Cloud **Security** Assessment

Methodology and Overview

Environment Reviewed

- 34 Windows Servers
- 4 Linux Servers
- 123 Clients
- 92% of Active Directory reported devices

Methodology Used

- **Discover** the presence and specifications of current on-prem and cloud environment
- **Identify** security or supportability concerns and how they might apply to the Zero Trust framework
- **Interview** stakeholders to assess additional details and requirements

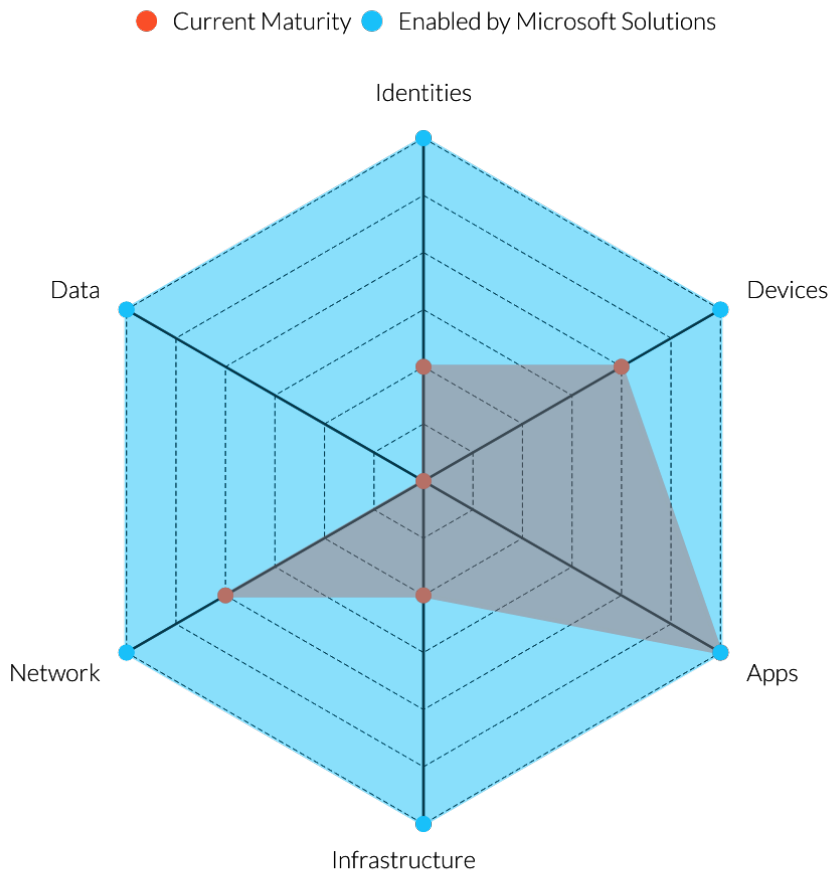
Deliverables Included

- Identified risks and considerations
- General remediation recommendations where applicable
- Available Microsoft solutions that can enable cybersecurity maturity

Please Note

Microsoft does not guarantee nor imply compliance in the Zero Trust or any other Cybersecurity Framework. Recommendations do not imply coverage of respective controls as they are often one of several courses of action for approaching requirements which is unique to each customer. Recommendations should be considered a starting point for planning full or partial coverage of respective control requirements.

Key Observations



Current Security	• 120 endpoints were detected without Endpoint Protection • 7 endpoints were detected with exposures to Ransomware attacks • 42 endpoints were detected with vulnerabilities to RDP-borne attacks • 403 security vulnerabilities of moderate to high severity were detected at the application layer
Standardization & Supportability	• By 2023, 67% of the Windows servers in the environment will be out of support. • 2 versions of Windows server detected in the environment are beyond mainstream support. • By 2023, 100% of the SQL servers in the environment will be out of support. • 1 different versions of SQL were observed in use in the environment.
Tools and Readiness	• 4 Threat Management tools were observed in use • 0 Systems Management tools were observed in use • Data Loss Prevention was not enabled in Microsoft 365
General Maturity	• Formally gauge your current Zero Trust maturity with a partner-led engagement • Leveraging the included recommendations will assist in enabling the controls you require for cybersecurity maturity

Azure Security Center Secure Score

Did You Know?

Microsoft noted these areas of improvement to increase your security posture.

Control Area	Score Impact
Ensure all users can complete multi-factor authentication for secure access	+9.47%
Enable policy to block legacy authentication	+8.42%
Turn on sign-in risk policy	+7.37%
Turn on user risk policy	+7.37%
Install Defender for Identity Sensor on all Domain Controllers	+4.21%
Do not allow users to grant consent to unmanaged applications	+4.21%
Set automated notifications for new OAuth applications connected to your corporate environment	+4.21%
Set automated notifications for new and trending cloud applications in your organization	+3.16%
Use Cloud App Security to detect anomalous behavior	+3.16%
Restrict unauthorized network access	+2.11%

Your current Secure Score is

39%

or 21 of 55 possible points

There are

15

Risks currently unaddressed

You could improve your score by

37%

By actioning the top 5 recommendations

This Matters Because...

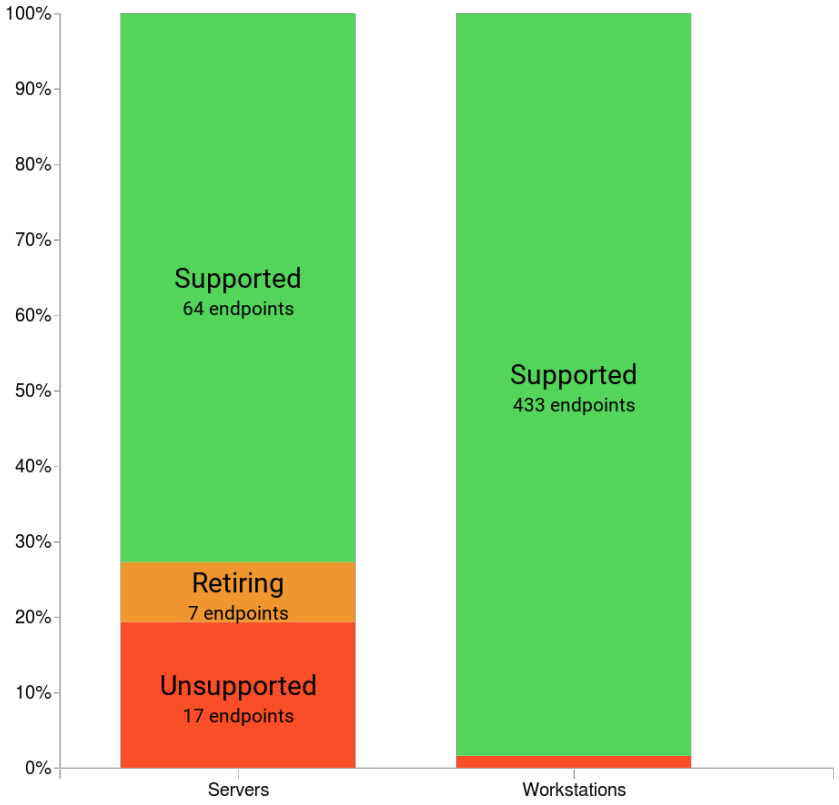
Following these recommendations will ensure that you're following best practices, as well as providing prescriptive guidance on fixing common misconfigurations and overlooked security control points.

...Have You Considered?

By following the guidance provided by the Secure Score, you can customize your security policy to focus on what you need to..

The Microsoft Secure Score will also allow you to gain visibility across your environment to verify compliance with regulatory requirements, such as CIS, PCI DSS, SOC, and ISO.

Supportability: Desktop Operating Systems



Did You Know?

- 24 workstations are running an unsupported operating system
- 7 workstations are running an operating system with an upcoming end-of-support event in the next year

This Matters Because...

Endpoints outside of extended support will no longer receive security or functionality updates—even those deemed critical. Windows XP is no longer receiving updates, and as of January, 2020 neither will Windows 7.

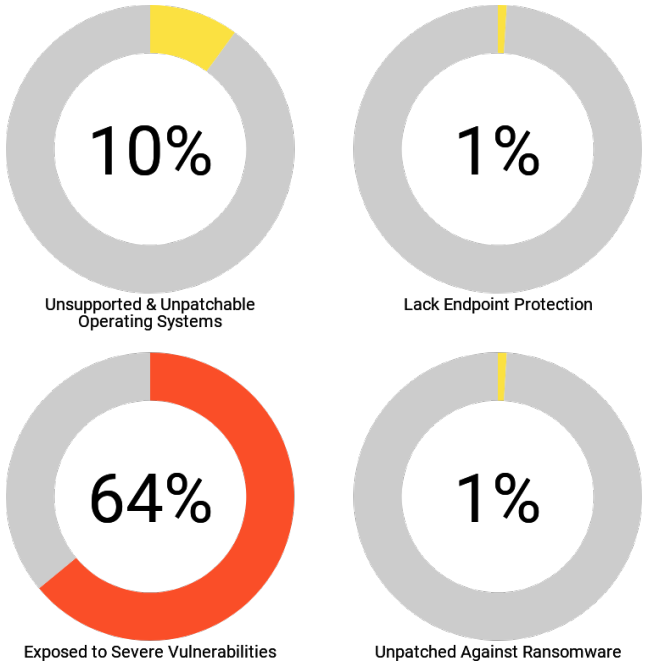
...Have You Considered?

- Windows 7 machines that are present due to older hardware should be targeted for replacement
- Microsoft 365 provides access to the most current desktop operating systems, and would help keep your organization up-to-date
- In addition to remaining current, ongoing patching of both mobile and local desktops through technologies such as Endpoint Configuration Manager and Endpoint Manager are a key first-line defense against new threats

Device and Application Security

Did You Know?

48 vulnerabilities of Severity 9.0 or higher were detected on the desktops, servers, and bare metal host operating systems in the environment.



This Matters Because...

Many high profile exploits—such as the Solarwinds breaches of 2021—were made possible by a lack of application-level patching. A healthy patch management regimen and more tightly managed standardization can greatly reduce the likelihood of an exploit.

There were **48** vulnerable vendors detected in your environment

The average vulnerability severity was **9.3** on the Common Vulnerability Scoring System scale

Your threat profile could be reduced by **64%** through patching and standardization

...Have You Considered?

- Leveraging application patching tools such as Microsoft Endpoint Manager to ensure your client applications are up to date and properly patched
- Defender for Endpoint can assist in detecting and blocking vulnerabilities from being acted upon

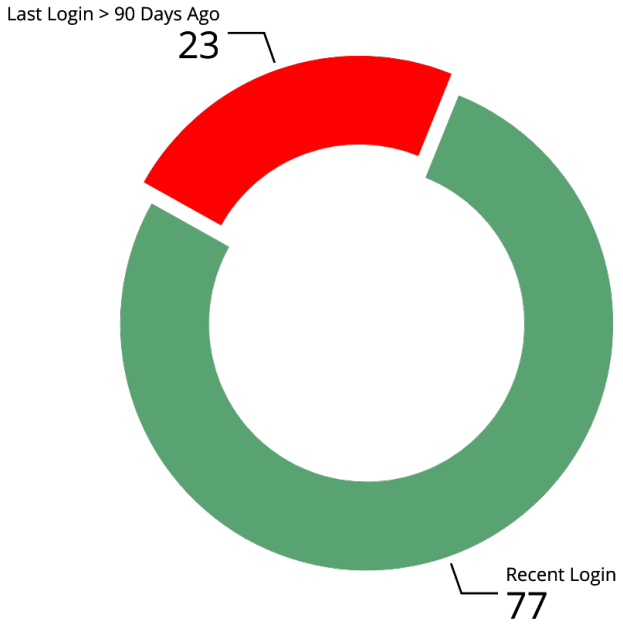
Get There Fast

Detect malicious traffic & vulnerabilities & patch endpoints automatically: Schedule a security workshop today.

Organizational Security: Active Directory Accounts

Did You Know?

23 accounts with no recent activity were observed to remain active and available for use.



This Matters Because...

User accounts that are no longer in use should be deactivated, to prevent them from potentially being leveraged by threat actors.

There are **63** Accounts able to operate without a password

There are **173** Accounts with non-expiring passwords but no recent activity

There are **225** Accounts with passwords that have not changed in 2+ years

...Have You Considered?

- Conducting regular clean-up of Active Directory accounts
- Leveraging Azure Active Directory rules to ensure accounts are properly retired when no longer required

Security Profile: Coverage by Function

Threat Protection	Information Protection	Identity & Access Management
ESET	ESET	Cisco
Microsoft		
Fortinet		
Malwarebytes		
$8,373.99 spent per year	**$1,650.00 spent per year**	**$864.00 spent per year**

Did You Know?

- 6 security products from 5 different vendors were observed in use.

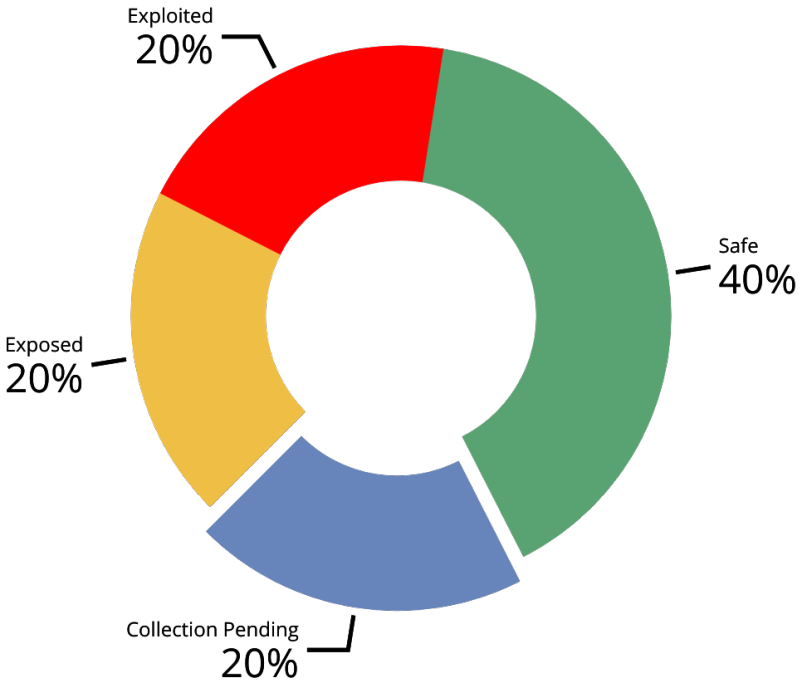
This Matters Because…

$10,878 in security products currently in use could be replaced with comparable offerings from Microsoft.

…Have You Considered?

- Microsoft 365 E5 is capable of providing a complete security solution

Security Profile: Exchange "ProxyLogon" Exploit



Did You Know?

- 2 Exchange Servers appear to be exposed to the ProxyLogon vulnerability allowing privilege escalation without authentication on vulnerable Exchange servers
- 1 Exchange Servers appear to have been exploited by this vulnerability

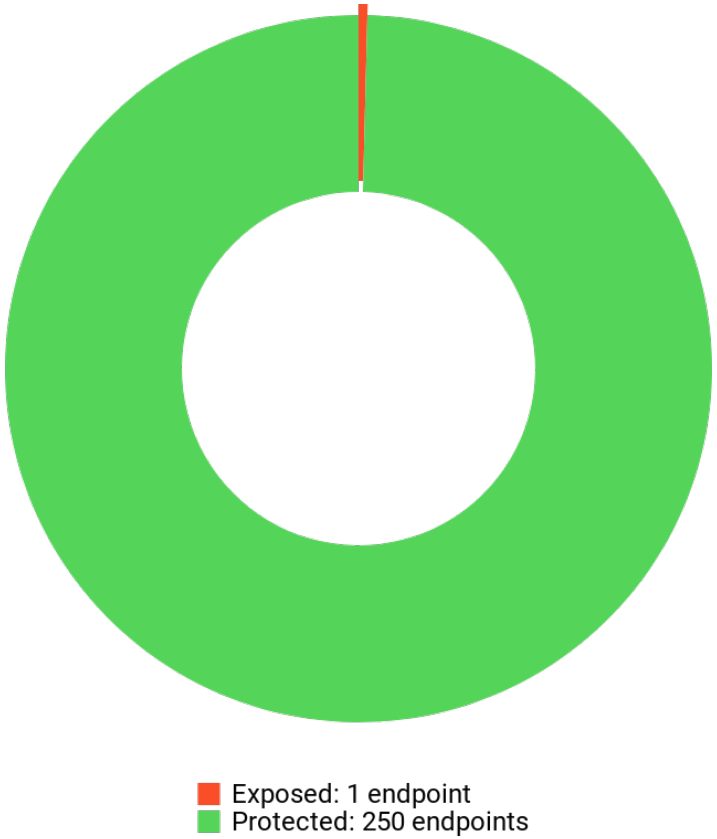
This Matters Because…

ProxyLogon is being used to exfiltrate data from organizations, or in some cases, leverage encryption to render machines unusable. Such attacks can leave an organization unable to function, with the only option often being rolling back to previous backups.

…Have You Considered?

- Endpoint Manager can assist in patching operating systems in the environment
- Microsoft Defender ATP can assist in detecting and prioritizing previously unseen attack variants
- Exchange Online coupled with Defender for Office 365 can be quite useful in preventing similar attacks from succeeding

Security Profile: BlueKeep / RDP Exposure



Did You Know?

- 1 machines are currently exposed to BlueKeep, an RDP-delivered exploit that allows remote code execution or even the complete takeover of an unprotected system.

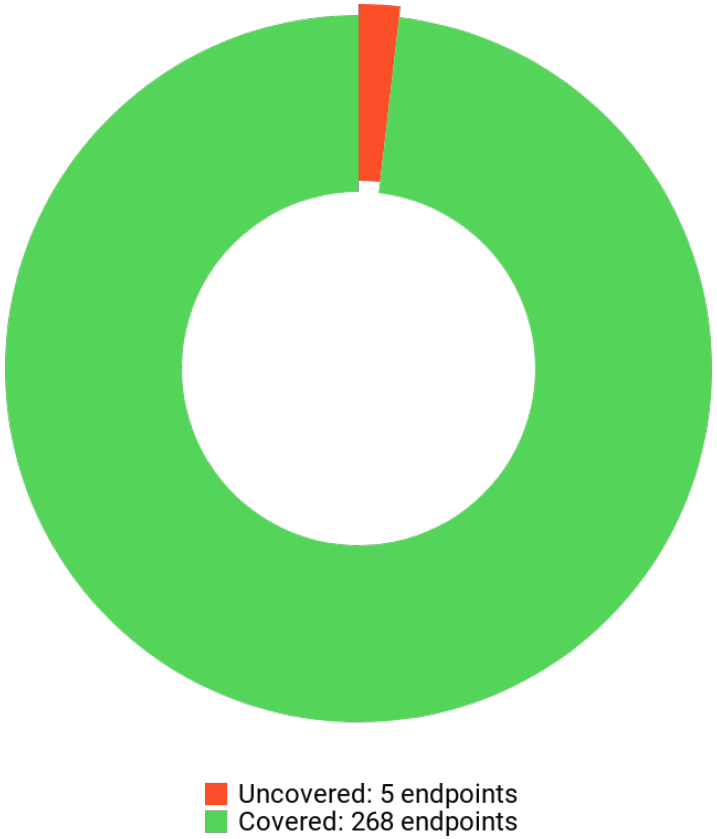
This Matters Because...

Users from outside your network could leverage this exploit via Remote Desktop Services and gain elevated privileges, carry out damaging internal attacks, or remove sensitive data.

...Have You Considered?

- Disabling any unnecessary RDP access and sandboxing / airgapping relevant machines where possible
- Operating System patching is the first line of defense against attacks such as BlueKeep
- Endpoint Manager can assist in patching operating systems in the environment
- Microsoft Cloud App Security can assist in detecting and prioritizing previously unseen attack variants

Security Profile: Threat Management



Did You Know?

- 5 endpoints lack standardized, or in some cases, any Endpoint Protection

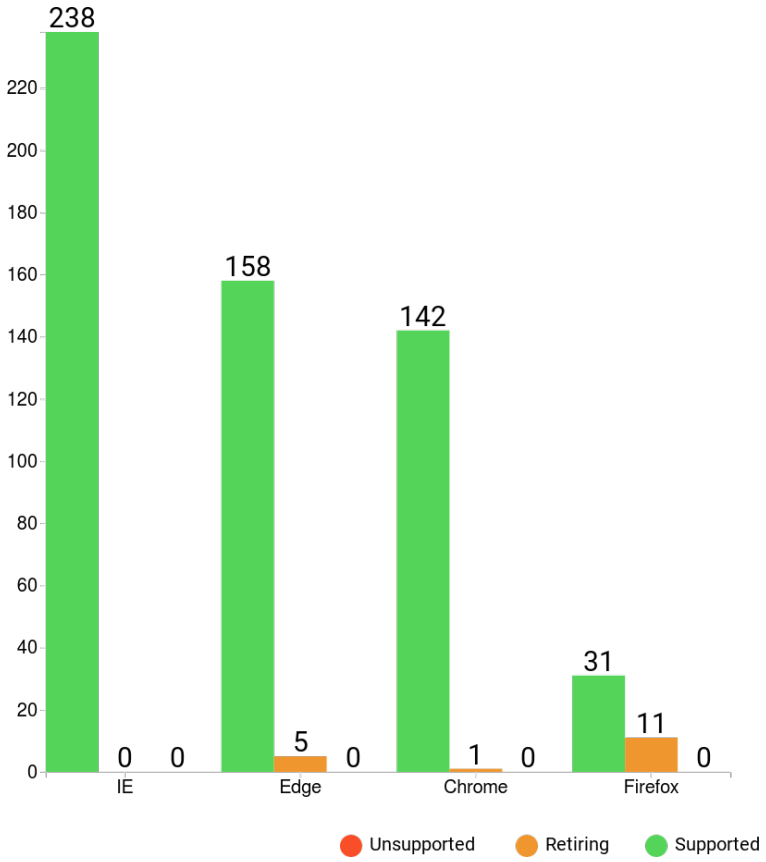
This Matters Because...

Devices without endpoint protection are unprotected from viruses, malware and other malicious code. In addition, the presence of multiple endpoint protection solutions can complicate patching and signature/definition updating.

...Have You Considered?

- Defender for Endpoint and Defender for Office 365 are available via Office 365 subscription and can assist greatly in securing devices in the environment

Device Security: Browser Standards



Did You Know?

- 115 observed browser installations are are out of support and are not considered current

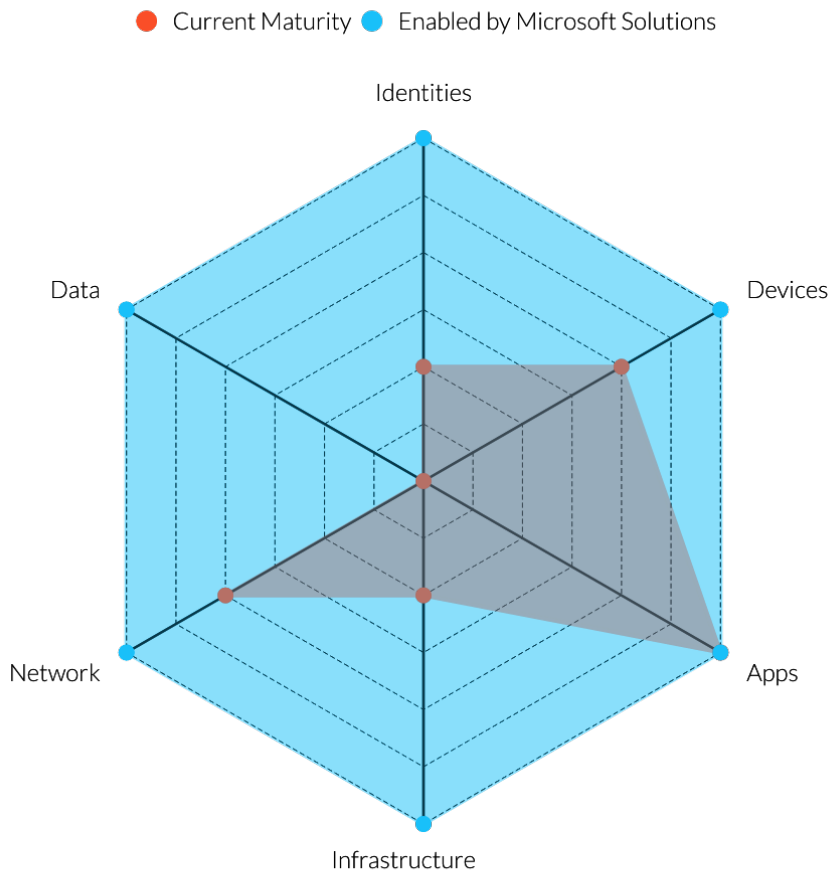
This Matters Because...

Browsers are a common vector for online attack. Ensuring your browsers are current is a key step in decreasing the client attack surface.

...Have You Considered?

- Standardizing on a single and current browser platform
- Leveraging application patching tools such as Microsoft Endpoint Manager to ensure your client applications are up to date and properly patched

Solution Map



Zero Trust Focus Area	Relevant Microsoft Solution(s)
Identities	Azure Active Directory Identity Governance Microsoft Defender for Identity Azure MFA
Devices	Endpoint Manager Endpoint Configuration Manager Windows Virtual Desktop in Azure
Apps	Azure Conditional Access
Infrastructure	Azure Sentinel Microsoft Cloud App Security
Network	Azure Firewall Azure VPN Gateway Azure Virtual Networks
Data	Azure Information Protection Microsoft 365 Information Protection O365 Security and Compliance

Taking Action: What's Next

Actions

- Address unsecured endpoints
- Patch exposed devices (WannaCry / Bluekeep)

- Standardize threat management tooling
- Address application vulnerabilities

- Update and/or migrate End-of-life Operating Systems
- Carry out optimization recommendations

- Implement ARC for remaining/hybrid workloads

Questions?