

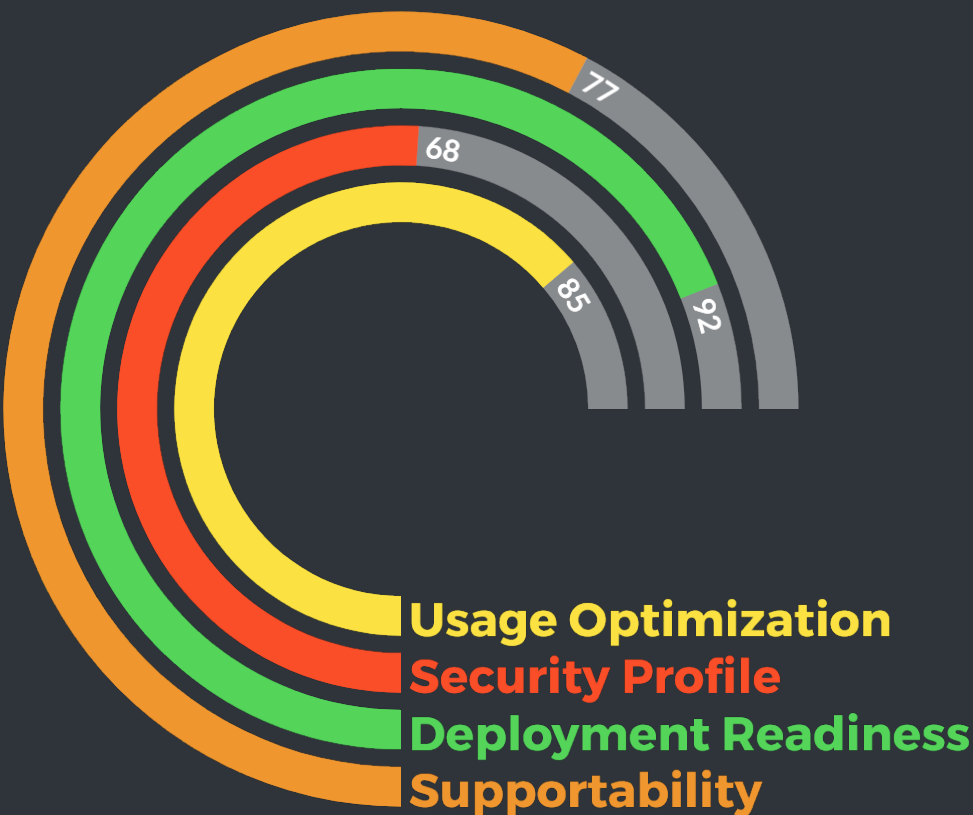
Threat and Opportunity Advisor

Summary of Findings

Sample Customer

Prepared for Sample Customer / March 26th, 2020

Threat & Opportunity Map: Overview



Security Profile

- 88 endpoints were detected without Endpoint Protection
- 78 endpoints were detected with exposures to Ransomware attacks
- 109 endpoints were detected with vulnerabilities to RDP-borne attacks
- 403 security vulnerabilities of moderate to high severity were detected at the application layer
- No email gateway security appeared to be in place

Supportability

- 132 of Office applications in use are at or approaching end-of-support
- 257 of servers and 248 of workstations are running an operating system with an upcoming end-of-support event in the next year

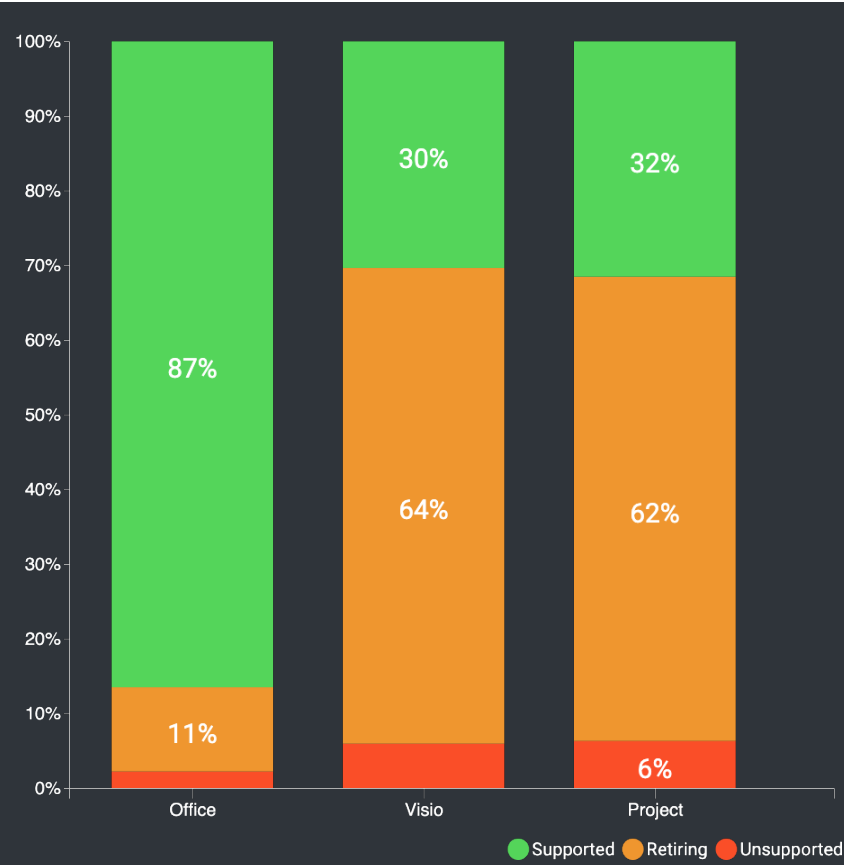
Cost Optimization

- \$25,800.00 per year in potential savings could be realized through proper management of licenses
- \$0.00 in potential cost-reduction opportunities could be realized through standardization of security technologies

Deployment Readiness

- A number of browsers in use will not support the use of Office 365 online components
- A variety of productivity applications were observed to be in use across several versions

Supportability: Productivity Applications



Did You Know?

- 132 of the Office versions in the environment are at or approaching end-of-support
- 193 of the Visio versions in the environment are at or approaching end-of-support
- 69 of Project versions in the environment are at or approaching end-of-support

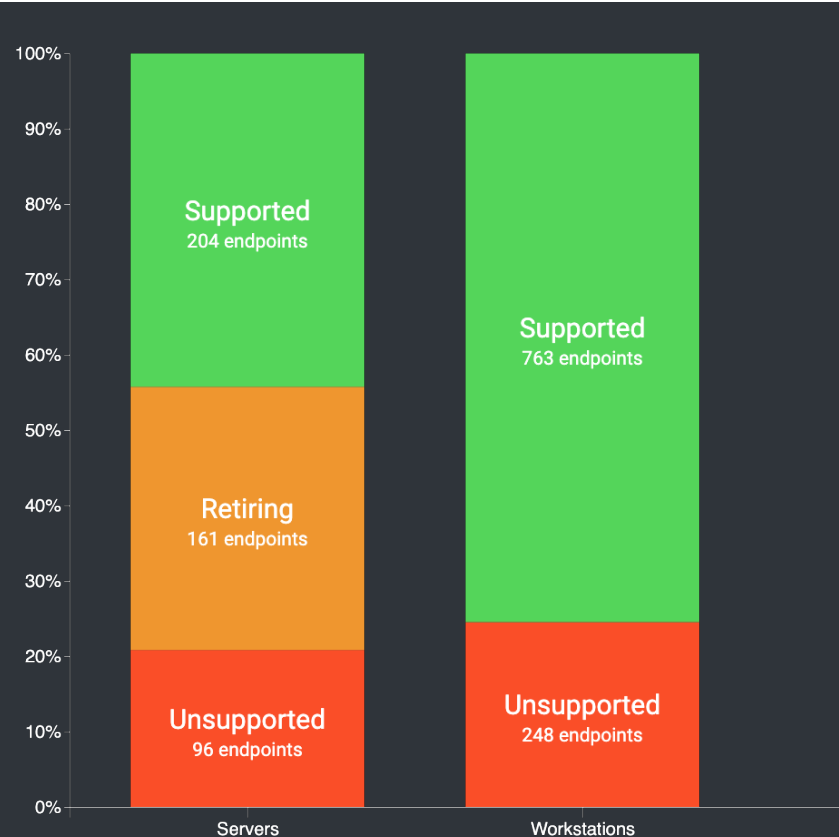
This Matters Because...

Applications outside of extended support will no longer receive security or functionality updates—even those deemed critical. Older applications such as Office 2010 are not being patched against new threats and are an avoidable vulnerability.

...Have You Considered?

- Moving to the available online versions of these productivity applications would ensure entitlement to the newest products, automatic updates, and efficient, user-based licensing
- Selecting an online option such as Visio Plan 2 or Project Online Professional will provide your users with continuity of experience provided by on-premise product availability, but will ease management concerns such as updates, entitlements to new versions as they are released, and the ease of per-user licensing

Supportability: Desktop Operating Systems



Did You Know?

- 342 of workstations are running an unsupported operating system
- 248 of 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 XP machines that are present due to older hardware in training labs 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 SCCM and Microsoft Intune are a key first-line defense against new threats

Security Profile: Coverage by Function

Threat Protection

Symantec Corporation

Fortinet Technologies

Sophos Limited

AVAST Software

\$17,678.99 spent per year

Did You Know?

- 13 security products from 9 different vendors were observed in use.



■ Threat Protection: \$17,678.99

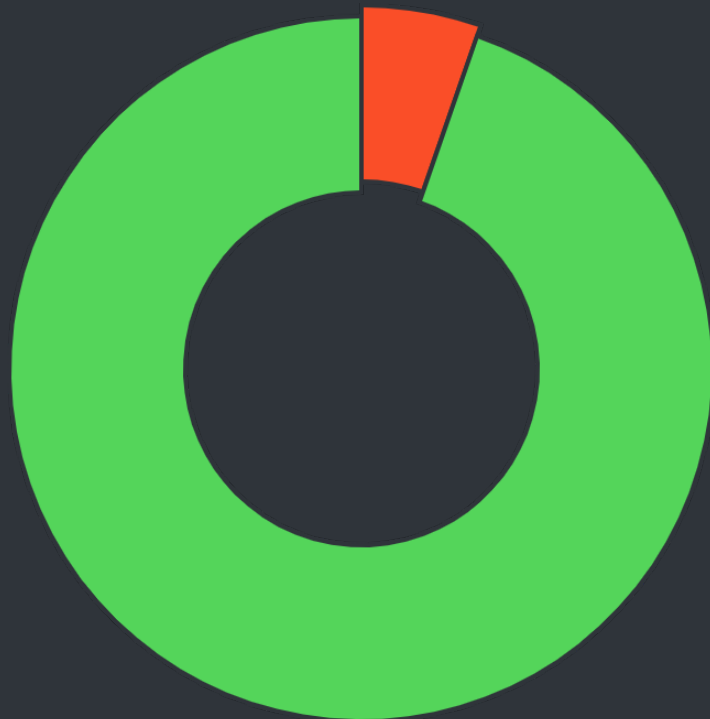
This Matters Because...

\$17,678 productivity products currently in use could be replaced with comparable offerings from Microsoft.

...Have You Considered?

- Windows Defender Advanced Threat Detection Threat & Vulnerability Management provide a single solution to protect, detect, and respond to advanced attacks
- Office 365 Advanced Threat Protection (ATP) is currently available to your E5-licensed users and could assist in detecting and actioning threats before they reach the local environment
- Microsoft 365 E5 is capable of providing a complete security solution

Security Profile: Ransomware Exposure



Exposed: 78 endpoints
Protected: 1385 endpoints

Did You Know?

- 78 machines are not currently patched or protected against the WannaCry / Petya / NotPetya ransomware threats

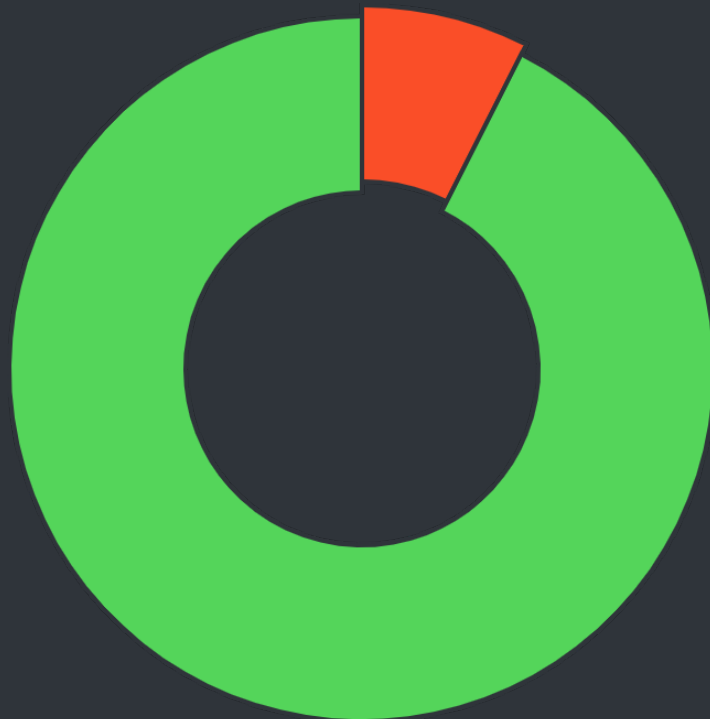
This Matters Because...

A ransomware attack can leave an organization unable to function, with the only option often being rolling back to previous backups. Should backups also be affected, a prolonged and costly outage is likely.

...Have You Considered?

- Operating System patching is the first line of defense against attacks such as WannaCry
- SCCM — and for remote users, InTune — would assist in patching operating systems in the environment
- InTune is included as part of Microsoft EMS
- Microsoft Defender ATP can assist in detecting and prioritizing previously unseen attack variants

Security Profile: BlueKeep / RDP Exposure



Exposed: 109 endpoints
Protected: 1352 endpoints

Did You Know?

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

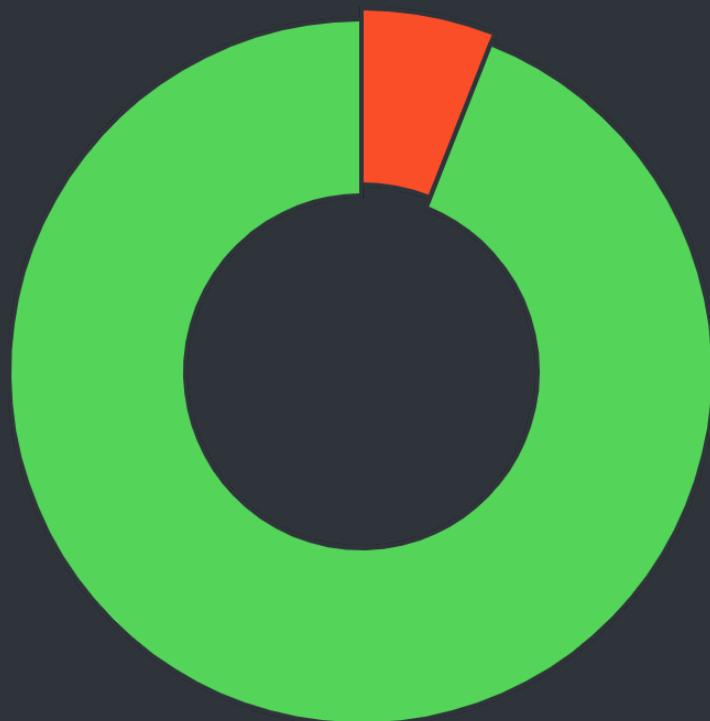
This Matters Because...

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
- SCCM — and for remote users, InTune — would assist in patching operating systems in the environment
- InTune is included as part of Microsoft EMS
- Microsoft Defender ATP can assist in detecting and prioritizing previously unseen attack variants

Security Profile: Endpoint Protection



Uncovered: 88 endpoints
Covered: 1384 endpoints

Did You Know?

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

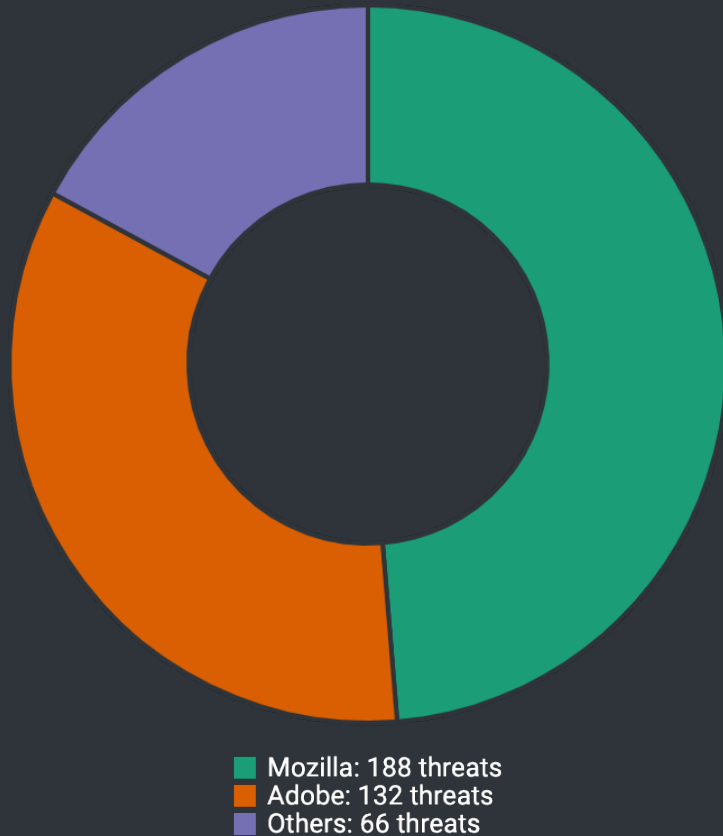
This Matters Because...

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?

- Office 365 Advanced Threat Protection (ATP) is included in numerous types of Office 365 subscription, or in many cases can be purchased as an add-on

Security Profile: Applications & OS



Did You Know?

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

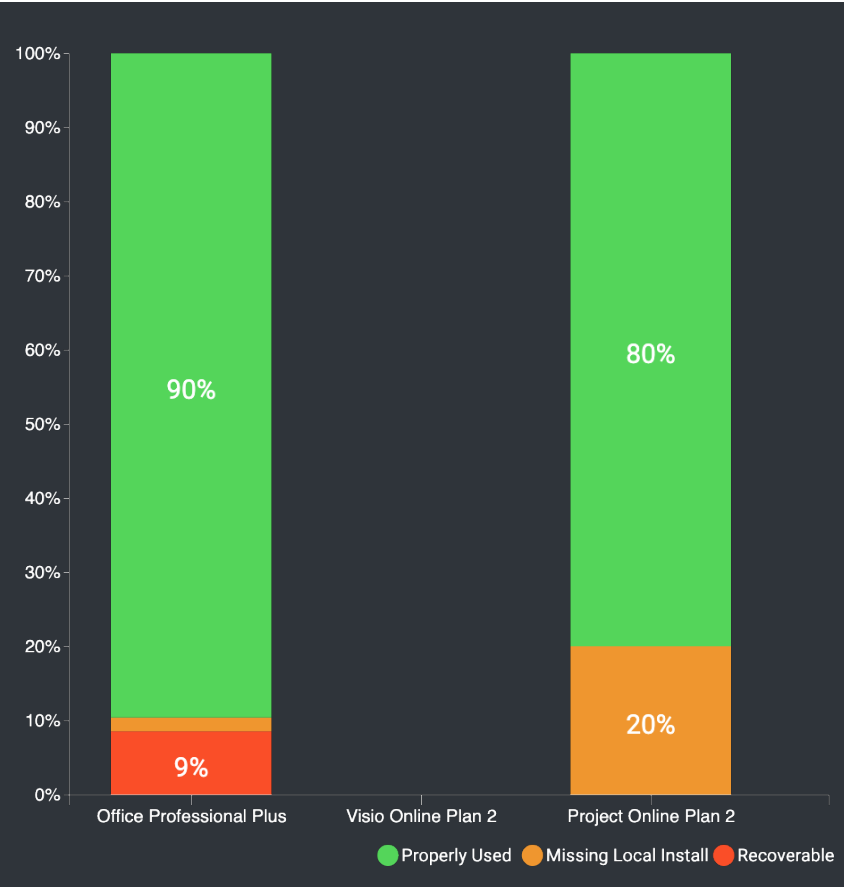
This Matters Because...

Many high profile exploits – such as the Equifax breach of 2016 – were made possible by a lack of application-level patching.

...Have You Considered?

- Implementing and following an application patch management policy
- Monitoring embedded operating systems—such as VMWare ESX and Cisco IOS, often overlooked attack vectors
- Microsoft Defender ATP can assist in detecting and prioritizing previously unseen attack variants
- Microsoft Threat & Vulnerability Management (TVM) can assist in ensuring detected vulnerabilities are passed to solutions such as SCCM and InTune for patching

Cost Optimization: License Management



Did You Know?

- 19 E3 users have not installed a local instance of Office Professional Plus
- 0 Visio Plan 2 users have not installed a local instance of Visio Professional
- 1 Project Plan 2 users have not installed a local instance of Project Professional
- 225 users with licenses assigned appear to have left the organization

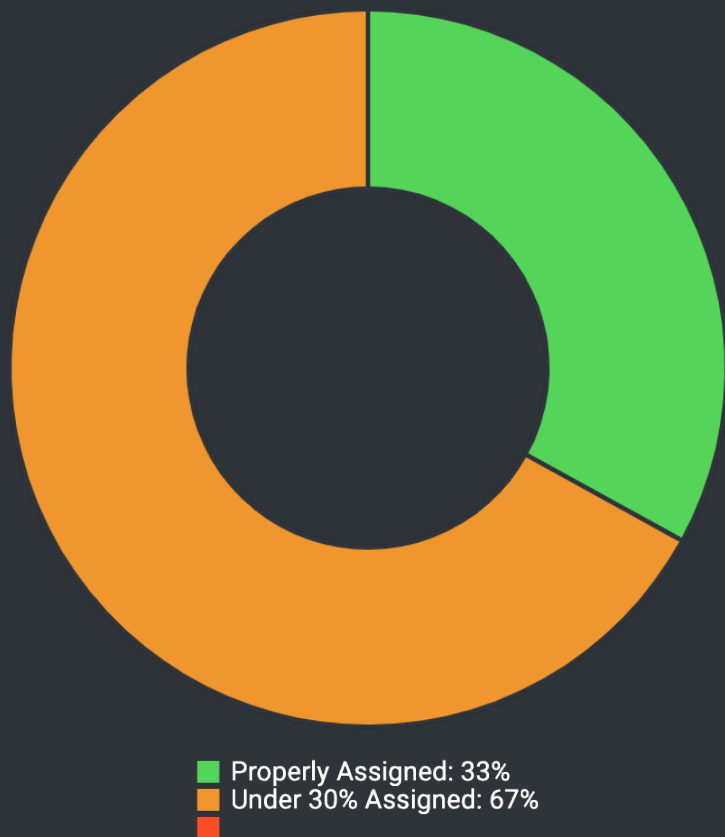
This Matters Because...

\$25,800.00 per year in potential savings could be realized through proper management of licenses.

...Have You Considered?

- Regular management of Office 365 needs and license consumption can ensure the full benefits of the offering are realized without waste being introduced
- Ensure that the process for departing employees includes decommissioning of associated licenses
- If email retention is required for archival or legal purposes, Office 365 E3 and E5 offer legal hold features, and Exchange Online Archiving assists in managing this need without consuming expensive licenses needlessly

Cost Optimization: Deployment & Activation



Did You Know?

- You have not provisioned any of the following assigned services:
- Less than 30% of the available licenses have been deployed for the following services:

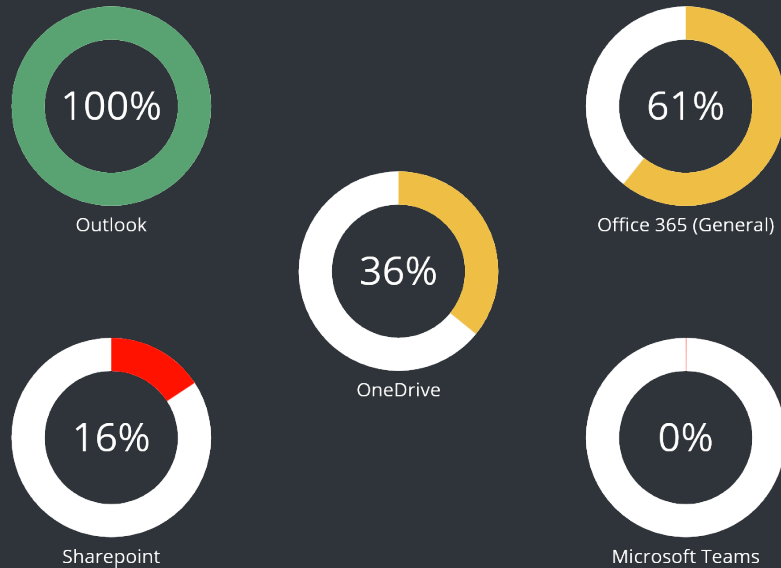
This Matters Because...

\$25,800.00 per year in potential savings could be realized through proper management of license need and deployment.

...Have You Considered?

- Regular management of Office 365 needs and license consumption can ensure the full benefits of the offering are realized without waste being introduced

Cost Optimization: Current Usage



Did You Know?

- 39% of users are presently not leveraging the majority of the Office 365 core services
- 64% users are not leveraging OneDrive

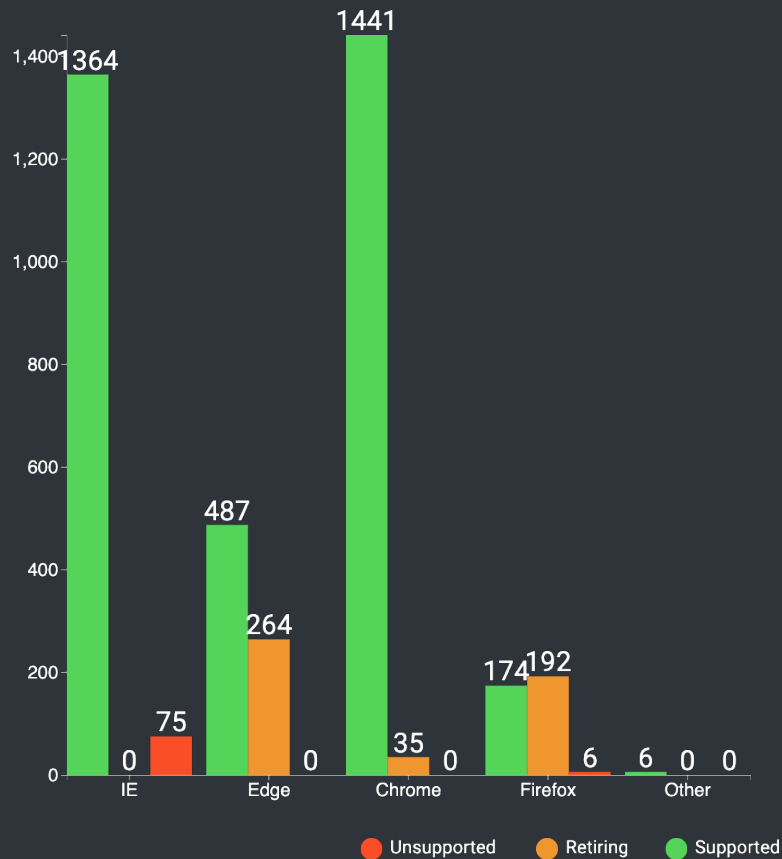
This Matters Because...

Re-levelling or properly deploying the Office 365 technologies you are entitled to will ensure waste is minimized.

...Have You Considered?

- Assessing the needs of your Project and Visio users may present an opportunity to properly size your requirements for the Plan 1 and Plan 2 userbase
- A Microsoft Solution Workshop can assist your organization in realizing the full value of the Office 365 suite you currently have available

Deployment Planning: Browser Standards



Did You Know?

- 76 of browsers are not running a browser or browser version recommended for use with the online components of Office 365.

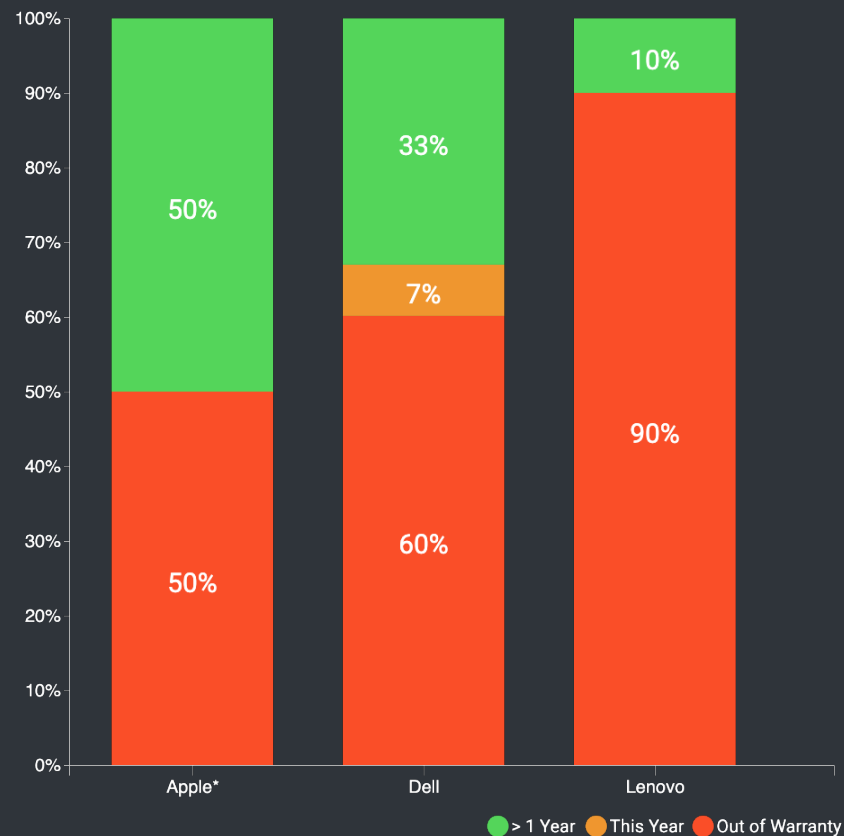
This Matters Because...

While Office 365 can be run on almost any PC and supports a variety of browsers, for optimal functionality Microsoft recommends Edge or IE11. When accessing Office 365 from older versions of IE, users will experience known issues and limitations depending on version. Microsoft no longer offers code fixes to resolve problems encountered while using IE9 or earlier versions.

...Have You Considered?

- Assessing the needs of your Project and Visio users may present an opportunity to properly size your requirements for the Plan 1 and Plan 2 userbase
- A Microsoft Solution Workshop can assist your organization in realizing the full value of the Office 365 suite you currently have available

Standardization: Endpoint Devices



Did You Know?

- 2 models from 1 manufacturer make up the client device footprint within the organization
- 65% of Devices have reached the end of warranty coverage
- 3% of Devices will be out of warranty coverage this year

This Matters Because...

Standardizing on a smaller number of hardware models, and ensuring your fleet is protected in the event of hardware failures can decrease support incidents, downtime and time to resolution, as well as allow you to benefit from consolidated purchasing power.

...Have You Considered?



Surface Laptop 3

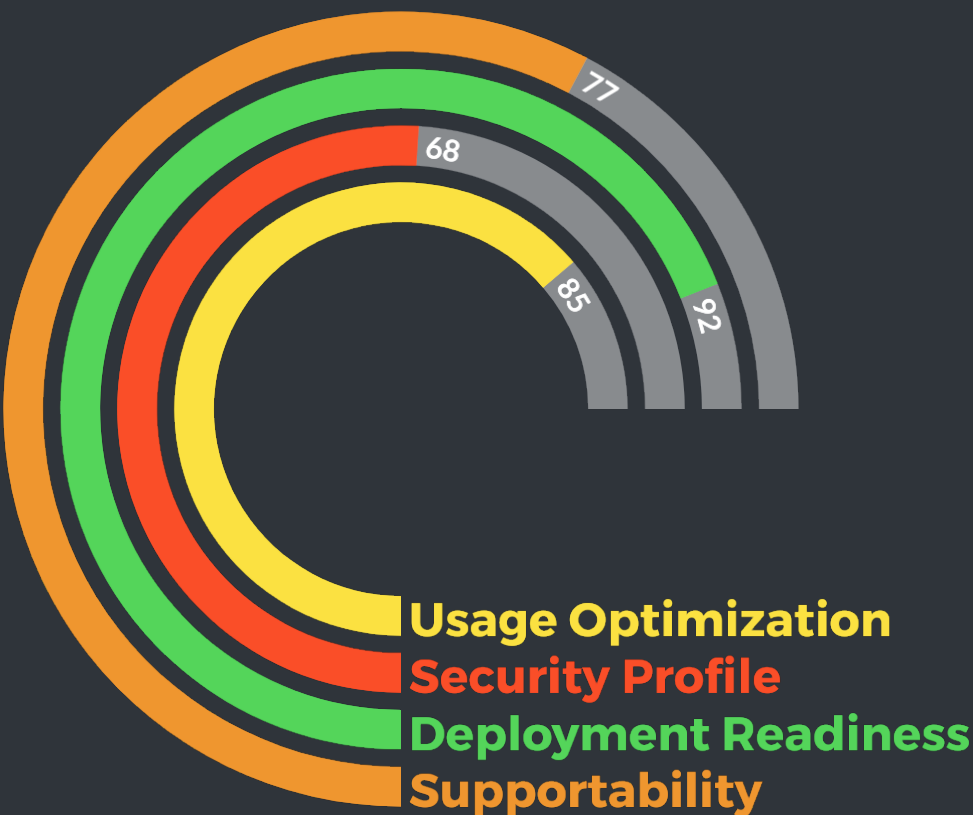
- Quad-core 10th Gen Intel® Core™ i7-1065G7
 - Up to 32GB LPDDR4x RAM & 1TB HDD
- This device is a suitable replacement for 145 of your end-of-life devices



Surface Studio 2

- Quad-core 7th Gen Intel® Core™ i7-7820HQ
 - Up to 32GB DDR4 RAM & 2TB SSD
- This device is a suitable replacement for 69 of your end-of-life devices

Action Map & Next Steps



Security Profile

- Patch management activities should be immediately undertaken for the detected vulnerabilities and policy gaps
- An email gateway security solution should be implemented at the earliest opportunity
- A Microsoft Security Workshop may be a logical next step to assist in shoring up gaps in coverage and consolidating the security portfolio
- Evaluation of Microsoft 365 E5 is recommended as a single solution to the observed issues

Supportability

- 132 of Office applications in use are at or approaching end-of-support
- 257 of servers and 248 of workstations are running an operating system with an upcoming end-of-support event in the next year
- Standardizing on SaaS or O365 versions of these productivity applications will assist in the process of maintaining standards







Cost Optimization

- \$25,800.00 per year in potential savings could be realized through proper management of licenses
- \$0.00 in potential cost-reduction opportunities could be realized through standardization of security technologies
- A follow-up with your CSP/LSP can assist in realizing these savings

Deployment Readiness

- A number of browsers in use will not support the use of Office 365 online components
- A variety of productivity applications were observed to be in use across several versions

Next Steps: Your Roadmap to Office 365

	Phase	Results	Estimated Time	Notes	Partner	Recommendation
	Networking	Your network is optimized for access to Microsoft 365's cloud-based services.				
	Identity	Your admin accounts are protected, your users and groups are synchronized, and your user authentication is strong.				
	Windows 10 Enterprise	Your existing Windows-based computers can upgrade to Windows 10 Enterprise and new devices are installed with Windows 10 Enterprise.				
	Office 365 ProPlus	Your existing users of Microsoft Office can upgrade to Office 365 ProPlus.				
	Mobile Device Management	Your devices can be enrolled and managed.				
	Information Protection	Office 365 security features are enabled and your labels and policies are ready to protect documents and email.				

Relevant Microsoft 365 Solutions

Issue Observed	Recommended Solution
Office Standardization	<ul style="list-style-type: none"> • 7 versions of Office currently in use • Moving to a standard Office platform would ensure updates are available and decrease attack surface
End-of-life Office Titles	<ul style="list-style-type: none"> • Several hundred instances of unsupported Office titles in use • Moving to a standard Office platform would ensure updates are available and decrease attack surface
Endpoint Protection	<ul style="list-style-type: none"> • Advanced Threat Protection would be available in certain O365 configurations and could assist in patching the vulnerable areas of the endpoint environment • Cost benefit to standardizing on a single, fully deployed endpoint protection solution
Ransomware Exposure	<ul style="list-style-type: none"> • InTune could assist in patching the local and distributed environment • Ongoing oversight of patching and the ability to report on threats would be an asset to the organization

Overview: Notable Products In Use

Category	Detected in Use	Microsoft Equivalent
Identity & Access Management	No Products Detected	Microsoft Advanced Threat Protection
Information Protection	No Products Detected	Microsoft Advanced Threat Protection
Threat Protection	<ul style="list-style-type: none"> • Symantec Endpoint Protection • FortiClient • Sophos Anti-Virus 	Microsoft Advanced Threat Protection
Security Management	No Products Detected	Microsoft Advanced Threat Protection
Collaboration	<ul style="list-style-type: none"> • Cisco WebEx Meetings • Cisco Webex Meetings Desktop App • Webex Recorder and Player 	Microsoft Teams
Cloud File Transfer	<ul style="list-style-type: none"> • Dropbox Update Helper • Dropbox • Google Drive 	Microsoft OneDrive
Productivity Suite	No Products Detected	Microsoft O365

Threat and Opportunity Advisor

For detailed reports, or to discuss data handling and privacy, please visit your Zones Online Portal or email CloudSupport@zones.com for assistance.