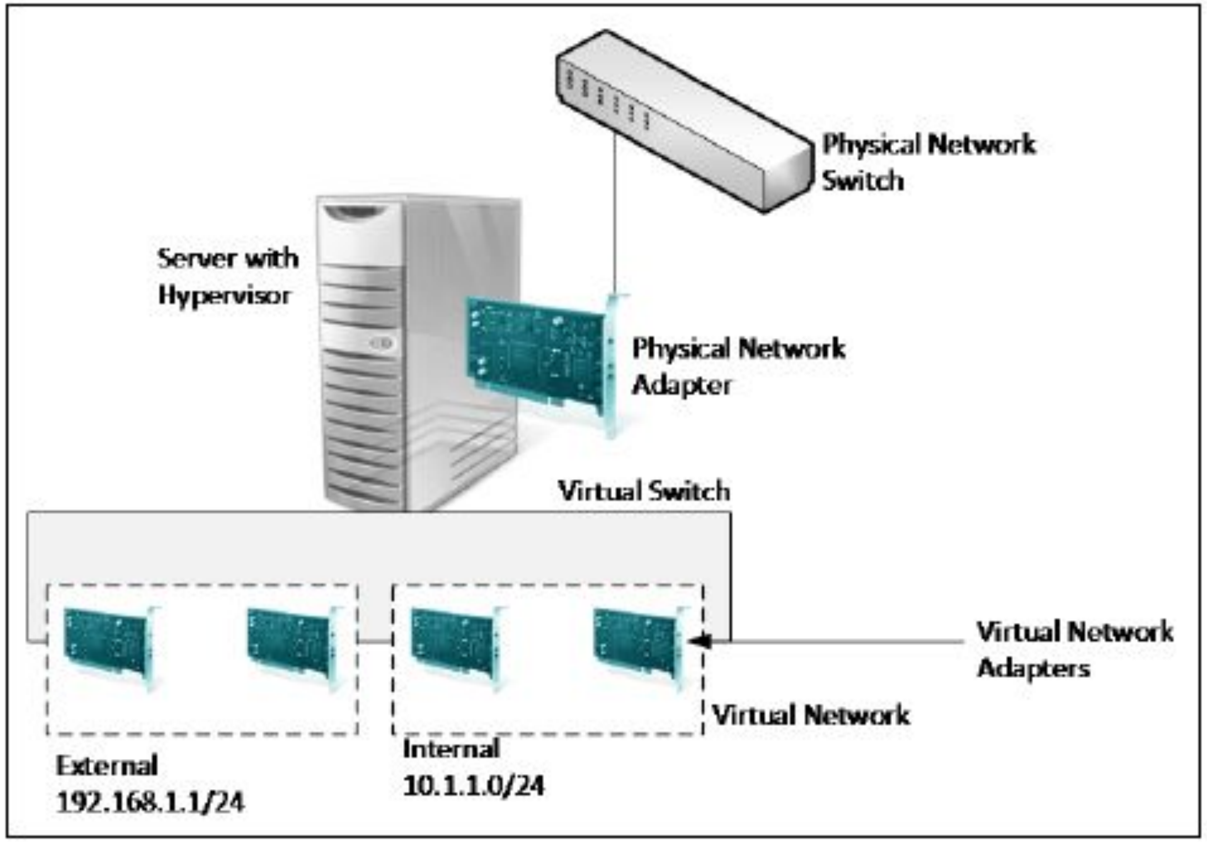
- Site-to-site VPNs are useful for companies that prioritize private, protected traffic and are particularly helpful for organizations with more than one office spread out over large geographical locations.

- These businesses often have to access resources housed on a primary network, which could include servers that facilitate email or store data.

- In some instances, a server may be the operational hub of an application essential to the company's business.

- A site-to-site VPN can, in that case, give all sites full access to the application—as if it were housed within their physical facility.

Virtual Segmentation



Virtual Segmentation

- When planning your virtual network segmentation, you must first access the virtualization platform to see which capabilities are available.

- Note that there is isolation within the virtual switch; in other words, the traffic from one virtual network is not seen by the other virtual network.

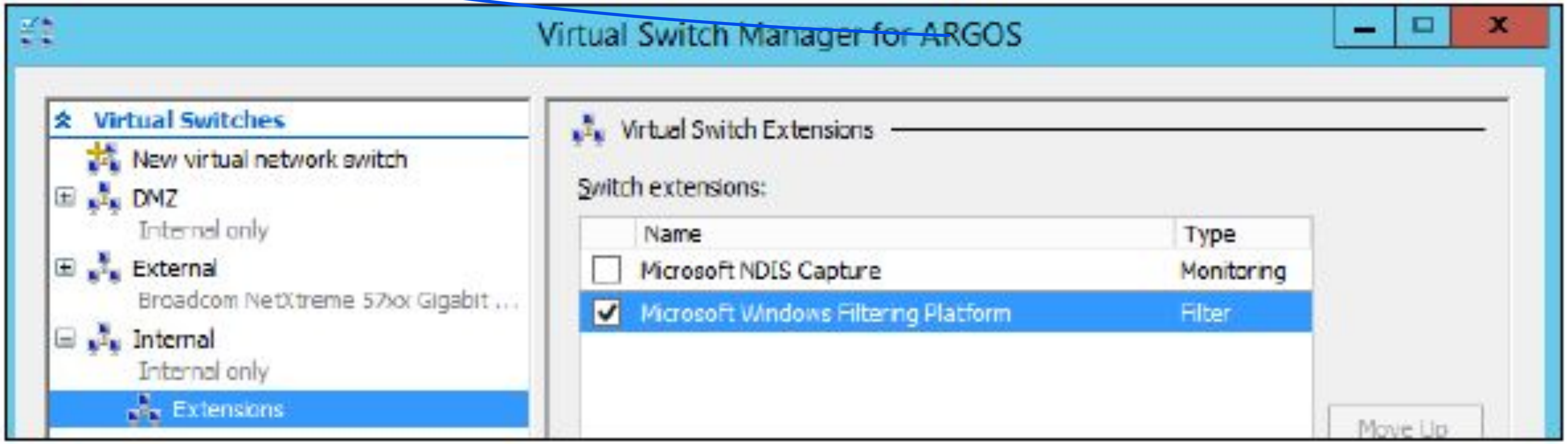
- Each virtual network can have its own subnet, and all virtual machines within the virtual network will be able to communicate among themselves, but it won't traverse to the other virtual network.

- To enhance Network Security:

1. Network packet inspection
2. Intrusion detection or firewall
3. Network packet filter

Virtual Segmentation

The below figure shows, how extension images are located



Virtual Switch Manager for ARGOS
Virtual Switches
New virtual network switch
DMZ
Internal only
External
Broadcom NetXtreme 57xx Gigabit ...
Internal
Internal only
Extensions
Virtual Switch Extensions
Move Up

Switch extensions:

	Name	Type
☐	Microsoft NDIS Capture	Monitoring
☑	Microsoft Windows Filtering Platform	Filter

Virtual Segmentation

- Oftentimes the traffic that originated in one VM can traverse to the physical network and reach another host connected to the corporate network.
- So it is important to always think that, although the traffic is isolated within the virtual network, if the network routes to other networks are defined, the packet will still be delivered to the destination.

- Enable the following capabilities in your virtual switch:

1. **MAC address spoofing**: This prevents malicious traffic from being sent from a spoof address
2. **DHCP guard**: This prevents virtual machines from acting or responding as a DHCP server
3. **Router guard**: This prevents virtual machines from issuing router advertisement and redirection messages
4. **Port ACL (access control list)**: This allows you to configure specific access control lists based on MAC or IP addresses

Hybrid Cloud Security

According to McAfee's report, *Building Trust in a Cloudy Sky*, released in April 2017, hybrid cloud adoption grew three times in the previous year, which represents an increase from 19% to 57% of the organizations that were surveyed.

In a nutshell, it is realistic to say that your organization will have some sort of connectivity to the cloud sooner or later, and according to the normal migration trend, the first step is to implement a hybrid cloud.

Hybrid Cloud Security

When designing your hybrid cloud network, you need to take everything that was previously explained into consideration and plan how this new entity will integrate with your environment.

Many companies will adopt the site-to-site VPN approach to directly connect to the cloud and isolate the segment that has cloud connectivity. While this is a good approach, usually site-to-site VPN has an additional cost and requires extra maintenance. Another option is to use a direct route to the cloud, such as the Azure ExpressRoute.