EFFECTIVELY MANAGING MICROSOFT 365 ENVIRONMENTS WITH MICROSOFT TOOLS

Robert Crane

SMBiT PROFESSIONALS

NEXTLEVEL

“Microsoft was originally — and should view itself again as — ‘a maker of tools and platforms,’ enabling others to create.”

— Satya Nadella

Hammer

M365 Business Premium Features Map

M365 Business Premium Features List

Defender

Inventories

Software | Vulnerable components

Software
20

Export

Name	OS platform	Vendor	Weaknesses	Threats	Exposed devices	Impact	Tags
Firefox	Windows	Mozilla	137		1 / 1	84.20	EOS versions
Visual Studio Code	Windows	Microsoft	6		1 / 1	30.80	
Notepad++	Windows	Notepad Plus Plus	1		1 / 1	25.60	
Snagit	Windows	Techsmith	0		0 / 1	0.00	
Edge Chromium-based	Windows	Microsoft	0		0 / 1	0.00	
Windows Defender	Windows	Microsoft	0		0 / 1	0.00	
Defender Security Intelligence Updates	Windows	Microsoft	0		0 / 1	0.00	
Windows 10	Windows	Microsoft	0		0 / 1	0.00	Upcoming EOS versions
.net Framework	Windows	Microsoft	0		0 / 1	0.00	
Office	Windows	Microsoft	0		0 / 1	0.00	

Weaknesses

Vulnerabilities in my organization	Exploitable vulnerability	Critical vulnerabilities	Zero-day vulnerabilities	Vulnerabilities with no security update	Vulnerabilities with some security updates
144	1	2	0	0	0

Export

Filters: Exposed devices: Affects my organization

Name	Severity	CVSS	Affected Software	Age	Published on	First detected	Updated on	Threats	Exposed devices	Tags
CVE-2025-9187	High	8.8	Mozilla Firefox (+ 6 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 19, 2025 10:00 AM		1	
CVE-2025-9185	High	8.8	Oracle Firefox (+ 34 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 9, 2025 12:24 AM		1	
CVE-2025-9184	High	8.8	Mozilla Thunderbird (+ 19 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 8, 2025 9:07 PM		1	
CVE-2025-9183	Medium	6.5	Mozilla Firefox (+ 14 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 8, 2025 9:07 PM		1	
CVE-2025-9182	Medium	6.5	Oracle Firefox (+ 28 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 9, 2025 12:24 AM		1	
CVE-2025-9181	High	8.8	Oracle Firefox (+ 34 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 9, 2025 12:24 AM		1	
CVE-2025-9180	Medium	6.5	Oracle Firefox (+ 34 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 9, 2025 12:24 AM		1	
CVE-2025-9179	High	8.8	Oracle Firefox (+ 34 more)	2 months	Aug 19, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 9, 2025 12:24 AM		1	
CVE-2025-8044	High	8.8	Mozilla Firefox (+ 6 more)	2 months	Jul 22, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Jul 29, 2025 12:09 AM		1	
CVE-2025-8043	Medium	6.5	Mozilla Firefox (+ 6 more)	2 months	Jul 22, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Jul 29, 2025 12:05 AM		1	
CVE-2025-8042	Medium	6.5	Mozilla Firefox (+ 5 more)	2 months	Jul 22, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 20, 2025 2:53 AM		1	
CVE-2025-8040	High	8.8	Mozilla Firefox (+ 29 more)	2 months	Jul 22, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Jul 31, 2025 10:00 AM		1	
CVE-2025-8039	Medium	6.5	Mozilla Firefox (+ 29 more)	2 months	Jul 22, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Jul 31, 2025 10:00 AM		1	
CVE-2025-8038	Medium	6.5	Mozilla Firefox (+ 29 more)	2 months	Jul 22, 2025 10:00 AM	Sep 30, 2025 7:50 PM	Sep 30, 2025 9:03 AM		1	

Incidents

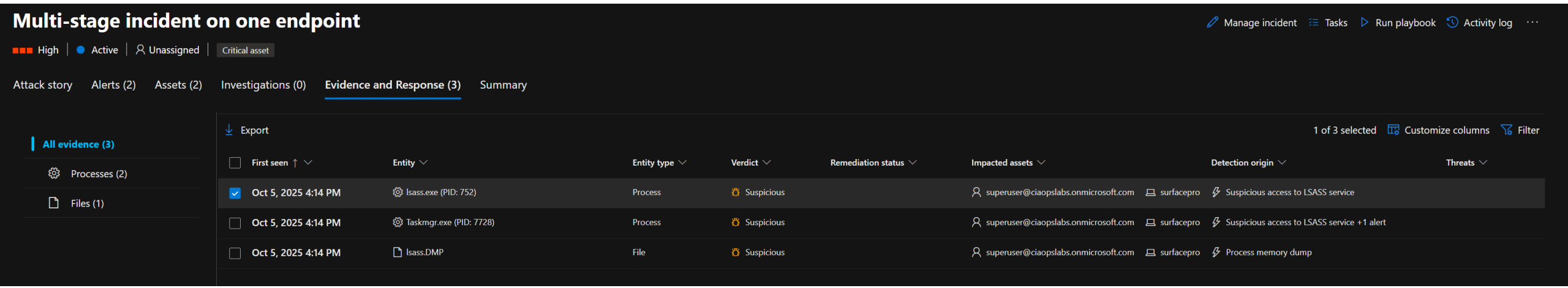
Most recent incidents and alerts

Export | Copy list link | Refresh

Filter set: Save

Status: New, In progress | Add filter | Reset all

Incident name	Incident Id	Severity	Investigation state	Categories	Impacted assets	Active alerts
Rare and potentially high-risk Office operations in...	480	Low		Suspicious activity	NT AUTHORITY\SYSTEM (Microsoft.Exchang	1/1
Rare and potentially high-risk Office operations in...	479	Low		Suspicious activity	NT AUTHORITY\SYSTEM (Microsoft.Exchang	1/1
Rare and potentially high-risk Office operations in...	478	Low		Suspicious activity	NT AUTHORITY\SYSTEM (Microsoft.Exchang	1/1


Multi-stage incident on one endpoint
Manage incident
Tasks
Run playbook
Activity log
High
Active
Unassigned
Critical asset
Attack story
Alerts (2)
Assets (2)
Investigations (0)
Evidence and Response (3)
Summary
All evidence (3)
Processes (2)
Files (1)
Export
1 of 3 selected
Customize columns
Filter
First seen
Entity
Entity type
Verdict
Remediation status
Impacted assets
Detection origin
Threats
Oct 5, 2025 4:14 PM
lsass.exe (PID: 752)
Process
Suspicious
superuser@ciaopslabs.onmicrosoft.com
surfacepro
Suspicious access to LSASS service
Oct 5, 2025 4:14 PM
Taskmgr.exe (PID: 7728)
Process
Suspicious
superuser@ciaopslabs.onmicrosoft.com
surfacepro
Suspicious access to LSASS service +1 alert
Oct 5, 2025 4:14 PM
lsass.DMP
File
Suspicious
superuser@ciaopslabs.onmicrosoft.com
surfacepro
Process memory dump

Part of incident: Multi-stage incident on one endpoint View incident page

surfacepro Risk level Low
Windows10

AzureAD\SuperUser

AzureAD\RobertCrane

Alert story

Maximize

Process tree | Alert timeline

Expand all | Copy story to clipboard

10/1/2025 5:46:00 PM [620] smss.exe

5:46:01 PM [840] winlogon.exe

10/5/2025 4:10:55 PM [3608] userinit.exe

4:10:55 PM [4656] explorer.exe

4:14:35 PM [7728] Taskmgr.exe /7

4:14:50 PM Taskmgr.exe opened a handle to lsass.exe

Suspicious access to LSASS service High Detected New

4:14:50 PM [7728] Taskmgr.exe created file lsass.DMP Malware

Process memory dump High Detected New

4:14:51 PM Taskmgr.exe opened a handle to lsass.exe

Suspicious access to LSASS service High Detected New

4:15:03 PM Defender detected and terminated active 'Behavior:Win32/DumpLsass.l!attk' in process 'an unknown process' during behavior monitoring Malware

Suspicious 'DumpLsass' behavior was blocked Low Blocked New

10/1/2025 5:46:00 PM [628] wininit.exe

5:46:00 PM [752] lsass.exe

Suspicious access to LSASS service High Detected New

Suspicious access to LSASS service

High | Detected | New

Manage alert | Tune alert | Move alert to another incident

Details | Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification
Not Set
Set Classification

Assigned to
Unassigned

Alert details

Alert ID
da7c617f63-7d7a-4f89-82e4-636514d35af1_1

Category
Credential access

Detection source
EDR

Service source
Microsoft Defender for Endpoint

Detection status
Detected

Detection technology
Behavior,Memory

Generated on
Oct 5, 2025 4:20:15 PM

First activity
Oct 5, 2025 4:14:50 PM

Last activity
Oct 5, 2025 4:14:51 PM

Workspace
-

Evidence

Entity Name	Remediation Status	Verdict
lsass.exe (PID: 752)		Suspicious
Taskmgr.exe (PID: 7728)		Suspicious

Process tree | **Alert timeline**

Expand all | Show related alerts | Ungroup | Copy story to clipboard

Suspicious access to LSASS service — High | Detected | New

10/1/2025
5:46:00 PM

[628] wininit.exe created **[752] lsass.exe**

Process id	752
Execution details	Token elevation: Default, Integrity level: System
Image file path	C:\Windows\System32\lsass.exe
Image file SHA1	5874c705ebb39053378b2aa653a707e31541ad1f
Image file creation time	Oct 1, 2025 12:31:21 PM
Image file last modification time	Oct 1, 2025 12:31:21 PM
Mitre techniques	T1003.001: LSASS Memory
Signer	Microsoft Windows
Issuer	Microsoft Windows Production PCA 2011
VirusTotal detection ratio	0/72
Initiating process	[628] **wininit.exe**
PE metadata	**lsass.exe**
User	**NT AUTHORITY\SYSTEM**

10/5/2025
4:14:50 PM

Taskmgr.exe opened a handle to lsass.exe

Initiating process	[7728] **Taskmgr.exe** /7

Initiatives

Key initiatives

External Attack Surface Protection
No data available

SaaS Security
46%
No change (last 14 days)

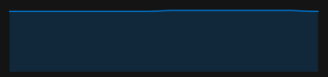
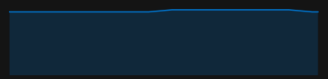
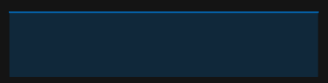
CIS M365 Foundations Benchmark
61%
No change (last 14 days)

Zero Trust (Foundational)
28%
↑ 4% (last 14 days)

Identity Security
14%
No change (last 14 days)

Domain initiatives | Threat initiatives

13 items | Search | Filter

14-day trend	Initiative name	Mark as favorite	Current score	Workloads	14 day change drift	Last updated
	**Business Email Compromise - Financial fraud** Business email compromise (BEC) financial fraud is a social engineering attack that aims to steal money or sensitive information. The attacker tricks the target into believing they are interacting with a trusted entity to conduct either personal or professional business. After deceiving the target, the attacker persuades them to share valuable information or process a payment.	☆	58%	Defender for Office, Microsoft Information Protection, Defender for Cloud Apps, Entra ID,...	No change	Oct 5, 2025 1:07:42 AM
	**CIS M365 Foundations Benchmark** The CIS Microsoft 365 Foundations Benchmark (v3.0.0) is a set of security assessments developed by the Center for Internet Security (CIS). It provides prescriptive guidance for establishing a secure baseline configuration for Microsoft 365. The benchmark includes configuration baselines and best practices for securely configuring a system. The benchmark is internationally recognized as a security standard for defending IT systems and data against cyber attacks. This initiative contains a subset of security assessments recommended by the CIS	☆	61%	Defender for Cloud Apps	No change	Oct 5, 2025 1:07:42 AM
No data	**Cloud Security [Preview]** This initiative aims to reflects the status around cloud security coverage, ROI, health, configuration and performance. It consists of measurements across multiple domains and disciplines to provide security managers with a high-level view into how posture is enforced in cloud ops.	☆	-	Defender for Cloud	-	None in 90 days
No data	**Critical Asset Protection** Critical asset protection refers to the strategies, processes, and technologies implemented to safeguard an organization's most valuable and important assets from various threats and risks. It involves identifying, prioritizing, and applying targeted security measures to ensure the resilience and integrity of these critical assets.	☆	-	Defender for Cloud, Defender for Endpoint	-	None in 90 days
	**Endpoint Security** Monitor the coverage and configuration of physical and virtual workstations, servers and mobile phones.	☆	78%	Defender for Endpoint	No change	Oct 5, 2025 12:16:56 AM

Business Email Compromise - Financial fraud: 58%

Mark as favorite | Set target score | Suggest new initiative | ...

No change (last 14 days) • Your target score: 99% • Last updated: Oct 5, 2025 1:07:42 AM

Overview | Security metrics (17) | **Security recommendations (52)** | History

Note: these recommendations are based on global compliance considerations and might not necessarily relate to specific aspects of this initiative.

Export | 49 items | Search | Filter

Filters: State: Compliant +3

Name ↑	State	Impact	Workload	Domain	Last calculated	Last state change	Related initiatives	Related metrics
Create Safe Links policies for email messages	COMPLIANT	High	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	9	3
Create zero-hour auto purge policies for malware	COMPLIANT	Medium	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	4	3
Create zero-hour auto purge policies for phishing messages	COMPLIANT	Low	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	10	3
Create zero-hour auto purge policies for spam messages	COMPLIANT	Low	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	4	2
Don't add allowed IP addresses in the connection filter policy	COMPLIANT	Low	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	2	4
Enable Conditional Access policies to block legacy authentication	NOT COMPLIANT	High	Entra ID	identity	Oct 3, 2025 3:41 PM	None in 90 days	15	8
Enable impersonated domain protection	COMPLIANT	High	Defender for Office	apps	Oct 4, 2025 7:43 AM	Jul 17, 2025 10:00 AM	2	2
Enable impersonated user protection	COMPLIANT	High	Defender for Office	apps	Oct 4, 2025 7:43 AM	Jul 17, 2025 10:00 AM	2	2
Enable Microsoft Entra ID Identity Protection sign-in risk policies	NOT COMPLIANT	High	Entra ID	identity	Oct 3, 2025 3:41 PM	None in 90 days	26	9
Enable Microsoft Entra ID Identity Protection user risk policies	NOT COMPLIANT	High	Entra ID	identity	Oct 3, 2025 3:41 PM	None in 90 days	24	9
Enable the domain impersonation safety tip	COMPLIANT	Low	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	2	2
Enable the user impersonation safety tip	COMPLIANT	Low	Defender for Office	apps	Oct 4, 2025 7:43 AM	None in 90 days	2	2

Live response on surfacepro

Connected

Disconnect session | Upload file to library

Entity summary

Device details

View device details

Session Information

Session ID
CLRf6871c44-ffe6-4129-9f69-0778b8db5e64

Session created by
superuser@ciaopslabs.onmicrosoft.com

Session started
Oct 5, 2025 4:05 PM

Session ended
N/A

Duration
35s

Device Information

Command console | Command log

Maximize

Command index

```
C:\> connect
Session established

C:\> dir
Path                        Created              Modified             Size         Is Directory   Read Only      Hidden
==========================  ===================  ===================  ===========  ============   =========      ======
$Recycle.Bin                2019-12-07 09:14:52  2024-02-12 07:06:16  0            true           false          true
$SysReset                   2024-02-12 06:18:03  2024-02-13 01:39:49  0            true           false          true
$WinREAgent                 2025-04-23 13:00:43  2025-04-23 13:00:43  0            true           false          true
DumpStack.log               2023-06-22 00:13:58  2023-08-18 02:46:03  8192         false          false          true
DumpStack.log.tmp           2023-06-22 00:13:58  2025-10-01 07:46:00  8192         false          false          true
Intel                       2023-06-22 00:14:47  2023-06-22 00:14:47  0            true           false          false
LastMileClient              2023-07-14 06:41:09  2023-07-14 06:41:09  0            true           false          false
OneDriveTemp                2024-03-28 03:18:32  2024-03-28 03:18:32  0            true           false          true
PerfLogs                    2024-02-13 01:27:07  2024-02-13 01:27:07  0            true           false          false
Program Files               2024-02-13 01:27:07  2024-11-23 02:57:50  0            true           true           false
Program Files (x86)         2024-02-13 01:27:07  2024-12-13 05:38:09  0            true           true           false
ProgramData                 2024-02-13 01:27:07  2024-03-22 07:06:13  0            true           false          true
Recovery                    2023-06-22 00:50:56  2024-02-29 03:32:28  0            true           false          true
Resources                   2023-08-01 01:26:41  2023-08-01 01:26:41  0            true           false          false
Scripts                     2023-07-14 05:50:18  2023-07-14 05:51:11  0            true           false          false
System Volume Information   2021-09-23 05:35:41  2021-11-16 23:10:30  0            true           false          true
Users                       2024-02-13 01:20:14  2024-11-05 00:54:20  0            true           true           false
Windows                     2024-02-13 01:20:14  2025-10-01 07:42:29  0            true           false          false
Windows.old                 2024-02-13 01:33:38  2024-02-15 05:43:26  0            true           false          false
hiberfil.sys                2021-09-23 05:38:12  2025-10-01 07:45:57  1669206016   false          false          true
inetpub                     2025-04-08 19:03:36  2025-04-08 19:03:36  0            true           false          false
pagefile.sys                2021-09-23 05:35:43  2025-10-01 07:46:00  738197504    false          false          true
swapfile.sys                2021-09-23 05:35:43  2025-10-01 07:46:00  16777216     false          false          true

C:\> _
```

Intune

Tenant admin | Remote Help

Search

Tenant status
Remote Help
Microsoft Tunnel Gateway
Cloud PKI
Connectors and tokens
Assignment filters
Roles
Microsoft Entra Privileged Identity Management
Diagnostics settings
Audit logs
Device diagnostics
Multi Admin Approval
Intune add-ons
Copilot

Remote Help is now generally available. To use this add-on, you can start a trial or obtain licenses. Learn more about Remote Help

Monitor | Settings | Remote Help sessions

Refresh | Filter

Current active sessions

0

Average session time

No data to display

Total sessions

No data to display

Reports | Workbooks | Gallery

Search

Overview

Device management

- Device attestation status (preview)
- Device compliance
- Device configuration
- Group policy analytics
- Windows updates
- Cloud attached devices (preview)
- Cloud PC overview
- Apple updates

Endpoint security

- Microsoft Defender Antivirus
- Firewall

Analytics

- Endpoint analytics

New | Refresh | Feedback | Help | Community Git repo | Browse across galleries | Open recycle bin

All | Workbooks | **Public Templates** | My Templates

Filter by name or category

7 Public Templates

Template name	Category	Description	Publishe
Quick start (2)			
Audit (1)			
Intune Audit Activity	Audit		Microsof
Activity Logs Insights (1)			
Activity Logs Insights	Activity Logs Insights	Activity Logs Insights	Microsof
Enrollment (1)			
Intune Enrollment Activity	Enrollment		Microsof
Compliance (1)			
Intune Compliance Activity	Compliance		Microsof
Devices (1)			
Intune Devices Activity	Devices		Microsof

Problem

- Reporting for MSP’s a challenge
- Reports all over the place- Different sites and pages required for Device management, Windows updates, Security , Apps.
- Poor experience with RMM tools – confusing and inaccurate windows update reports, limited security reporting.
- Lack of ability to produce customer reporting
- Lack of single view across all aspects of IT and all customers.

Opportunity

- Microsoft Intune and Security Centre have many powerful and extremely useful sets of reports.

- That means there is lots of data that can be used for reporting

Reports | Device compliance

Search

Overview

Device management

Device attestation status (preview)

Device compliance

Device configuration

Group policy analytics

Windows updates

Cloud attached devices (preview)

Cloud PC overview

Apple updates

Endpoint security

Microsoft Defender Antivirus

Summary | Reports

Generate | Last refreshed on: 08/09/2025, 12:23:04 pm

Device compliance

Compliant	Noncompliant	Managed by Configuratio...	Total
66 devices	**4** devices	**0** devices	**70** devices

Device compliance status

Status	Devices
Compliant	
Compliant	66
In grace period	0
Noncompliant	

Reports | Windows updates

Search

Overview
Device management
Device attestation status (preview)
Device compliance
Device configuration
Group policy analytics
Windows updates
Cloud attached devices (preview)
Cloud PC overview
Apple updates

Summary | Reports

Windows Feature updates

Due to the amount of data, this report might take some time to generate and will expire after 72 hours.

Generate again | Cancel | Report generated 08/09/2025, 12:24 pm

Columns | 1 item

Policy	Versions	In progress	Success	Error	Rollback initiated or completed	Cancelled
Windows 11 with WIndows 10 c...	Windows 11, version 24H2	2	60	0	0	59

Endpoint analytics | Overview

Search

Overview
Settings
Reports
Startup performance
Application reliability
Work from anywhere
Resource performance
Battery health

Enroll and reboot devices to see scores and insights. For enrolled devices, It can take up to 24 hours after restart to appear on this report. Learn more →

Overview | Anomalies | Model scores | Device scores

Proactively optimize the user experience and track your progress Learn more

Device scope : **All Devices**

Refresh

Baseline ⓘ All organizations (median)

Endpoint analytics score ⓘ

Endpoint analytics score
87

Baseline ⓘ
50

Score categories ⓘ

Metric	Score
Startup performance	79
Application reliability	89
Work from anywhere	93

Reports | Firewall

Search

Overview

Device management

Device attestation status (preview)

Device compliance

Device configuration

Group policy analytics

Windows updates

Cloud attached devices (preview)

Cloud PC overview

Apple updates

Due to the amount of data, this report might take some time to generate and will expire after 72 hours.

Firewall status

All

Generate again | Cancel | Report generated 08/09/2025, 12:26 pm

Export | Columns

Search

Enabled	Disabled	Limited	Temporarily disabled (defa...	Not applicable	Total
70	0	0	0	0	70

Microsoft Secure Score

Overview | **Recommended actions** | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 182 items | Search | Filter | Group by

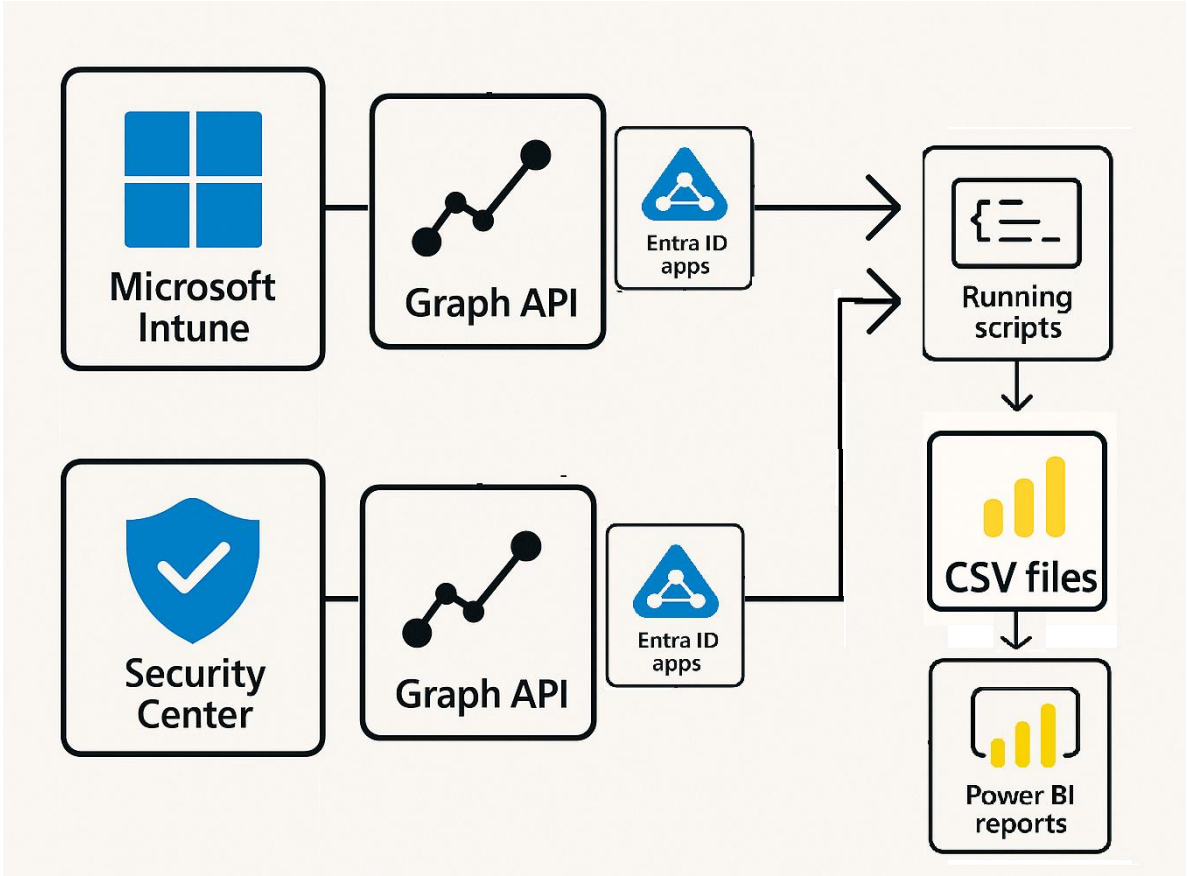
Rank	Recommended action	Score i...	Points achi...	Status	Regress...	Have license?	Cat...	Product
1	Block executable files from running unless they meet a prevalel	+0.86%	0/9	To address	No	Yes	Device	Defender for Endpoint
2	Block persistence through WMI event subscription	+0.86%	0/9	To address	No	Yes	Device	Defender for Endpoint
3	Use advanced protection against ransomware	+0.86%	0/9	To address	No	Yes	Device	Defender for Endpoint
4	Block untrusted and unsigned processes that run from USB	+0.86%	0/9	To address	No	Yes	Device	Defender for Endpoint
5	Block abuse of exploited vulnerable signed drivers	+0.86%	0/9	To address	No	Yes	Device	Defender for Endpoint

Challenge

- How to access all reports from all tenants
- Avoid needing to log onto all tenants and go through different report pages
- Present in an easy to understand and useable format.

Solution

- Use PowerBI
- Run Powershell scripts to call Graph API and extract data to csv files
- Access Programatically via EntraID apps – no log on required
- Process is completely automatic. Script run on schedule and PowerBI refreshed automatically
- Leverages 16 different Intune and Security reports into 8 PowerBi consolidated reports



Power BI Reports

Nexora Solutions

- Device Security
- Non Compliance
- Device Health
- Assets
- Apps
- Security Recommendati...
- Security Incidents
- Email Protection

Customer	Device	User	Last Update - months	OSType	Version	Sku	Last Reported Date	Viruses Detected	Compliance	Malware Protection Enabled	RealTime Protection Enabled	Signature Update Overdue	Tamper Protection Enabled	Firewall Status
Nexora Solutions	Nex-001	David.Thompson@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-001	Karen.Taylor@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-001	Noura.Anderson@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-002	Charles.Moore@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-002	Layla.Garcia@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-002	Richard.Guo@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-002	Elizabeth.Smith@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Noncompliant	TRUE	TRUE	FALSE	TRUE	Disabled
Nexora Solutions	Nex-003	Ahmed.Martinez@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-003	Aisha.Guo@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-003	Patricia.Johnson@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-004		0	Windows 11	24H2				Not Evaluated					
Nexora Solutions	Nex-004	Charles.Yang@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-004	Fatima.Martin@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Compliant	TRUE	TRUE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-004	Ming.Liu@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Noncompliant	TRUE	FALSE	FALSE	TRUE	Enabled
Nexora Solutions	Nex-004	Joseph.Huang@nexorasolutions.com.au	0	Windows 11	24H2	Pro		Clean	Noncompliant	TRUE	TRUE	FALSE	TRUE	Enabled

PowerBI Reports

Nexora Solutions

Customer	Device	User	Policy	Reason
			Default Device Compliance Policy	Is active
Nexora Solutions	Nex-002	Elizabeth.Smith@nexorasolutions.com.au	windows 10 Default Compliance Policy	Firewall
Nexora Solutions	Nex-004	Joseph.Huang@nexorasolutions.com.au	windows 10 Default Compliance Policy	Secure Boot
Nexora Solutions	Nex-004	Ming.Liu@nexorasolutions.com.au	windows 10 Default Compliance Policy	Antivirus
Nexora Solutions	Nex-004	Ming.Liu@nexorasolutions.com.au	windows 10 Default Compliance Policy	Real-time protection
Nexora Solutions	Nex-006	Layla.Tariq@nexorasolutions.com.au	windows 10 Default Compliance Policy	Trusted Platform Module (TPM)
Nexora Solutions	Nex-008	Joseph.Hernandez@nexorasolutions.com.au	Default Device Compliance Policy	Is active
Nexora Solutions	Nex-010	Robert.Zhang@nexorasolutions.com.au	windows 10 Default Compliance Policy	Trusted Platform Module (TPM)
Nexora Solutions	Nex-016	Aisha.Garcia@nexorasolutions.com.au	Default Device Compliance Policy	Is active
Nexora Solutions	Nex-016	Aisha.Garcia@nexorasolutions.com.au	windows 10 Default Compliance Policy	Microsoft Defender Antimalware security intelligence up-to-date
Nexora Solutions	Nex-016	Karen.Taylor@nexorasolutions.com.au	Default Device Compliance Policy	Is active
Nexora Solutions	Nex-029	Mohammed.Haddad@nexorasolutions.com.au	windows 10 Default Compliance Policy	Microsoft Defender Antimalware security intelligence up-to-date
Nexora Solutions	Nex-030	Hassan.Guo@nexorasolutions.com.au	Default Device Compliance Policy	Is active
Nexora Solutions	Nex-033	Fatima.Martin@nexorasolutions.com.au	windows 10 Default Compliance Policy	Secure Boot
Nexora Solutions	Nex-6HF	James.Martin@nexorasolutions.com.au	windows 10 Default Compliance Policy	Secure Boot

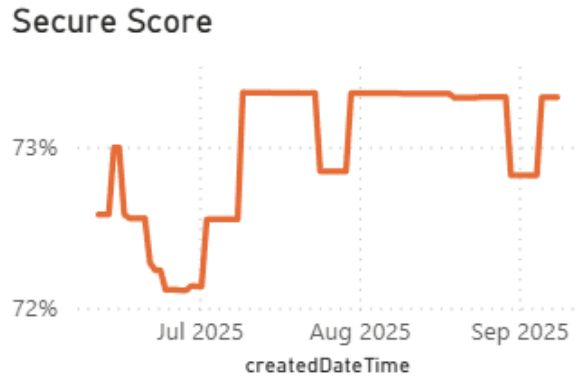
PowerBI Reports

Amberline Publishing

Recommendation Category

- Select all
- Accounts
- Application
- Component
- Network
- OS

CustomerName	Sum of Secure Score
AetherGrid Systems	48.90%
Amberline Publishing	73.31%
BluePeak Analytics	76.45%
BrightForge Studios	44.16%
Cloudmere Networks	48.06%
Cobalt Finch Finance	46.30%
Crimson Oak Ventures	71.36%
Driftwood & Co.	40.29%
EchoNest Media	67.53%
Everpine Wellness	47.09%
Forge & Feather Marketing	47.25%
Total	**2591.52%**



CustomerName	Vendor	Security Recommendation	Related Component	Impact	Remediation Type	Exposed Devices	Category
Amberline Publishing	microsoft	Update Microsoft Visual C++	Visual C++	35.87	Update	6	Application
Amberline Publishing	microsoft	Update Microsoft Teams	Teams	34.63	Update	6	Application
Amberline Publishing	openssl	Attention Required: vulnerabilities in Openssl	Openssl	30.50	AttentionRequired	6	Component
Amberline Publishing	microsoft	Block persistence through WMI event subscription	Windows 11	21.00	ConfigurationChange	6	Security contro
Amberline Publishing	microsoft	Block process creations originating from PSExec and WMI commands	Windows 11	21.00	ConfigurationChange	6	Security contro
Amberline Publishing	mozilla	Update Mozilla Firefox to version 142.0.1.0	Firefox	14.03	Update	1	Application
Amberline Publishing	microsoft	Update Microsoft Office	Office	13.17	Update	6	Application
Amberline Publishing	7-zip	Update 7-zip to version 25.01.0.0	7-zip	10.27	Update	1	Application
Amberline Publishing	microsoft	Update Microsoft Edge Chromium-based to version 140.0.3485.54	Edge Chromium-based	10.27	Update	6	Application
Amberline Publishing	apple	Update Apple Itunes to version 12.13.7.1	Itunes	6.67	Update	1	Application
Total				**264.71**		**211**	

PowerBI Reports

Nexora Solutions

Email Protection Statistics past 30 days

16K	12K	26K	1002	6%	264	2%
Inbound	IntraOrg	InboxCount	JunkCount	Junk % of Inbound	QuarantineCount	Quarantine % of inbound

CustomerName	Timestamp	Sender From Address	Recipient Email Address	Subject
Nexora Solutions	26/08/2025 11:18:12 AM	Charles.Basil@neonemberentertainment.com.au	Patricia.Johnson@nexorasolutions.com.au	TS2-00653 Tidal River Visitor Centre: RFI #48 - Clash Betweer Bolt Cages and Screw Pile Heads ? New Toilet Block has been
Nexora Solutions	26/08/2025 11:18:14 AM	Charles.Basil@neonemberentertainment.com.au	William.Rahman@nexorasolutions.com.au	TS2-00653 Tidal River Visitor Centre: RFI #48 - Clash Betweer Bolt Cages and Screw Pile Heads ? New Toilet Block has been
Nexora Solutions	3/09/2025 9:38:52 AM	David.White@cobaltfinchfinance.com.au	Hua.Rahman@nexorasolutions.com.au	"Detailed drawings", "Window detail" and 5 other boards insp recent activity

Advantages of PowerBI

- Easily customisable to your needs
- Swap fields, add or delete columns
- What ever colour you like.
- Can incorporate other sources (ie ticket stats, license info)
- Can be added to Customers own PowerBI tenant for instant update

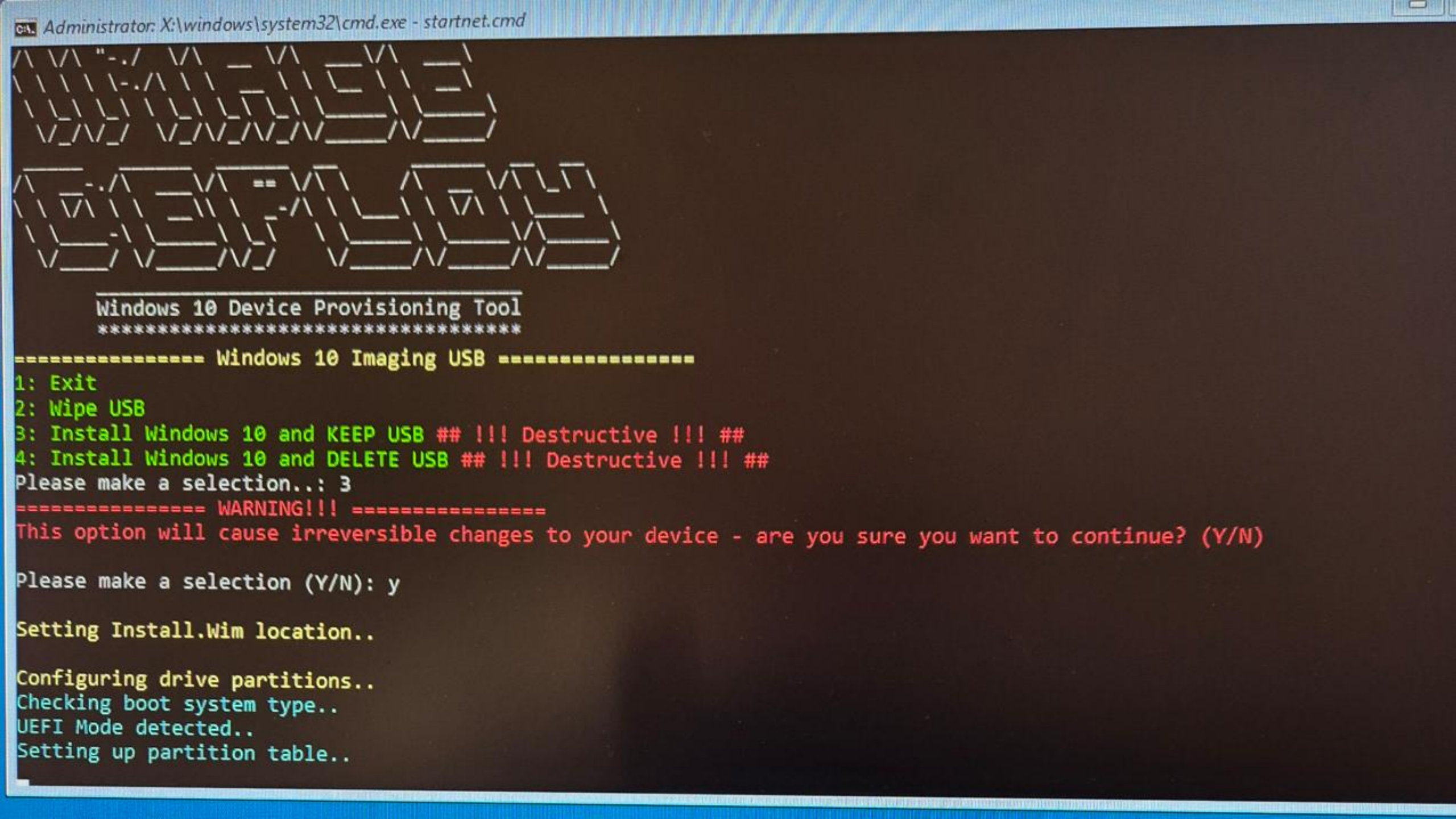
Implementation

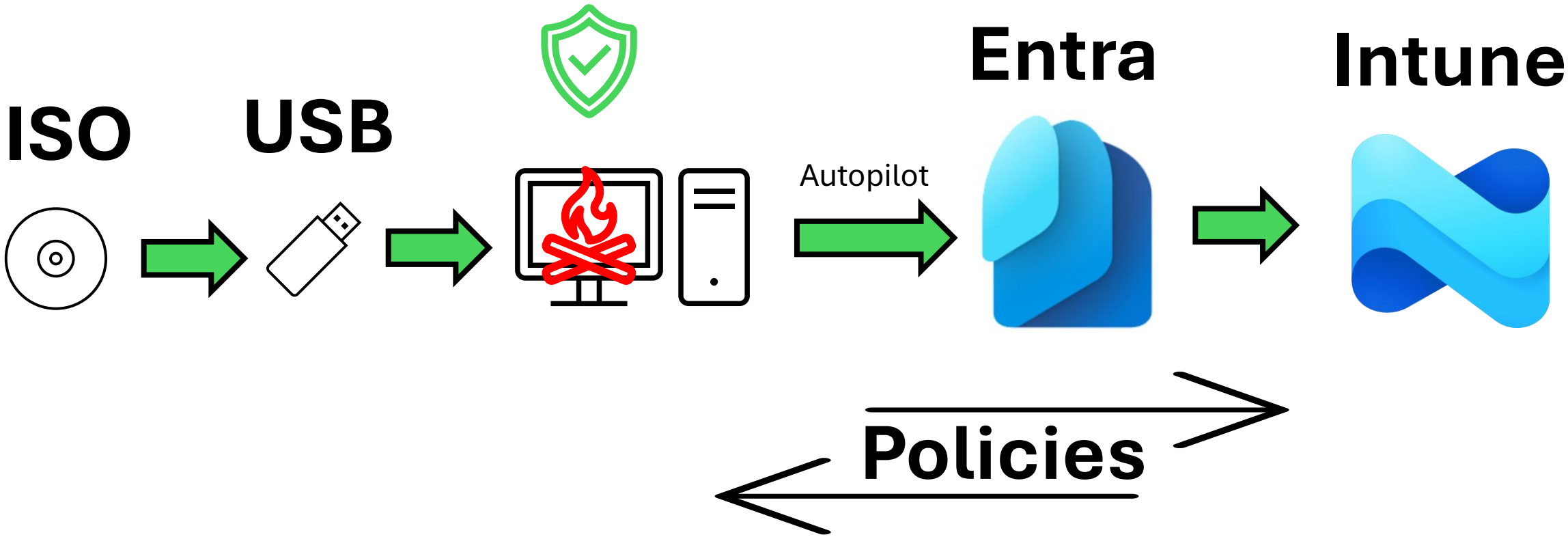
- For the recipe and ingredients – John Braakhuis john@excelero.com.au
- Scripts, Sample data, PowerBi Report and instructions.
- Skill set in EntraID apps, Powershell, PowerBI is helpful
- Reuseable skills
- Positions you as an expert
- DIY is better than anything you can buy

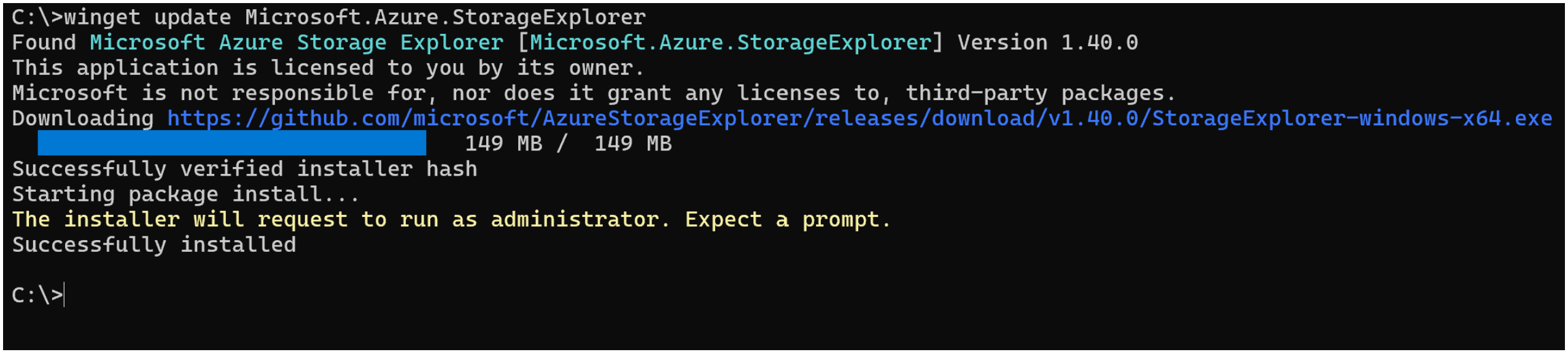
USB Autopilot imaging

Main issues were

- Bloatware installed on device with wasted time of removal.
- Ability for AutoPilot deployment.
- 100% new I had a fresh install of Windows with now outside interference.
- The ability to have anyone do this would be great due to distances of clients.


Administrator: X:\windows\system32\cmd.exe - startnet.cmd
Windows 10 Device Provisioning Tool
Windows 10 Imaging USB
1: Exit
2: Wipe USB
3: Install Windows 10 and KEEP USB ## !!! Destructive !!! ##
4: Install Windows 10 and DELETE USB ## !!! Destructive !!! ##
Please make a selection..: 3
WARNING!!!
This option will cause irreversible changes to your device - are you sure you want to continue? (Y/N)
Please make a selection (Y/N): y
Setting Install.Wim location..
Configuring drive partitions..
Checking boot system type..
UEFI Mode detected..
Setting up partition table..


ISO
USB
Entra
Intune
Autopilot
Policies


C:\>winget update Microsoft.Azure.StorageExplorer
Found Microsoft Azure Storage Explorer [Microsoft.Azure.StorageExplorer] Version 1.40.0
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
Downloading https://github.com/microsoft/AzureStorageExplorer/releases/download/v1.40.0/StorageExplorer-windows-x64.exe
149 MB / 149 MB
Successfully verified installer hash
Starting package install...
The installer will request to run as administrator. Expect a prompt.
Successfully installed
C:\>

Implementation

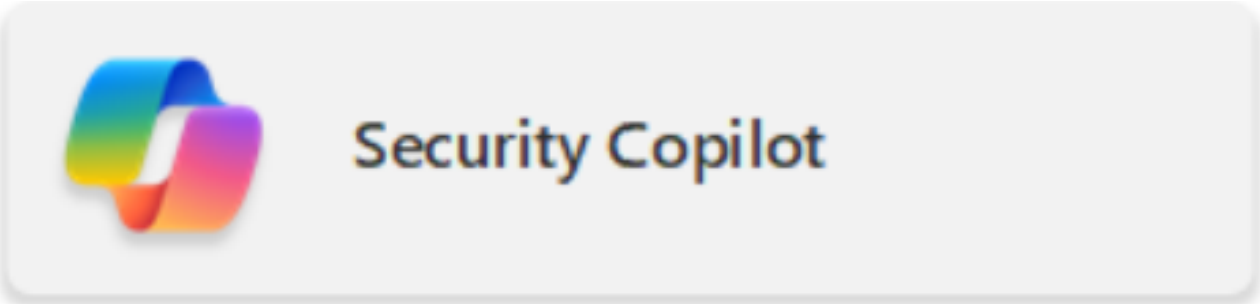
- For the process – Rod Firmer Rodney@caslek.com.au
- Scripts, Utilities, and instructions.
- Skill set in Windows, EntraID, Intune, Autopilot is helpful
- Reuseable skills
- Use what you have before you buy more

Cybersecurity incident response

Main issues were

- Investigation and reporting of a incident for customer
- Understanding how the attack transpired.
- Speed of response to incident.
- Confirmation of any business impact.

Security Copilot



- Use plain English prompts
- Auto generated appropriate KQL log queries
- An external security consultant wanted $10K to perform same actions but it only cost the MSP around $10!
- Retrieve and summarize all evidence of Persistence, Privilege Escalation, Lateral Movement, and Exfiltration activities involving the account in last 180 days, including mailbox rule changes, forwarding setup, group membership or privilege escalation, suspicious sign-ins from new devices or IPs, remote logons, lateral movement to other endpoints, data exfiltration attempts, and any related MITRE techniques. Results are presented in chronological order with details on the type of activity, time, involved devices, IP addresses, and context for each event.

Implementation

- For the process – Allan Michelmore allanm@controlnetworks.com.au
- Experience, set up and usage.
- What happened?
- What was the result?
- How Security Copilot helped

Vibe coding

Main issues were

- Need to report which extensions are blocked by Exchange rules
- Desire something to show customers that is nicely formatted.
- Provide consistent security for customers.

Blocked Attachment Types Analysis

EXTENSION	RISK LEVEL	CATEGORY	DESCRIPTION	COMMON USE	RELATED FILE TYPES
`.a`	LOW	Library/Development	Static Library - Unix/Linux static library archive	Unix/Linux static libraries for linking	`.lib` `.so` `.o` `.dylib`
`.accdb`	MEDIUM	Office Database	Access Database - Microsoft Access database file	Microsoft Access database applications	`.accde` `.mdb` `.mde` `.accdt`
`.accde`	HIGH	Office Database/Executable	Access Execute Only - Compiled Access database	Compiled Microsoft Access databases (executable code)	`.accdb` `.mde` `.mdb`
`.ace`	HIGH	Archive/Compression	WinAce Archive - Compressed archive format that can contain executable files	File compression and archiving	`.rar` `.zip` `.7z` `.arj` `.lzh`
`.action`	MEDIUM	Script/macOS	macOS Automator Action - Automator action	macOS Automator action plugins	`.workflow` `.app` `.scpt`
`.ade`	MEDIUM	Database Extension	Microsoft Access	Microsoft Access database	`.mdb` `.accdb`

Implementation

SOLVE
Business IT Services

- For the process – David Nicholls david@solvebusiness.com.au
- Experience, set up and usage.
- Dev environment setup
- Script

Honourable mentions:

- Privileged Identity Management (PIM)

- Global Secure Access

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, eBooks – http://github.com/directorcia/general
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365, Azure online training courses – http://www.ciaopsacademy.com
- Office 365 and Azure community – http://www.ciaopspatron.com
- CIAOPS Github – https://github.com/directorcia
- CIAOPS Best Practices Github – https://github.com/directorcia/bp

Twitter/X
@directorcia

LinkedIn
http://www.linkedin.com/in/ciaops

Email
director@ciaops.com

Teams
director@ciaops.com

https://bit.ly/ciamm365