zetta

Essential Eight in 2021

Relevance to Current Threat Landscape and Protection With Microsoft Security

Oct 2021

Acknowledgement of Country

We would like to acknowledge the custodians of this land, the Noongar people of the Whadjuk region and recognise their continuing connection to land, waters and communities. We pay our respects to them, their culture and to their Elders past, present and emerging.

Who? What? Why?

- Troy Phillips - Technology Strategist = Can Talk the Talk
- Chris Bell - Principal Technical Architect = Can Walk the Walk

- ACSC/ASD Essential Eight > 10 years
- Major update mid 2021

zetta

Agenda

- Australian Threat Landscape
- Essential Eight (E8) Maturity Model
  - 2021 changes
  - Impact for implementation with Microsoft Security solutions

zetta

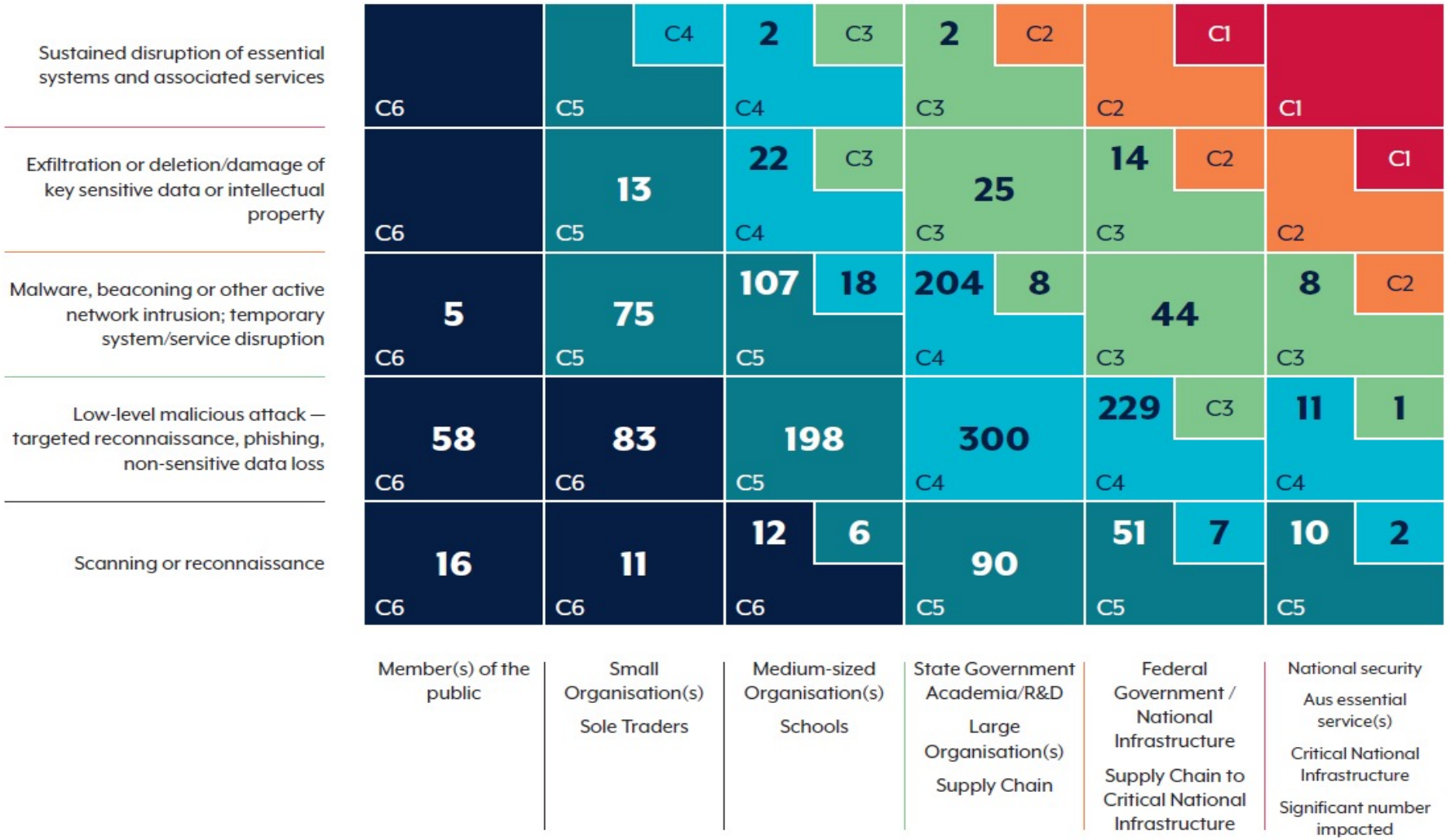
Australian Threat Landscape

- ACSC Cyber Threat Report FY21
- OAIC Notifiable Data Breaches 2021 H1
- Microsoft Digital Defense Report Oct 2021

ACSC Cyber Threat Report FY21

ACSC Cyber Threat - Categorised

Figure 6: Cyber security incidents by incident category for financial year 2020–21



zetta

ACSC Cyber Threat - Ransomware

Most common vectors for deploying ransomware:

- Phishing campaigns,
- targeted spear phishing,
- remote access through vulnerable machines and
- use of publicly available exploits

zetta

ACSC Cyber Threat - Ransomware

ACSC Ransomware Case Study

- Melbourne Metro Public Health Service
- Detected by unauthorised change to GPO
- Offline backups available and not affected by ransomware attack

Worse Alternative…

- Intrusion not detected
- Backups destroyed: reprovision services from scratch?

zetta

ACSC Cyber Threat – Business Email Compromise

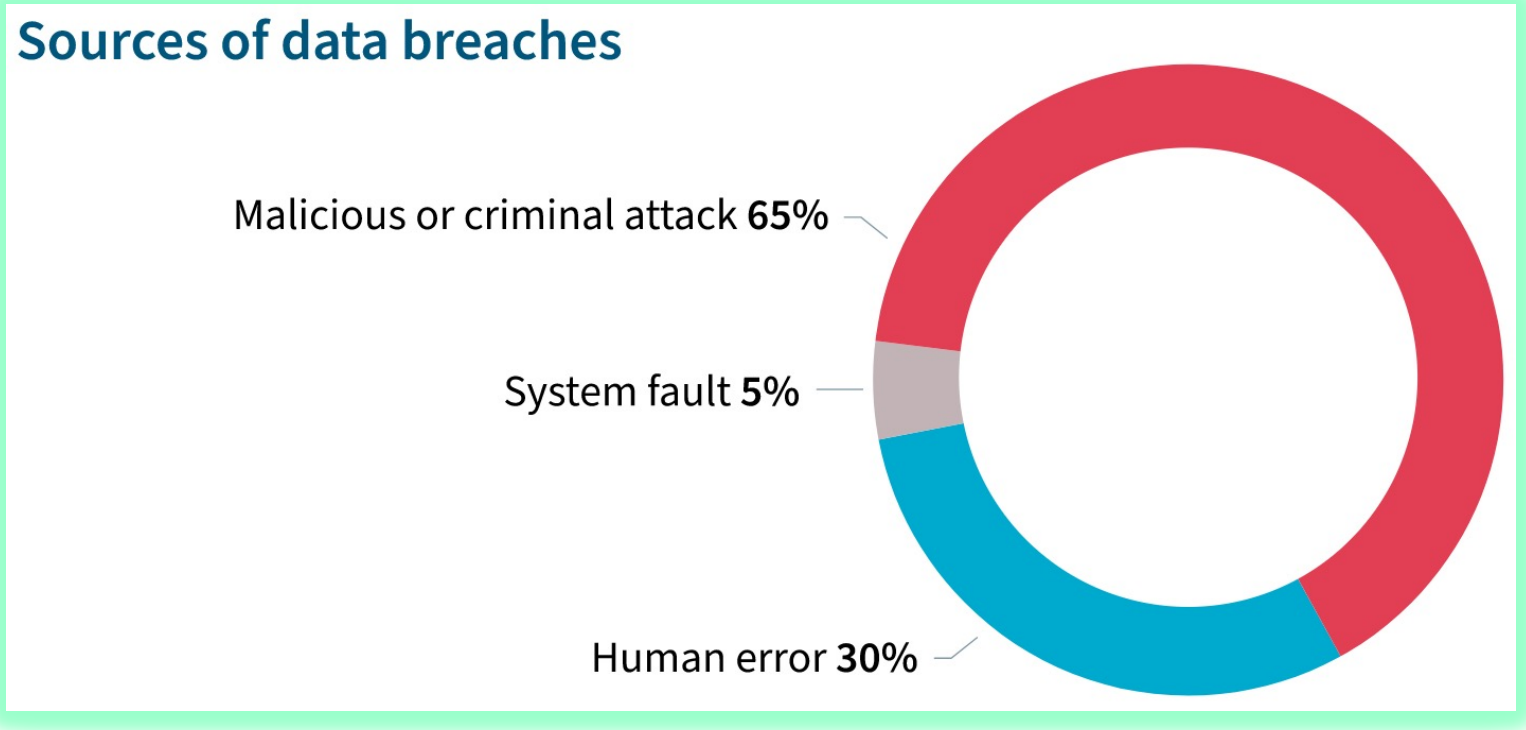
zetta

ACSC Cyber Threat – Business Email Compromise

ACSC BEC Case Study

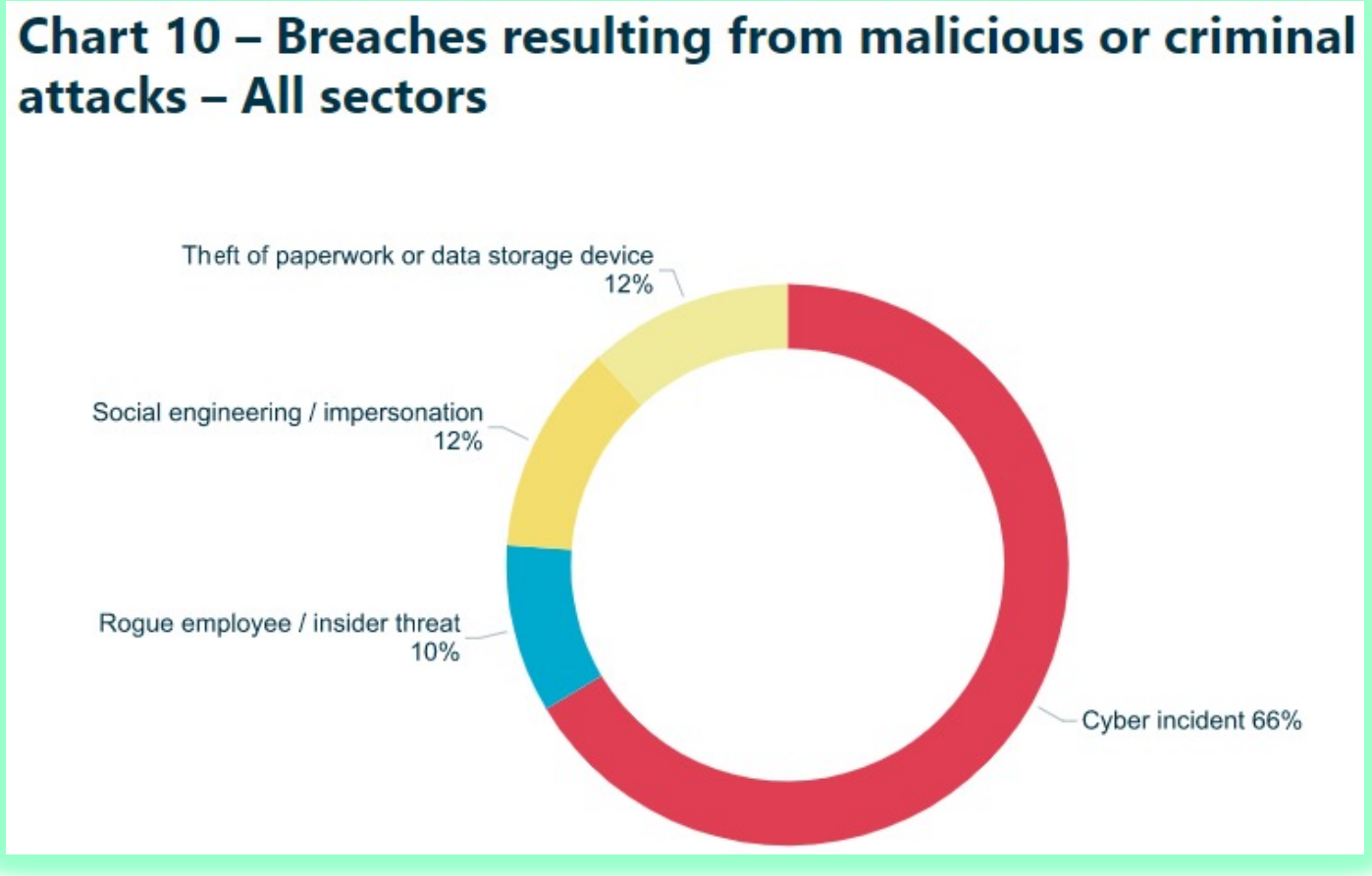
- In Sep 2020, AU Hedge Fund transferred AU$8.7M
- Money most recovered, but main client withdraw due to reputational damage
- AU Hedge Fund into receivership and bankruptcy

OAIC Notifiable Data Breaches Jan–Jun 2021



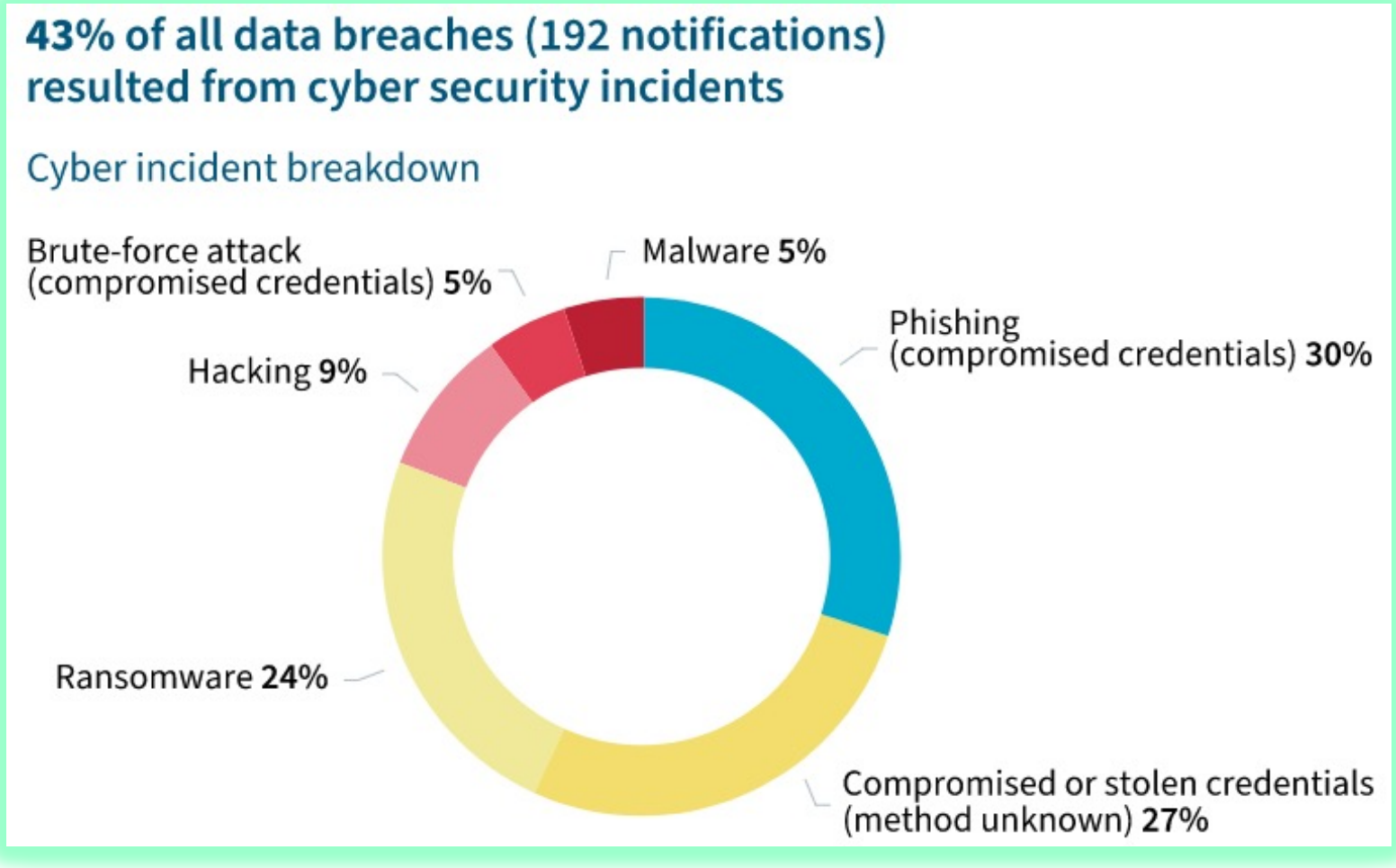
zetta

OAIC Notifiable Data Breaches Jan–Jun 2021



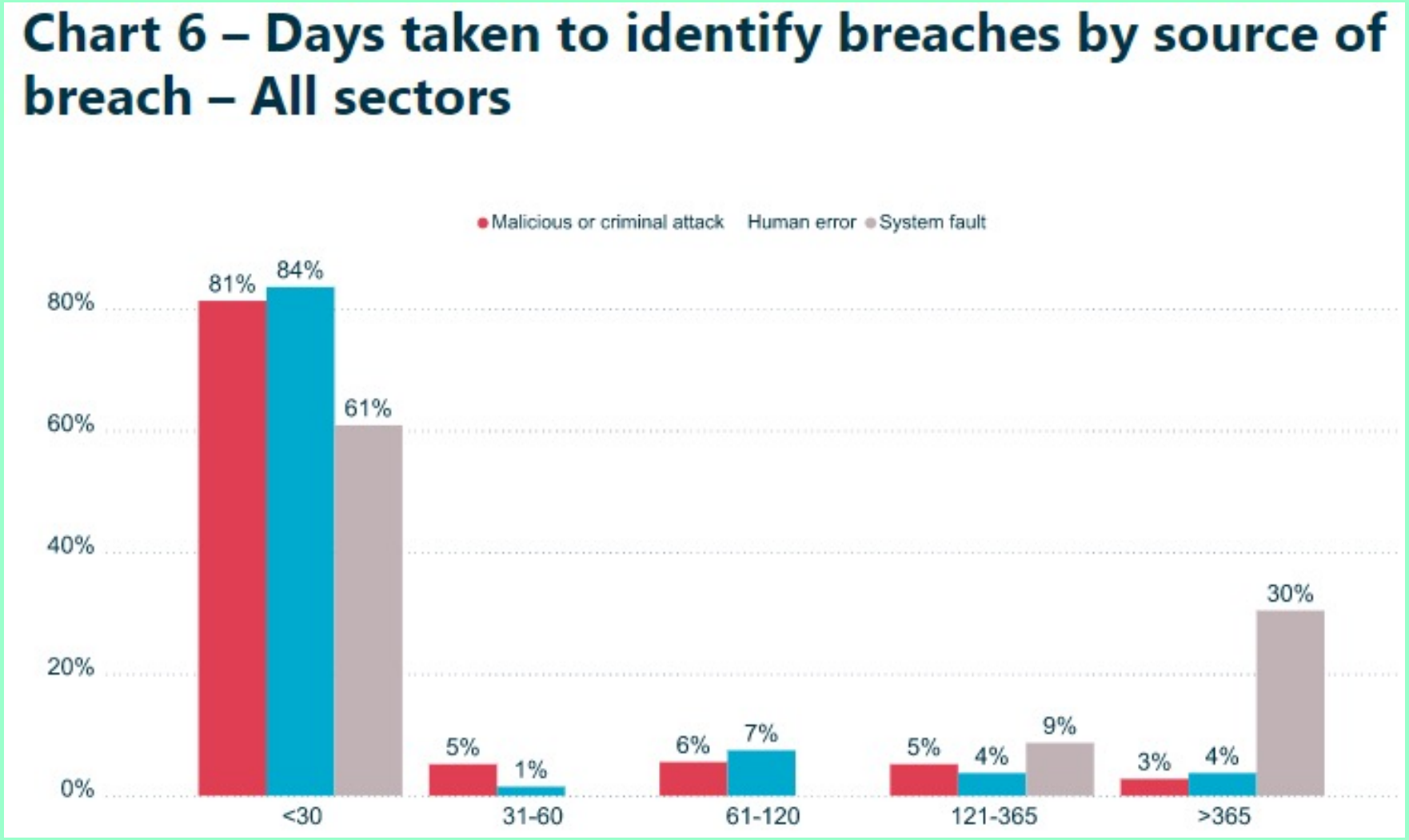
zetta

OAIC Notifiable Data Breaches Jan–Jun 2021



zetta

OAIC Notifiable Data Breaches Jan–Jun 2021

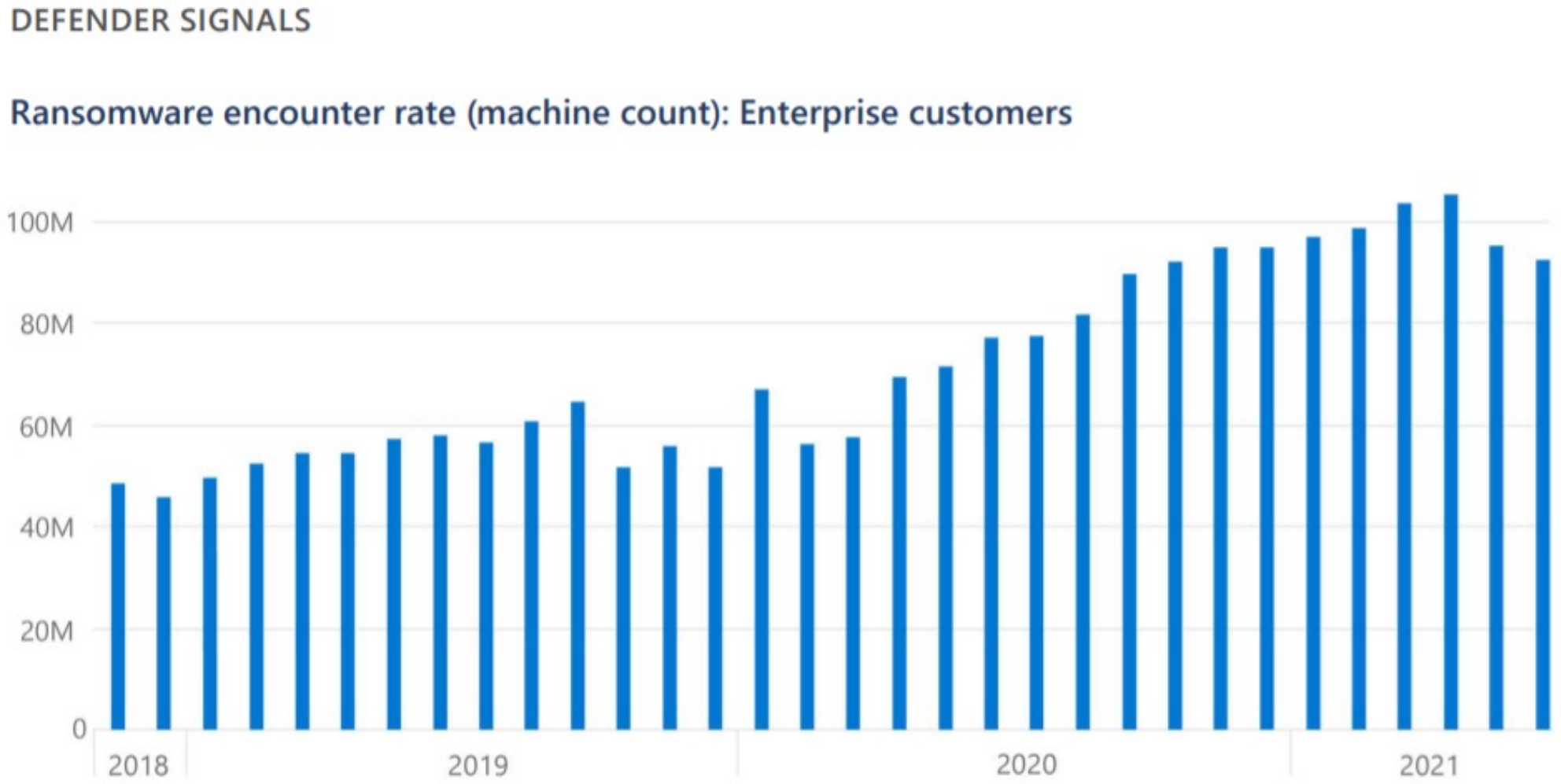


zetta

Microsoft Digital Defense Report FY21

zetta

Microsoft Digital Defense Report FY21



zetta

Microsoft Digital Defense Report FY21

Good news: e-mails with malware on a downward trend

zetta

zetta

Essential Eight (E8) Maturity Model

- Relevance
- 2021 Changes

The Essential Eight

Prevent Delivery and Execution:

1. Application Control
2. Patch Applications
3. Microsoft Office Macro Settings
4. User Application Hardening

Limit Extent of Incidents:

5. Restrict Admin Privileges
6. Patch Operating Systems
7. Multi-factor Authentication

Recover Data/System Availability:

8. Regular Backups

zetta

Is Essential Eight Relevant?

Perspective from critical infrastructure security provider (Aug 2021):

"At the end of the day, most of your customers are not the CIA or a government agency, which is what the Essential 8 was designed for, so it normally just comes down to highlighting the risks and having them understand and accept risks that are not practical to mitigate"

zetta

Is Essential Eight Relevant?

zetta

Microsoft Report Learnings

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks

Seems Familiar…

zetta

Maturity Model – 2021 Changes

- Package Deal: Mitigation strategies assessed as single package
- Focus: “Microsoft Windows-based internet-connected networks”
- Maturity Level 0 back; Levels 1-3 Redefined

zetta

Maturity Levels – 2021 Redefined

2020 Maturity Model
How aligned to “intent of mitigation strategy”?

1 2020 Level 1 (Good Start)

- Partly aligned with intent of mitigation strategy

2 2020 Level 2 (Nearly There)

- Mostly aligned with intent of mitigation strategy

3 2020 Level 3 (Gold Star!)

- Fully aligned with intent of mitigation strategy

2021 Maturity Model
Sophistication of adversary “tradecraft”.

New “Level 0” starting point (Sitting duck for script kiddies)

1 2021 Level 1 (Script kiddie)

SMB Only

- Adversaries using “commodity tradecraft” – publicly available exploit, or stolen/guessed credentials
- Generally common weakness in many targets

2 2021 Level 2 (Semi-Pro)

Large Enterprise

- Adversaries using “well-known tradecraft” – phishing for user credentials, seeking special privileges
- More selective targeting, but still conservative in time & effort

3 2021 Level 3 (Baba Yaga)

Critical Infrastructure (+ High Threat)

- Adversaries adaptive and able to exploit targets weaknesses
- Generally focused on particular targets – willing to invest time and effort

zetta

Essential Eight – Today's Focus

Prevent Malware Delivery and Execution:

1. **Application Control**
2. **Patch Applications**
3. ~~Microsoft Office Macro Settings~~
4. ~~User Application Hardening~~

Limit Extent of Cyber Security Incidents:

5. **Restrict Admin Privileges**
6. ~~Patch Operating Systems~~
7. ~~Multi-factor Authentication~~

Recover Data and System Availability:

8. **Regular Backups**

Defence Industry Service Provider (DISP) Entry Level

zetta

zetta

E8 Maturity Model Updates - Prevent

Prevent Malware Delivery and Execution:

1. **Application Control**
2. **Patch Applications**
3. Microsoft Office Macro Settings
4. User Application Hardening

1. Application Control Maturity Levels

2020 Maturity Level ❶, ❷, ❸

2021 Maturity Level ❶, ❷, ❸

	 Workstations (profile & temp)	 Workstations (other folders)	 Internet-Facing Servers	 Servers
Restrict executables	❶ ❶	❶ ❷	❶ ❷	❶ ❸
Restrict software libraries, scripts and installers	❷ ❶	❷ ❷	❷ ❷	❷ ❸
Restrict compiled HTML, HTML apps and control panel applets (❸revalidate rulesets annually)	❶	❷	❷	❸
Restrict drivers	❸	❸	❸	❸
Implement Microsoft 'recommended block rules' to prevent application control bypass (❸driver block rule)	❸ ❸	❸ ❸	❸ ❸	❸ ❸
Log allow/block (❸centrally logged, protected, monitor for compromise, and action cyber events)	❷	❷	❷	❸

zetta

1. Application Control Guidance

Implementing Application Control Guidance from the ACSC:

When determining how to enforce application control, the following methods are considered suitable if implemented correctly:

- Cryptographic hash rules
- Publisher certificate rules (combining both publisher names and product names)
- Path rules (ensuring file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents and individual files).

Conversely, the use of file names, package names or any other easily changed application attribute is not considered suitable as a method of application control.

zetta

1. Application Control WDAC or AppLocker

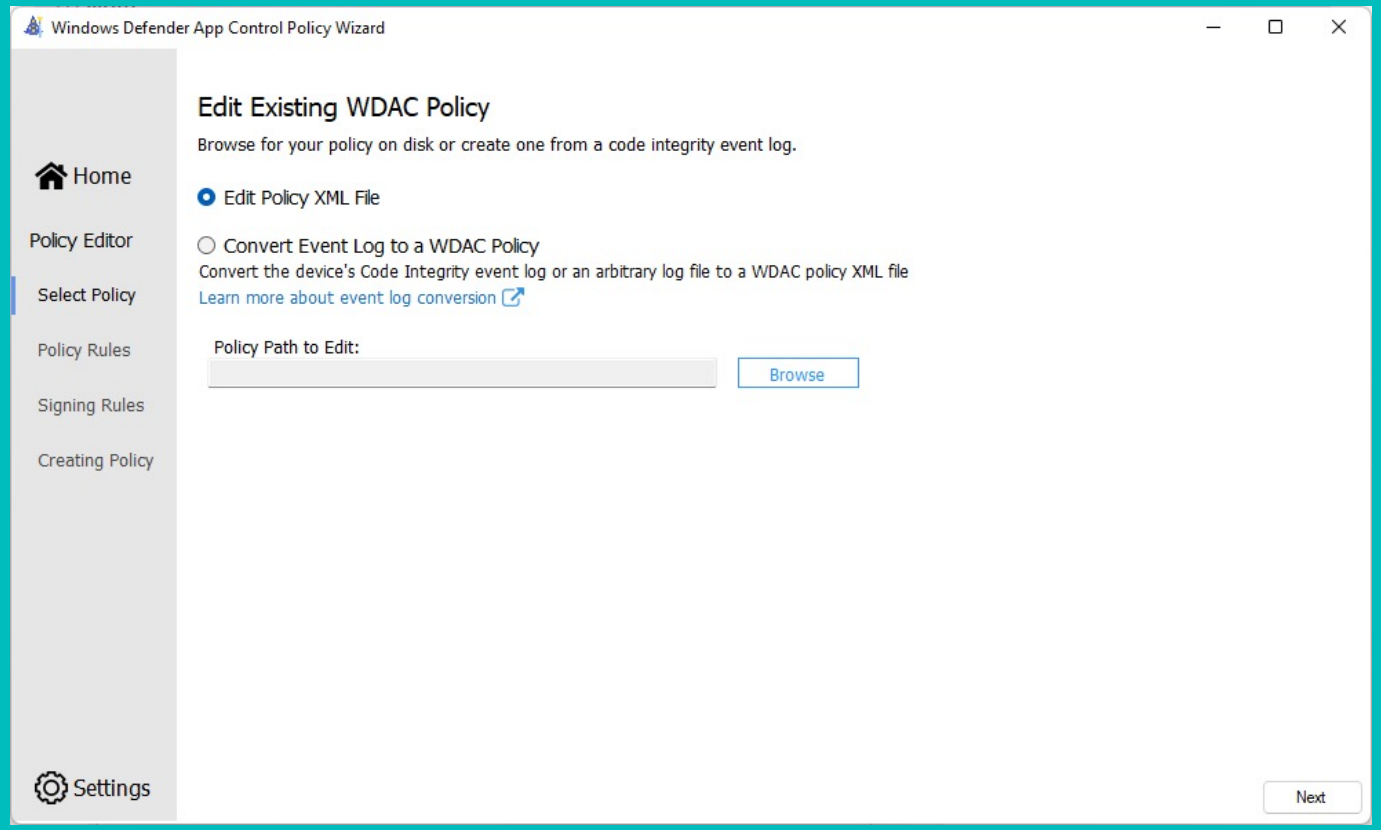
Windows Defender Application Control (WDAC)

- **Applies to the Device only (AppLocker can be either User or Device)**
- **Enables control of which Drivers can run**
- **Improves upon AppLocker by adding:**
  - The reputation of the app as determined by Microsoft's Intelligent Security Graph
  - The identity of the process that initiated the installation of the app and its binaries (managed installer)
  - The path from which the app or file is launched (beginning with Windows 10 version 1903)
  - The process that launched the app or binary
- **Policies now deployable using MEMCM, Intune, Group Policy or Script**
  - Code Integrity Policies configure WDAC
  - MEMCM and Intune can manage the deployment of WDAC Policies
- **Reference machines can be scanned to create baseline WDAC Policies**
  - **Supplemental Policies can be created to expand upon existing Base Policies**
- **Auditing logs to Event Logs, or captured by Defender for Endpoint Advanced Hunting**

zetta

1. WDAC Wizard

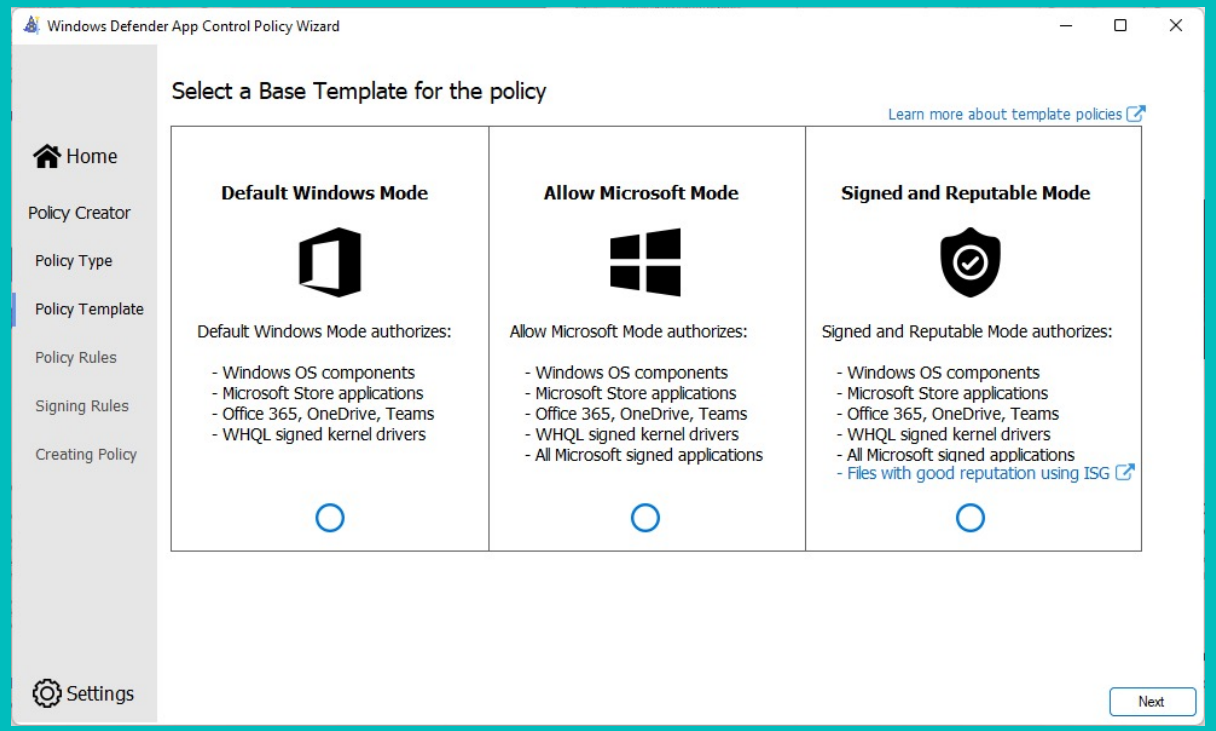
The WDAC Wizard can be used to Define or Edit policies

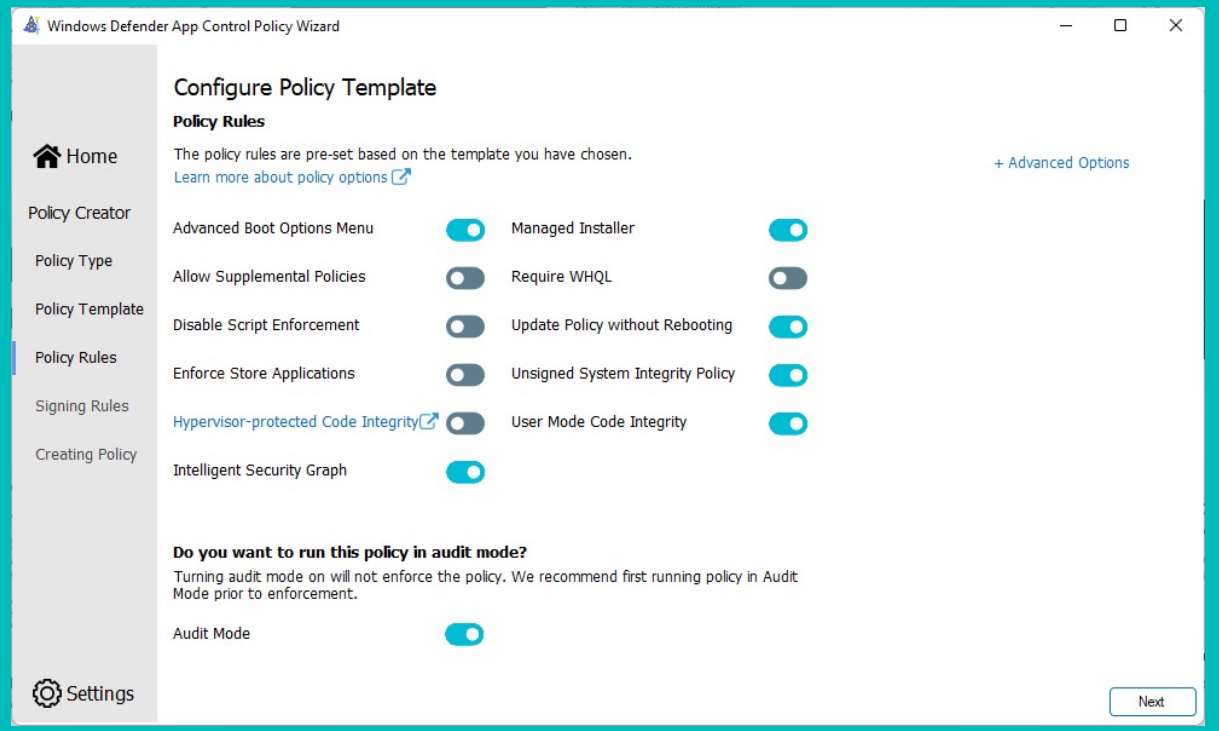


zetta

1. WDAC Wizard Templates

Configurable options for new Base Templates





zetta

2. Patch Applications Maturity Levels

2020 Maturity Level ❶, ❷, ❸

2021 Maturity Level ❶, ❷, ❸

	 'Extreme Risk' Vulnerabilities	 Internet-Facing Services	 'Higher Risk' Apps	 Other Apps
Patches, updates or vendor mitigation for security vulnerabilities ('higher risk' = office productivity suites, web browsers and their extensions, email clients, PDF software, *Adobe Flash Player*, and security products)	❶ 1 month ❷ 2 weeks ❸ 48 hrs	❶ 2 weeks (or 48 hrs) ❷ ❸	❶ 1 month ❷ 2 weeks ❸ 2 weeks (or 48 hrs)	❸ 1 month
Vulnerability scanner used to identify missing patches or updates for security vulnerabilities	❸	❶ daily ❷ daily ❸ daily	❶ fortnightly ❷ weekly ❸ weekly	❸ ?
Remove apps no longer supported by vendors	❶ ❷ ❸	❶ ❷ ❸	❶ ❷ ❸	❶ ❷ ❸ ❸

zetta

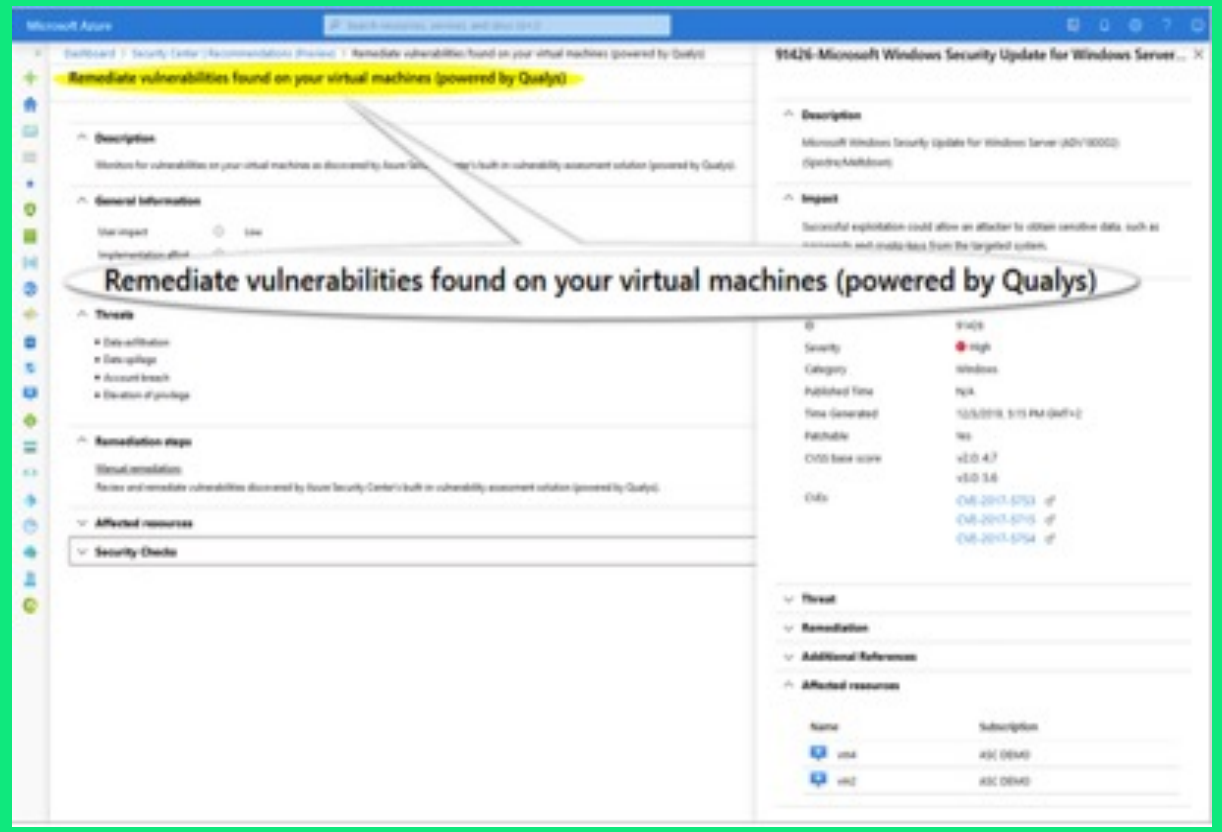
2. Patch Applications Vulnerability Assessment

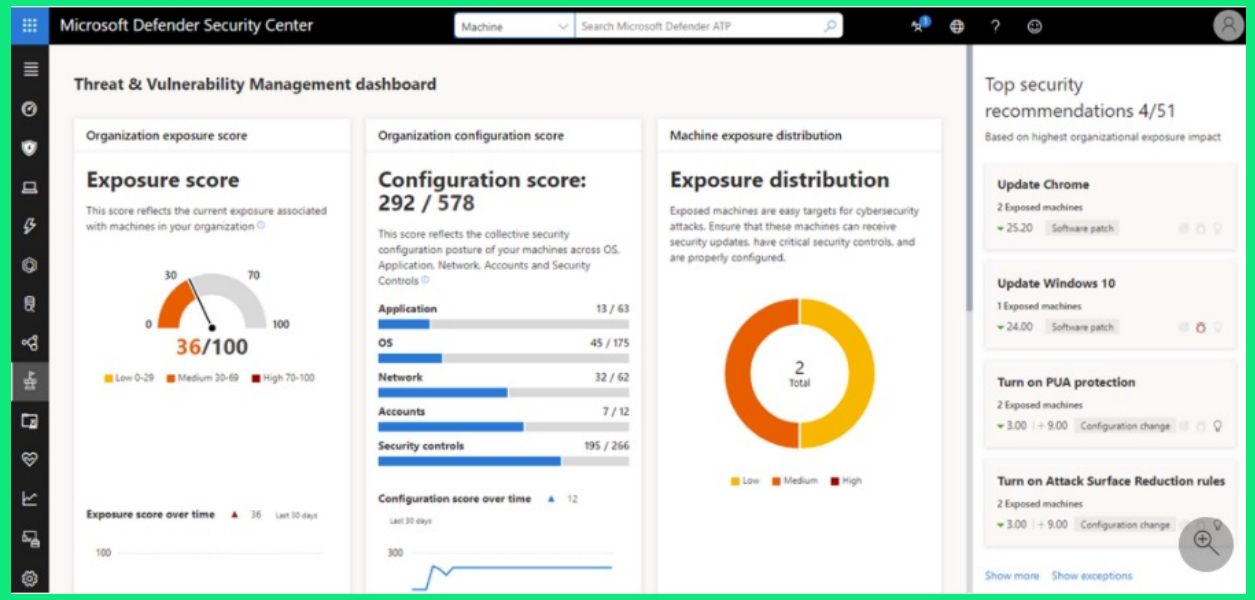
Deploy a Vulnerability Assessment solution:

- Defender for Endpoint Vulnerability Reporting
- Azure Security Center (Qualys)
- Australian Cyber Security Centre (ACSC)
- Monitor Common Vulnerabilities and Exposures (CVE)
- Microsoft Security Response Centre (MSRC)

zetta

2. Patch Applications Vulnerability Assessment



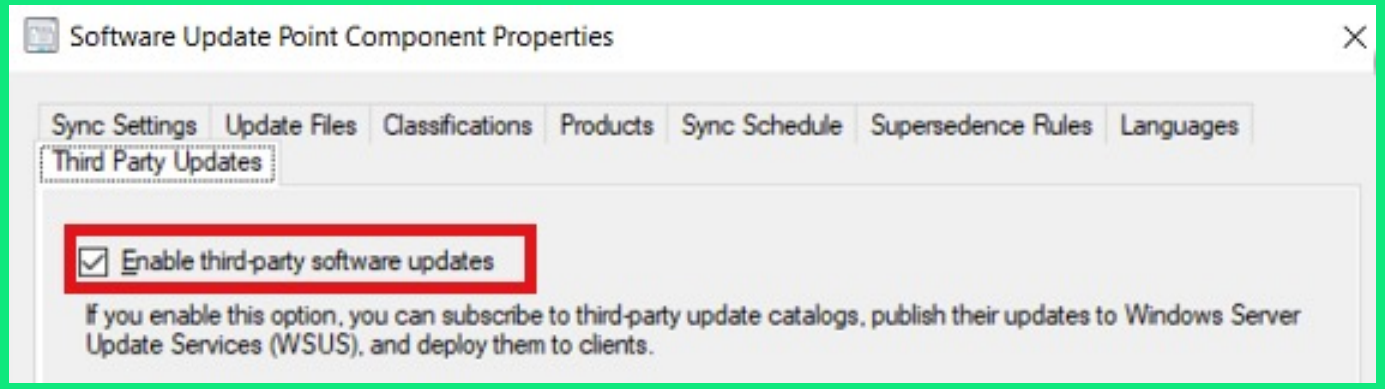


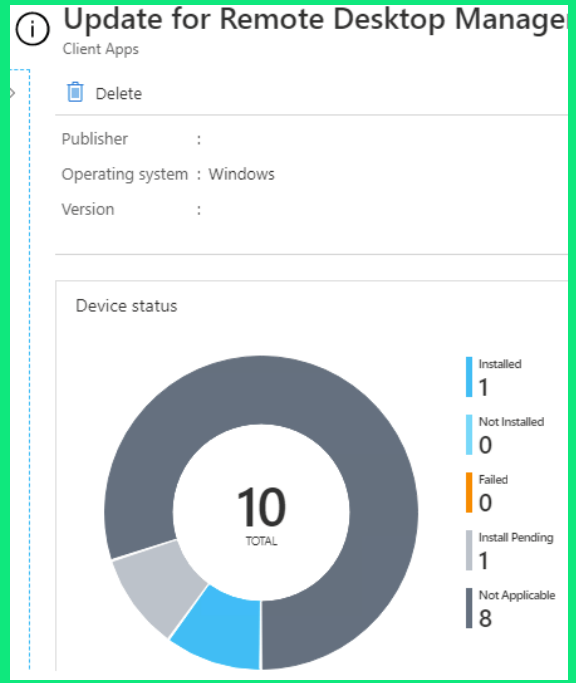
zetta

2. Patch Applications Third Party Updates

Managing 3rd party application updates is challenging

- Constrained to Internet Facing services, Browsers, and PDF Readers until Maturity Level 3
- Third-party Update Catalogs with Configuration Manager
- Third-party App update tool for Intune leveraging Win32 Applications





zetta

zetta

E8 Maturity Model Updates – Limit Extent

Limit Extent of Cyber Security Incidents:

5. **Restrict Admin Privileges**
6. Patch Operating Systems
7. Multi-factor Authentication

5. Restrict Admin Privileges Maturity Levels

2020 Maturity Level ❶, ❷, ❸

2021 Maturity Level ❶, ❷, ❸

Validated

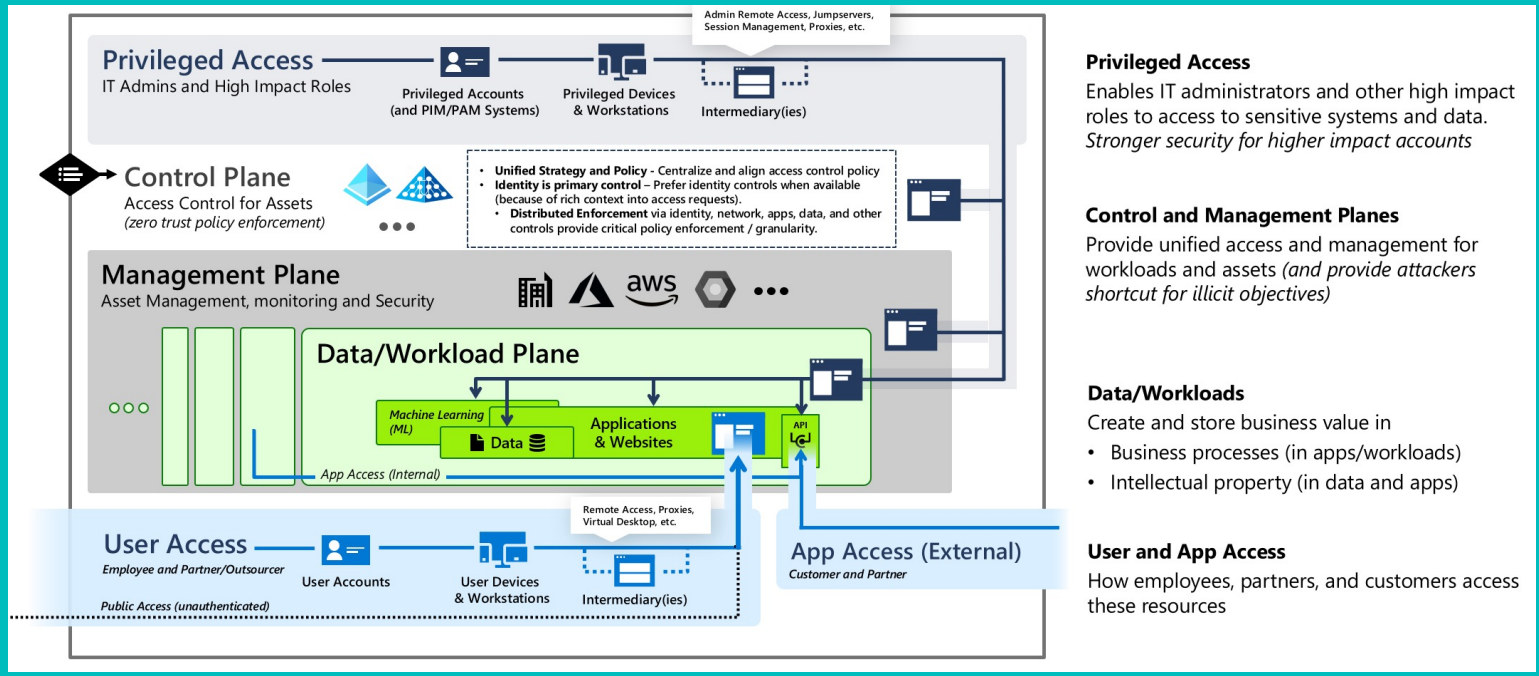
Disabled

Privileged Access	❶ At request ❷ At request ❸ + annually	❶ At request ❷ At request ❸ + annually	❷ Validate >12 mths. ❸ OR 45 days inactive
(Interactive) Privileged Account: No internet, email, web services	❶❷❸	❶❷❸	
Separate privileged/unprivileged operating environments	❷❸		
Use jump servers; local admin & service account passwords 'tricky'	❷❸		
Log use/change (❸central log, protected, monitor for compromise, action cyber events)	❷❸		
Privileged OE not VM in unprivileged			❸
JIT Admin			❸
Windows Defender Credential Guard and Windows Defender Remote Credential Guard			❸

zetta

5. Restrict Admin Privileges Enterprise Access Model

- Supersedes AD Tiering and Red Forest Models
- Consists of multiple ‘Planes’ to segregate identity usage within the environment
- Leverages PIM/PAM Systems, and Privileged Access Devices
- Mitigate unauthorized privilege escalation by preventing control of higher planes from lower planes

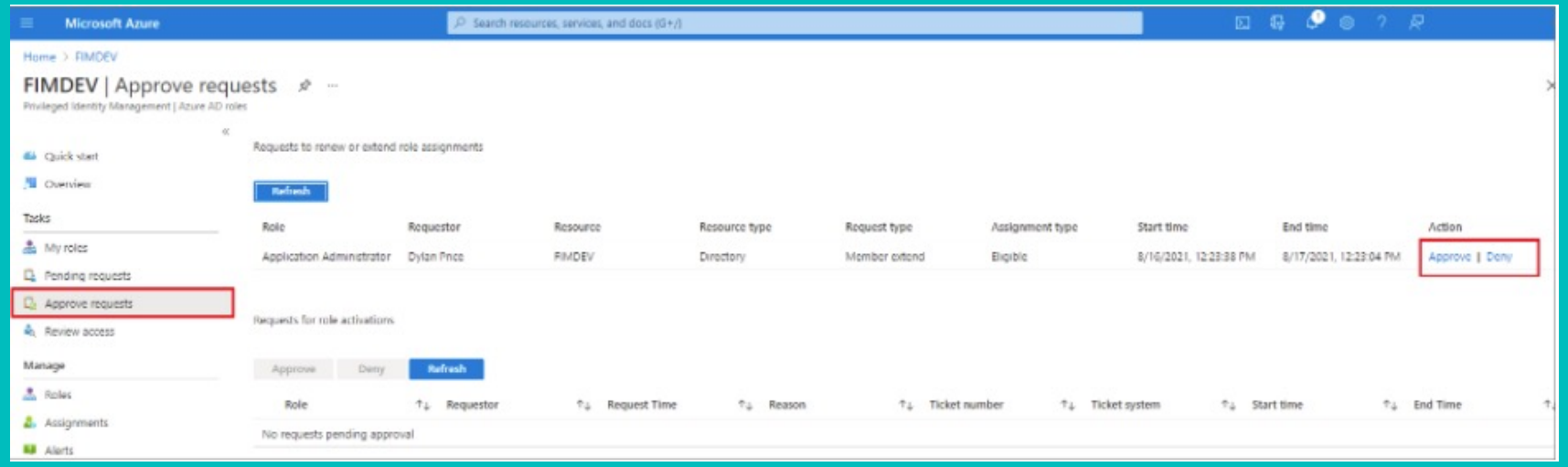


zetta

5. Restrict Admin Privileges PIM

Azure AD Privileged Identity Management (PIM)

- Time-bound, just-in-time access
- Configure to require justifications, approval, and MFA enforcement
- Enables notifications, access reviews and audit history

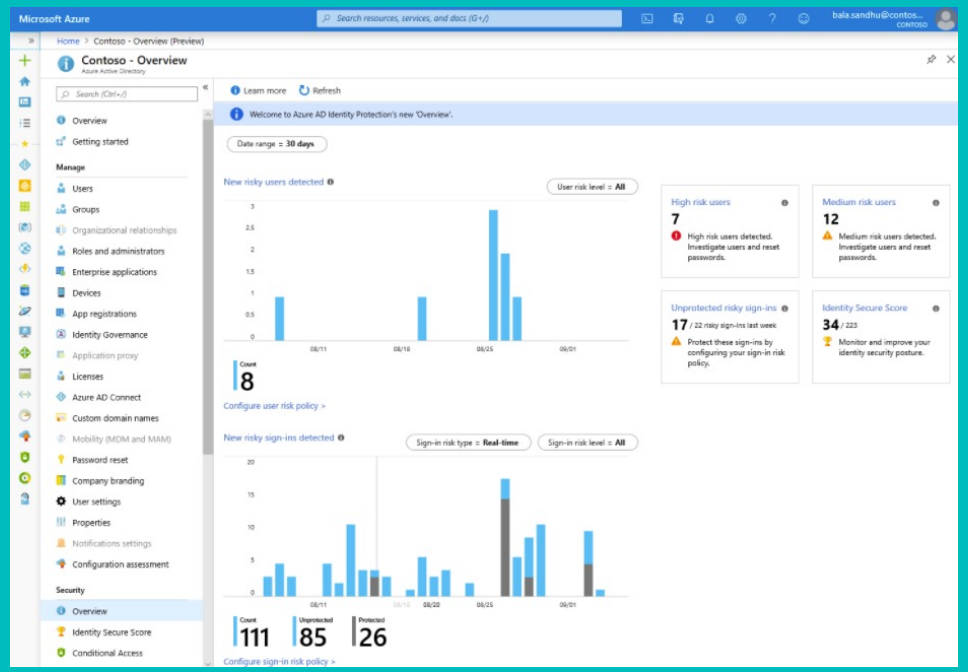


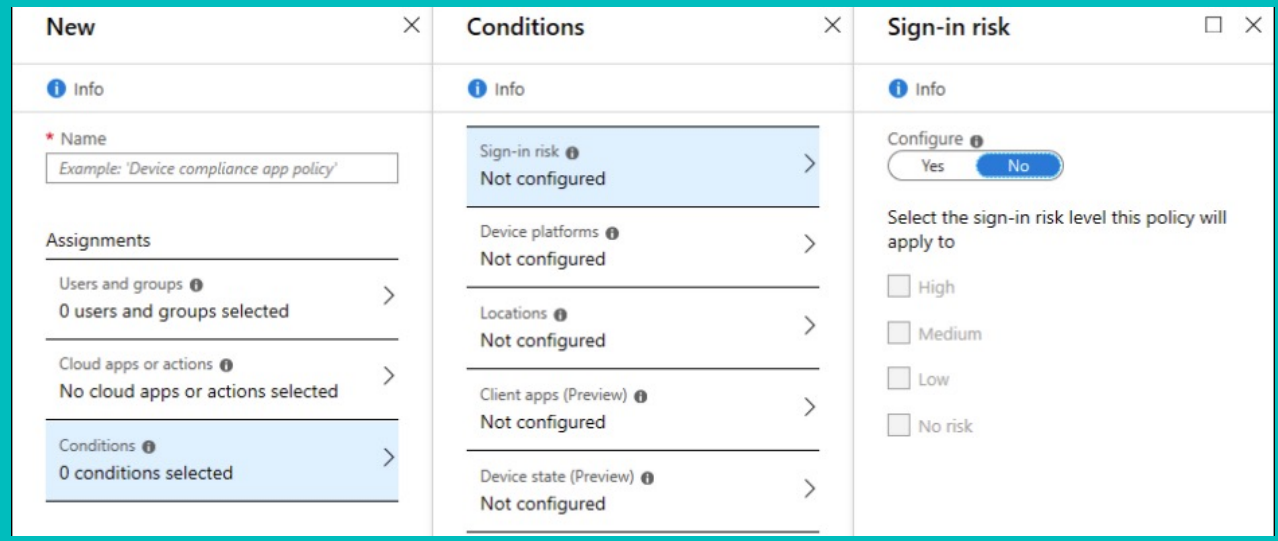
zetta

5. Restrict Admin Privileges Identity Protection

Azure AD Identity Protection

- Identify Risky Users and Sign-ins and take actions on these events



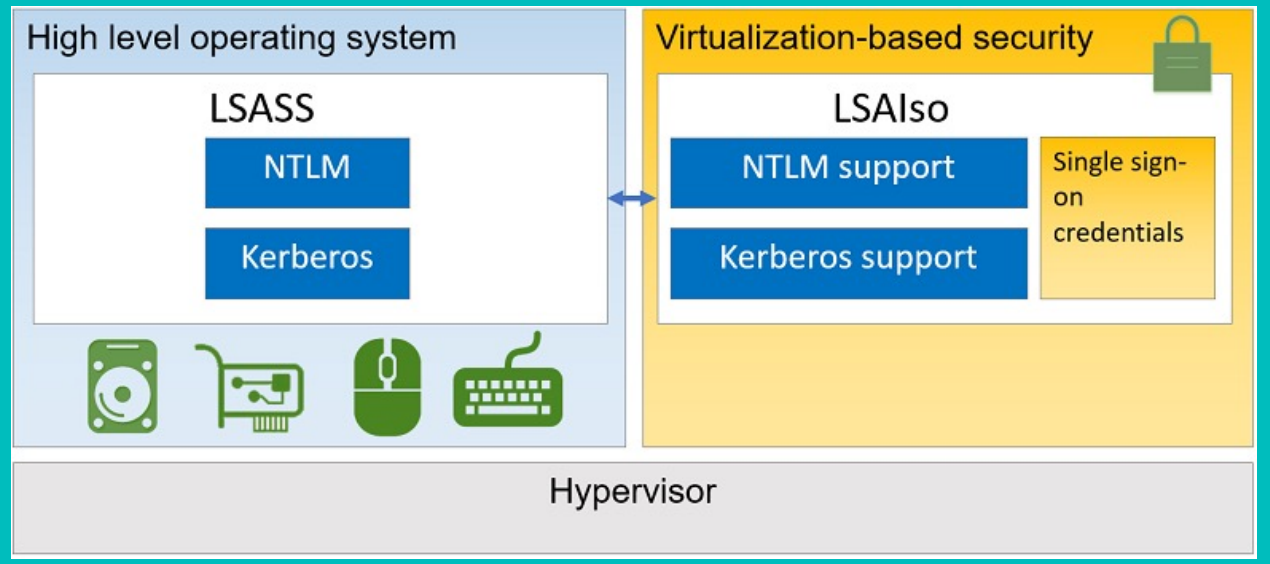


zetta

5. Restrict Admin Privileges Credential Guard

Windows Defender Credential Guard

- Isolates Local Security Authority (LSA) process
- Protecting NTLM password hashes, Kerberos TGTs, and credentials stored by applications
- Does not apply to Local or Microsoft Accounts
- Breaks legacy authentication and encryption such as NTLMv1 and Kerberos Unconstrained Delegation



zetta

E8 Maturity Model Updates - Recover

Recover Data and System Availability:

8. **Regular Backups**

8. Regular Backups Maturity Levels

2020 Maturity Level ❶, ❷, ❸

2021 Maturity Level ❶, ❷, ❸

	Perform Backup	Retain Backup	Test Restore (Full/Partial)
Backup important info, software and config	❶ monthly ❶ Per BC ❷ weekly ❷ Per BC ❸ daily ❸ Per BC	❶ monthly ❶ Per BC ❷ weekly ❷ Per BC ❸ daily ❸ Per BC	❶ NA/partial ❶ Per DR ❷ 1 / bi-annual ❷ Per DR ❸ Big changes /quarterly ❸ Per DR

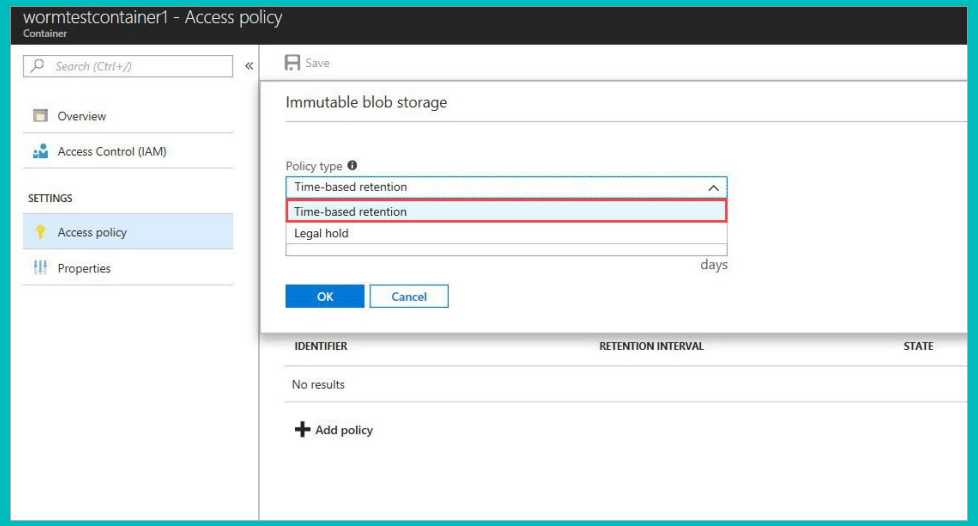
	Unprivileged Users	Backup Admins	Other Privileged Users
Block backup delete/modify (❸ or backup offline)	❶ ❷ ❷ ❸ ❸	❷ ❸	❷ ❷ ❸ ❸
Access backups	❶ Only own ❷ Only own ❸ None		❷ Only own ❸ None

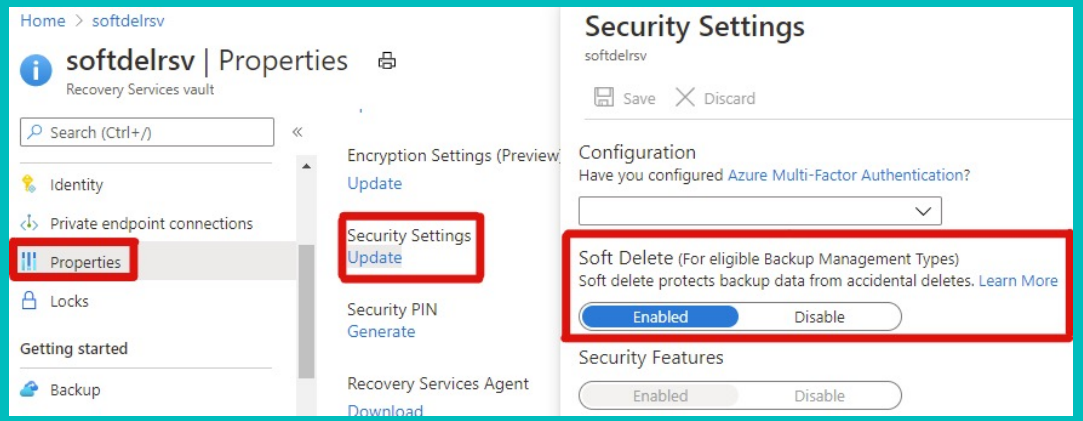
zetta

8. Regular Backups - Integrity

Protect Backup Integrity

- Azure Backup Soft Delete (Partial Protection)
- Immutable Azure Blob Storage with Time-based retention policies





zetta

8. Regular Backup

Limit Access to Backup Systems and Storage

- Implement MFA for Backup Software
- Enforce MFA when connecting to any Backup Systems

Create Runbooks for Data Recovery

- Understand the order for recovery
- Ensure Recovery processes are defined and tested

zetta

zetta

Wrap Up

Take Home - Call to Action

- Review current Essential Eight Maturity Model (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model) and the FAQ (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq)
- Nominate target Maturity Level (Enterprise at least 2, Critical Infrastructure 3)
- Assess the gap
- Remediate (E5 Security helps!)

zetta

Microsoft 365 Enterprise Benefits

FastTrack	FastTrack helps customers deploy Microsoft 365. Customers with 150+ eligible licenses can use FastTrack at no additional cost for the life of their subscription.
Office Professional Plus	One traditional Office Professional Plus device install for each existing Software Assurance (SA) user, and new users up to the number of existing from SA users.
Office Servers	Install SharePoint, Exchange, and Skype for Business Server, on dedicated hardware (not multi-tenant), for use by Microsoft 365 E3 & E5 licensed users. Excludes CSP/MCA.

Related Services

10-Year Audit Log Retention	Built-in long-term storage of audit logging data	Additional Storage	Additional storage for Office 365
Advanced Comms	Branding, monitoring, and meetings analysis	AI Builder Capacity	Extra capacity for AI Builder
Azure Purview	On-prem, multi-cloud, and SaaS data governance	Azure Sentinel	AI-enhanced cloud-native SIEM
Calling Plans	PSTN telephony calling plans	Compliance Premium Assessments	Compliance Manager premium assessment templates
Defender for Endpoint (Server)	Defender for Endpoint Server (Windows / Linux)	Dynamics 365 Customer Voice	More sophisticated surveys and customer feedback
Extra Graph Connector Capacity	Additional capacity for Microsoft Search and Graph	MCAS App Governance (preview)	Advanced app governance and monitoring
Microsoft Dataverse	Services for low-code application development	Microsoft Managed Desktop	Microsoft device management and monitoring
Multi-Geo	Split a tenancy over multiple geographies	Power Apps	The complete low-code/no-code app-dev platform
Power Automate	Advanced process automation features	Power BI Premium	More capacity and scale for business intelligence
Power Virtual Agents	Intelligent agents and bots	Privacy Management (preview)	Manage personal data in Microsoft 365
Project Online	Microsoft Project	Scheduler	Schedule meetings with the help of Cortana
SharePoint Syntex	AI knowledge extraction and analysis	Teams Operator Connect	Teams PSTN connection hosted as-a-service
Teams Rooms	Enable meeting room devices	Visio Online	Microsoft Visio
Viva Connections (preview)	Teams embedded intelligent intranet experiences	Viva Insights	Employee productivity and wellbeing insights
Viva Learning (coming soon)	Complete learning management platform in Teams	Viva Topics	Integrated knowledge & experts discovery
Windows 365 (Cloud PC)	Windows desktop as a subscription cloud service	Workplace Analytics	Analyse workplace trends and efficiencies

zetta

Q&A Discussion

www.zetta.com.au

linkedin.com/company/zetta-group

zetta