

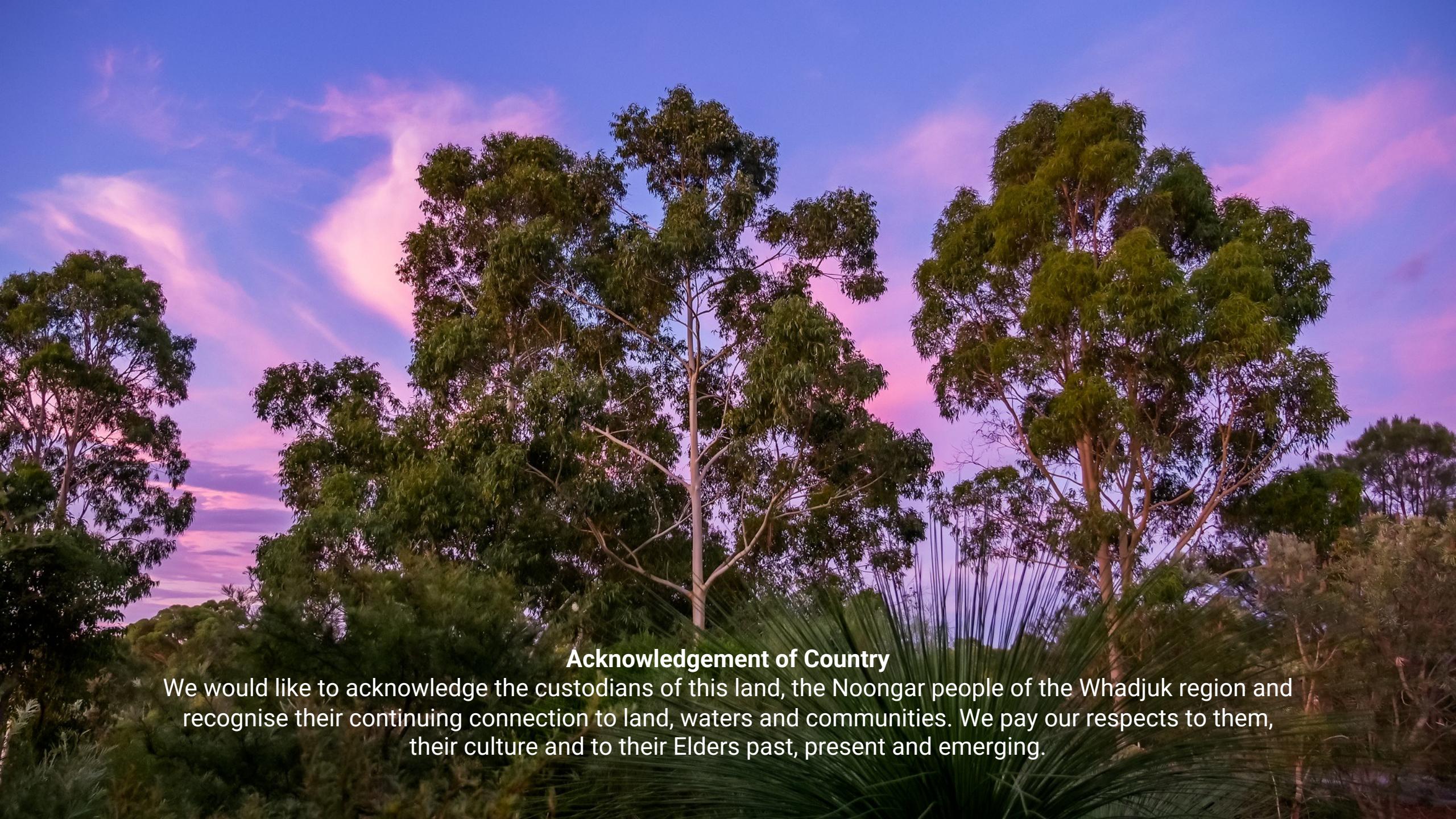


# Essential Eight in 2021

## 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

# Agenda

---

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



# Australian Threat Landscape

---

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

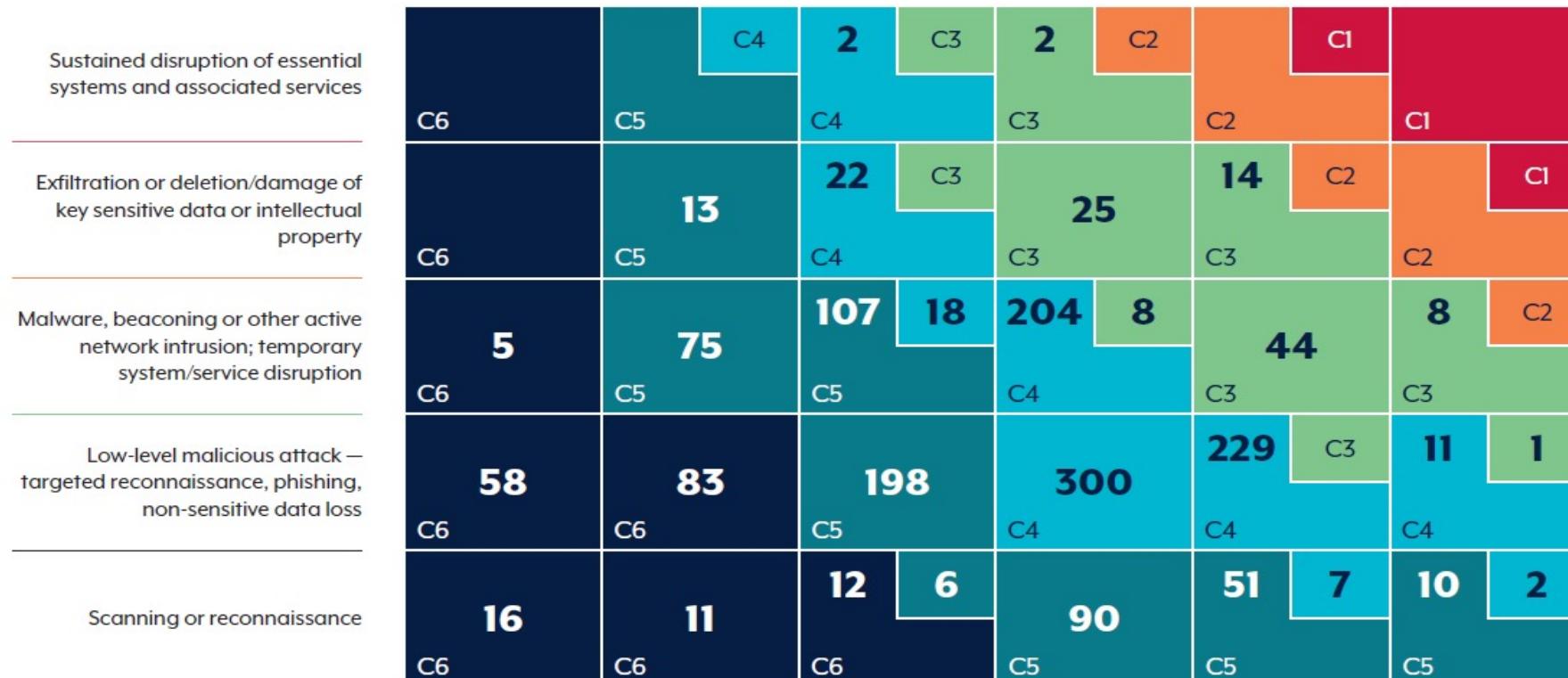


**GREAT SCOTT!!**

ACSC Cyber  
Threat  
Report FY21

# ACSC Cyber Threat - Categorised

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



Member(s) of the public	Small Organisation(s) Sole Traders	Medium-sized Organisation(s) Schools	State Government Academia/R&D Large Organisation(s) Supply Chain	Federal Government / National Infrastructure Supply Chain to Critical National Infrastructure	National security Aus essential service(s) Critical National Infrastructure Significant number impacted
-------------------------	---------------------------------------	---	--	--	---

# 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

# 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?

# ACSC Cyber Threat – Business Email Compromise

---

More than  
**4,600 BECs  
reported**

Over  
**\$81 million  
(AUD)**  
lost due to BEC

Increase in  
average financial  
losses per BEC  
report

---

▲ **54%**

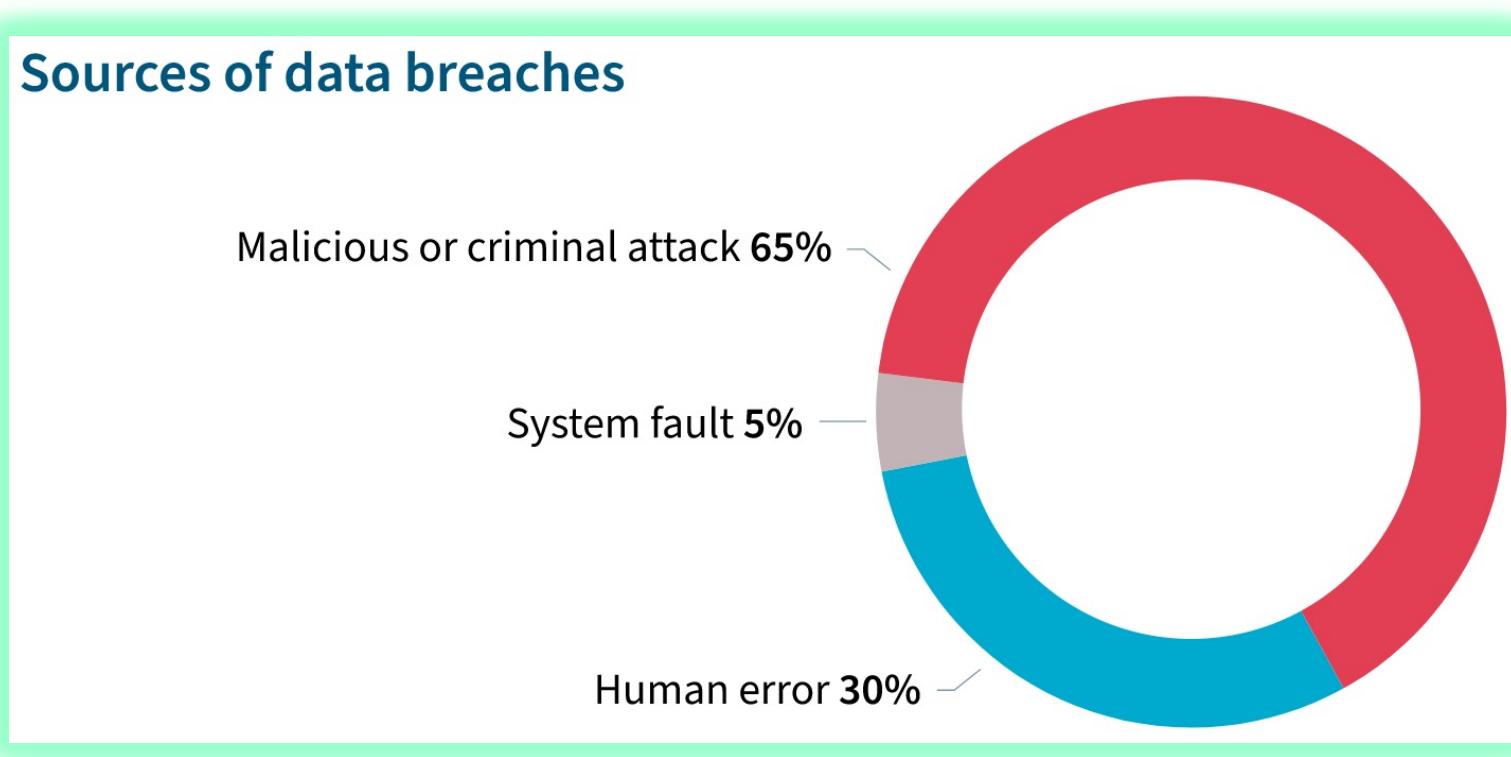
# ACSC Cyber Threat – Business Email Compromise

---

## ACSC BEC Case Study

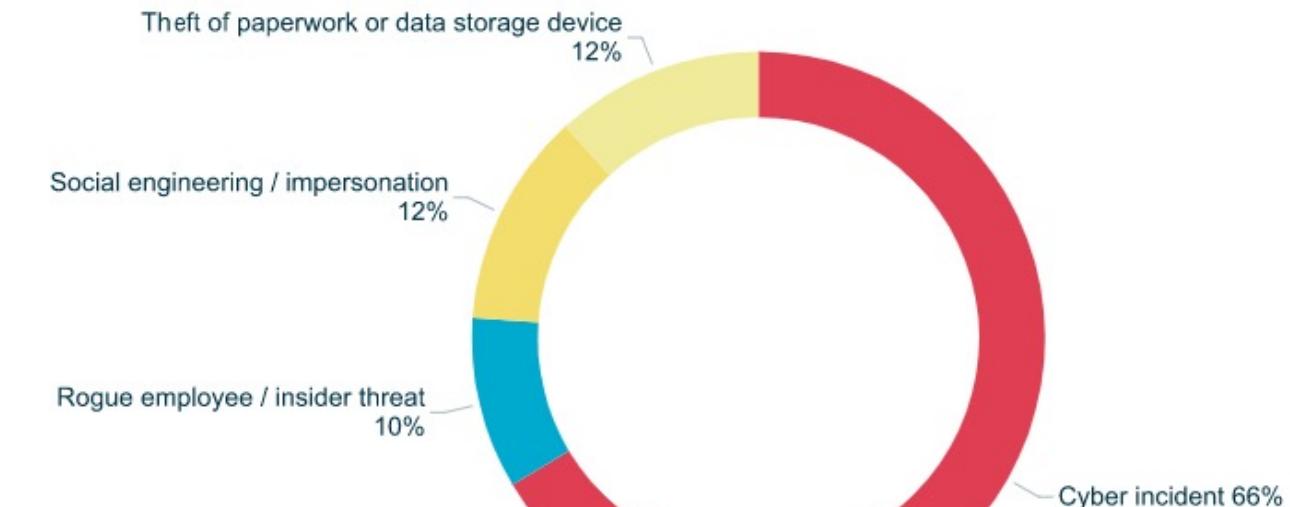
- In Sep 2020, AU Hedge Fund transferred AU\$8.7M
- Money most recovered, but main client withdraw due to reputational damage
- AU Hedge Fund into receivership and bankruptcy

# OAIC Notifiable Data Breaches Jan–Jun 2021



# OAIC Notifiable Data Breaches Jan–Jun 2021

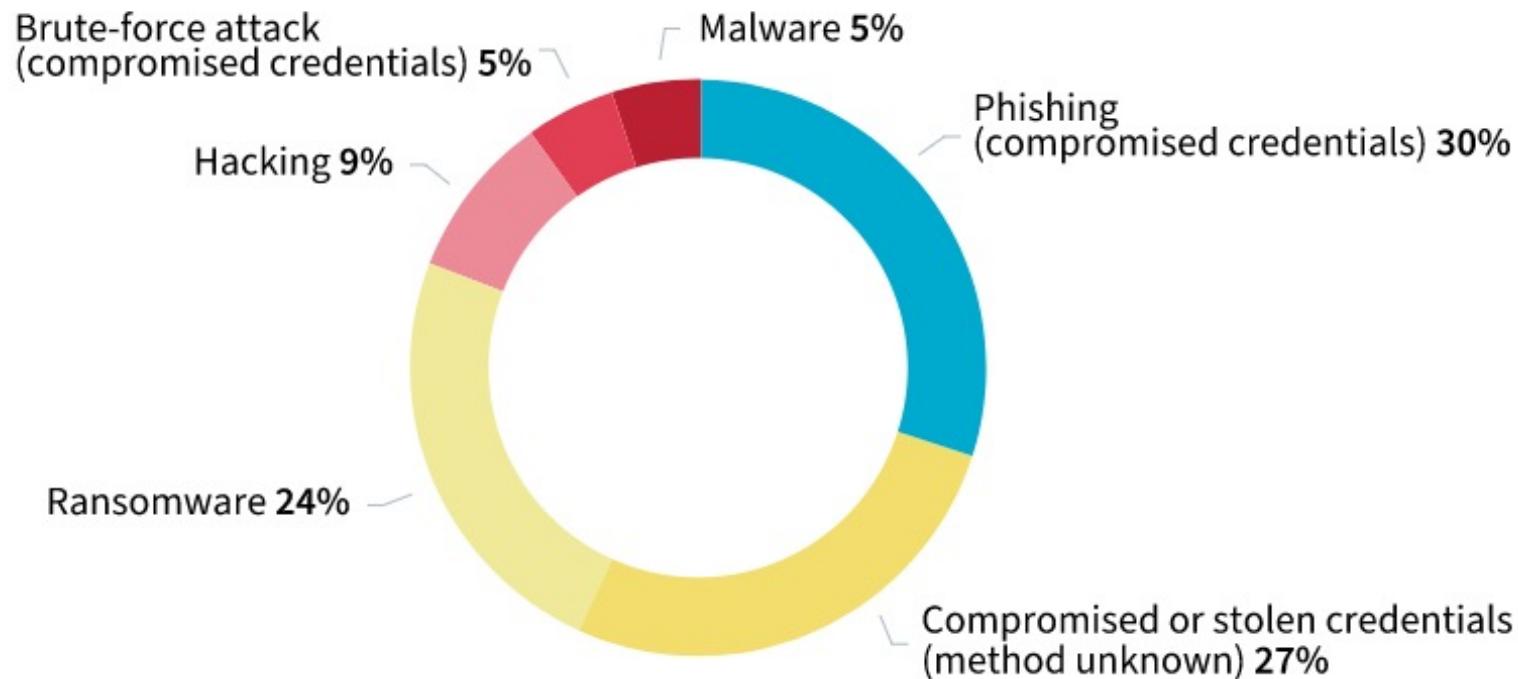
**Chart 10 – Breaches resulting from malicious or criminal attacks – All sectors**



# OAIC Notifiable Data Breaches Jan–Jun 2021

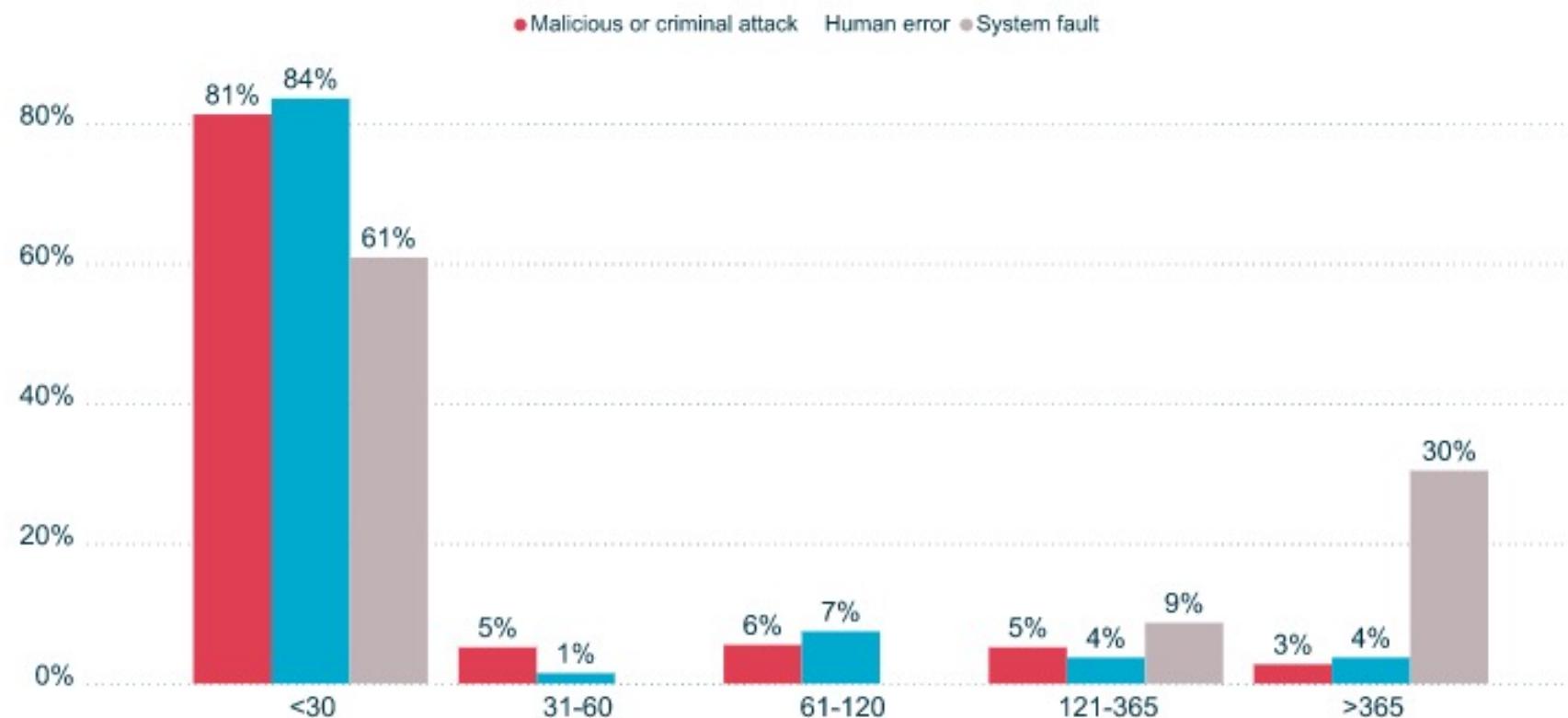
**43% of all data breaches (192 notifications) resulted from cyber security incidents**

Cyber incident breakdown



# OAIC Notifiable Data Breaches Jan–Jun 2021

**Chart 6 – Days taken to identify breaches by source of breach – All sectors**



# Microsoft Digital Defense Report FY21

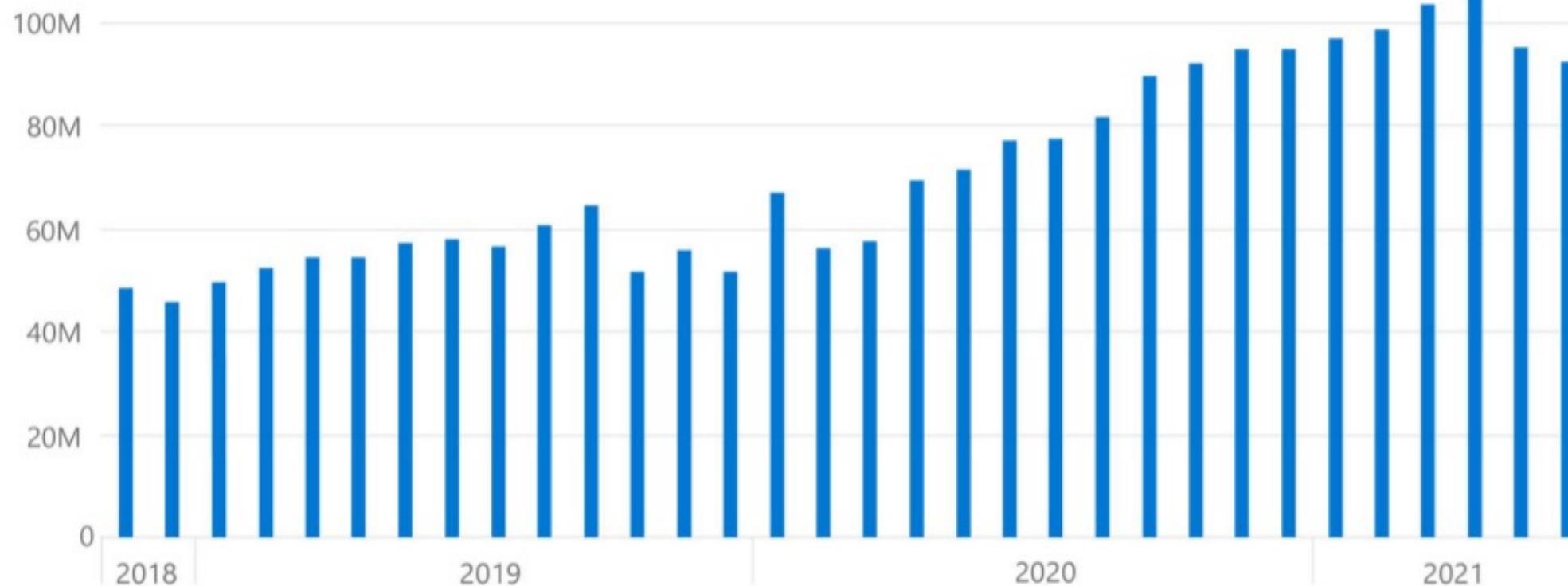
---



# Microsoft Digital Defense Report FY21

## DEFENDER SIGNALS

Ransomware encounter rate (machine count): Enterprise customers



# Microsoft Digital Defense Report FY21

Emails determined as phish



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



# 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

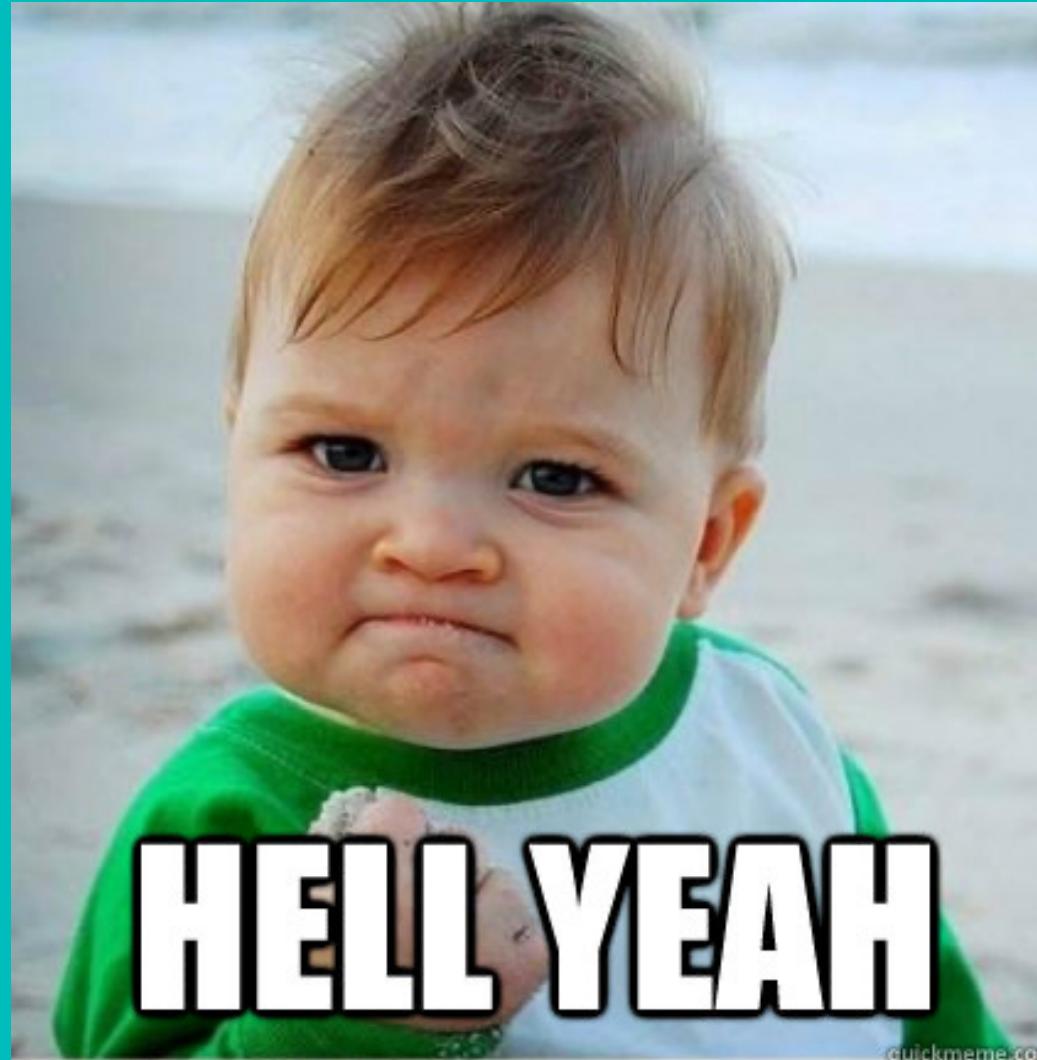
# Is Essential Eight Relevant?

---

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”

# Is Essential Eight Relevant?



= zetta

# Microsoft Report Learnings

The cybersecurity bell curve:

Basic security hygiene still protects  
against 98% of attacks



Seems Familiar...

# 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

# Maturity Levels – 2021 Redefined

## 2020 Maturity Model

How aligned to “intent of mitigation strategy”?



### 2020 Level 1 (Good Start)

- Partly aligned with intent of mitigation strategy



### 2020 Level 2 (Nearly There)

- Mostly aligned with intent of mitigation strategy



### 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)



### 2021 Level 1 (Script kiddie)

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



### 2021 Level 2 (Semi-Pro)

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



### 2021 Level 3 (Baba Yaga)

Large Enterprise

Critical Infrastructure  
(+ High Threat)

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

# 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**



# 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

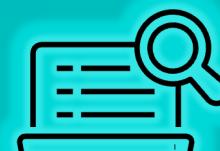
# 1. Application Control Maturity Levels

2020 Maturity Level ①, ②, ③

2021 Maturity Level ①, ②, ③



Workstations  
(profile & temp)



Workstations  
(other folders)



Internet-Facing  
Servers



Servers

	Workstations (profile & temp)	Workstations (other folders)	Internet-Facing Servers	Servers
Restrict executables	① ①	① ②	① ②	① ③
Restrict software libraries, scripts and installers	② ①	② ②	② ②	② ③
Restrict compiled HTML, HTML apps and control panel applets <small>(③revalidate rulesets annually)</small>	①	②	②	③
Restrict drivers	③	③	③	③
Implement Microsoft 'recommended block rules' to prevent application control bypass <small>(③driver block rule)</small>	③ ③	③ ③	③ ③	③ ③
Log allow/block <small>(③centrally logged, protected, monitor for compromise, and action cyber events)</small>	②	②	②	③

# 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.

# 1. Application Control WDAC or AppLocker

---

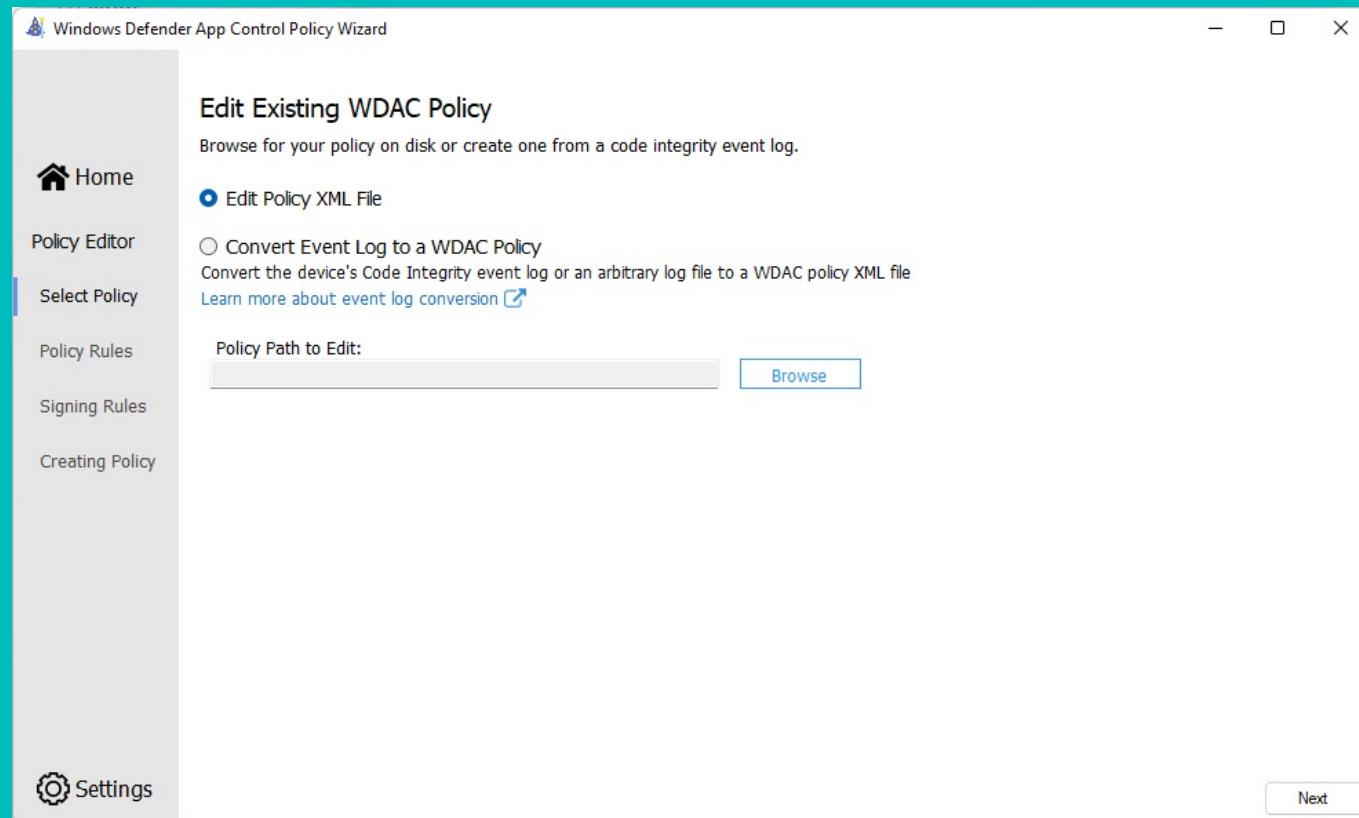
## Windows Defender Application Control (WDAC)

- **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**

# 1. WDAC Wizard

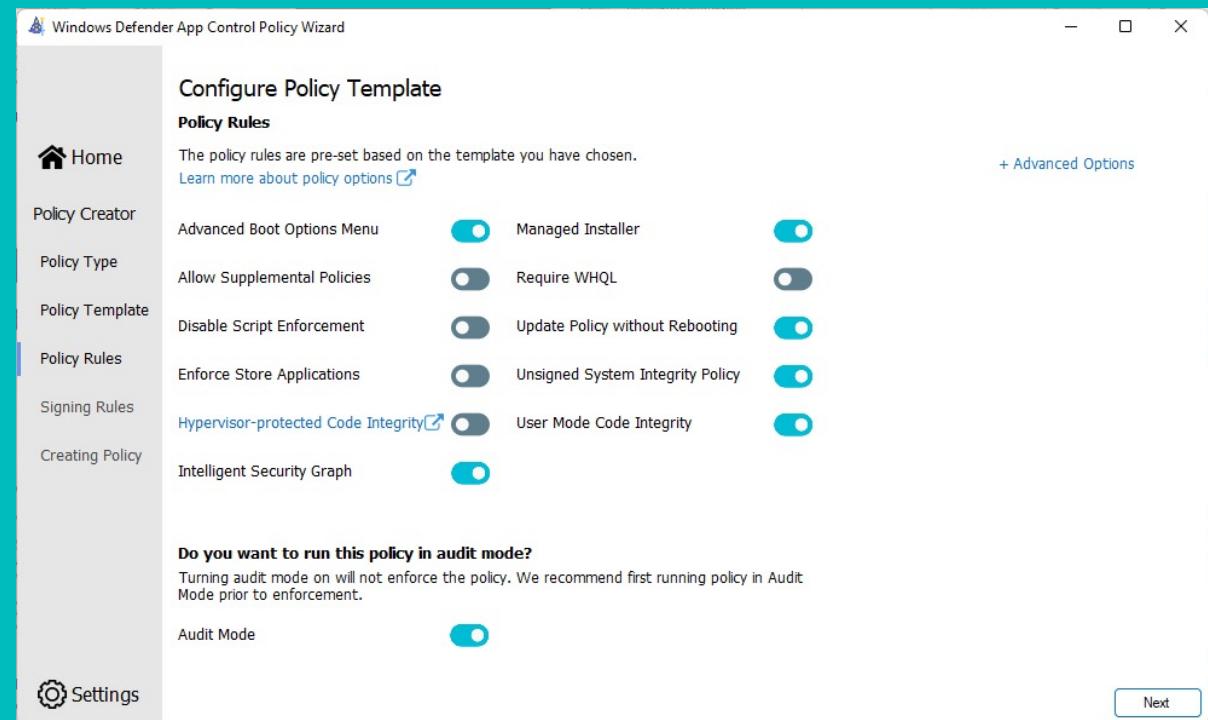
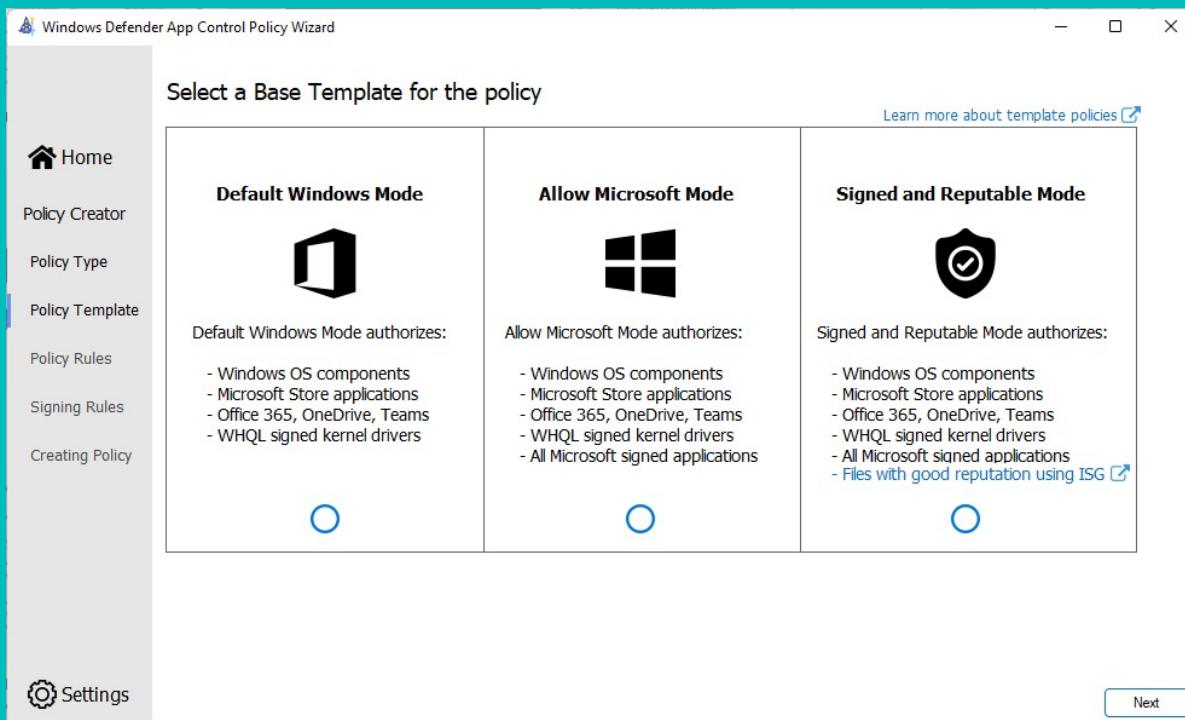
---

The WDAC Wizard can be used to Define or Edit policies



# 1. WDAC Wizard Templates

## Configurable options for new Base Templates



# 2. Patch Applications Maturity Levels

**2020 Maturity Level ①, ②, ③**

**2021 Maturity Level ①, ②, ③**



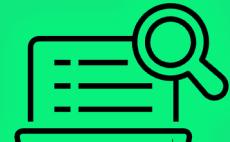
'Extreme Risk'  
Vulnerabilities



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)

- ① 1 month
- ② 2 weeks
- ③ 48 hrs

- ① 2 weeks  
(or 48 hrs)
- ②
- ③

- ① 1 month
- ② 2 weeks
- ③ 2 weeks  
(or 48 hrs)
- ④ 1 month

Vulnerability scanner used to identify missing patches or updates for security vulnerabilities

③

- ① daily
- ② daily
- ③ daily

- ① fortnightly
- ② weekly
- ③ weekly
- ④ ?

Remove apps no longer supported by vendors

①  
②  
③

①  
②  
③

①  
②  
③

①  
②  
③  
④

# 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)

# 2. Patch Applications Vulnerability Assessment

**Microsoft Azure** Search remediation history and details

**Remediate vulnerabilities found on your virtual machines (powered by Qualys)**

Description: Microsoft Windows Security Update for Windows Server... (ADV190002) (PatchLevel)

Impact: Successful exploitation could allow an attacker to obtain sensitive data, such as unencrypted user credentials from the targeted systems.

**Remediate vulnerabilities found on your virtual machines (powered by Qualys)**

**Threat:**

- Exploitability
- Exploitability
- Access breach
- Elevation of privilege

**Remediation steps:**

Visual remediation: Review and remediate vulnerabilities discovered by Azure Security Center's built-in vulnerability assessment solution (powered by Qualys).

**Affected resources:**

Security Checks

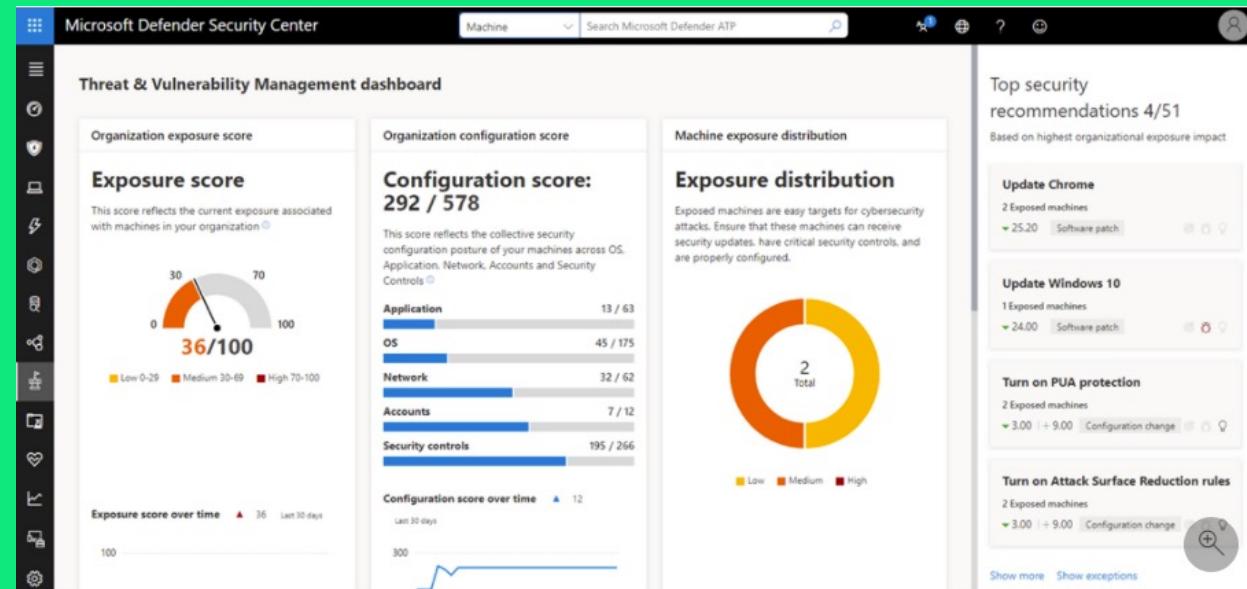
**Threat**

**Remediation**

**Additional References**

**Affected resources**

Name	Description
VM1	AS1 DEMO
VM2	AS2 DEMO

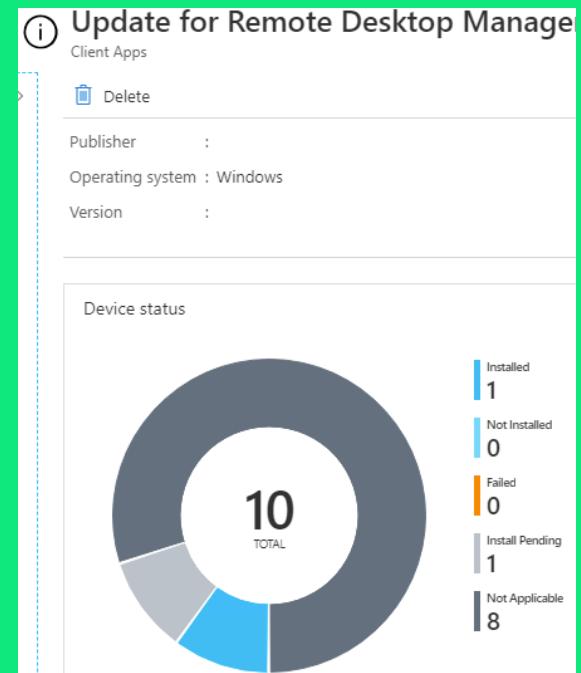
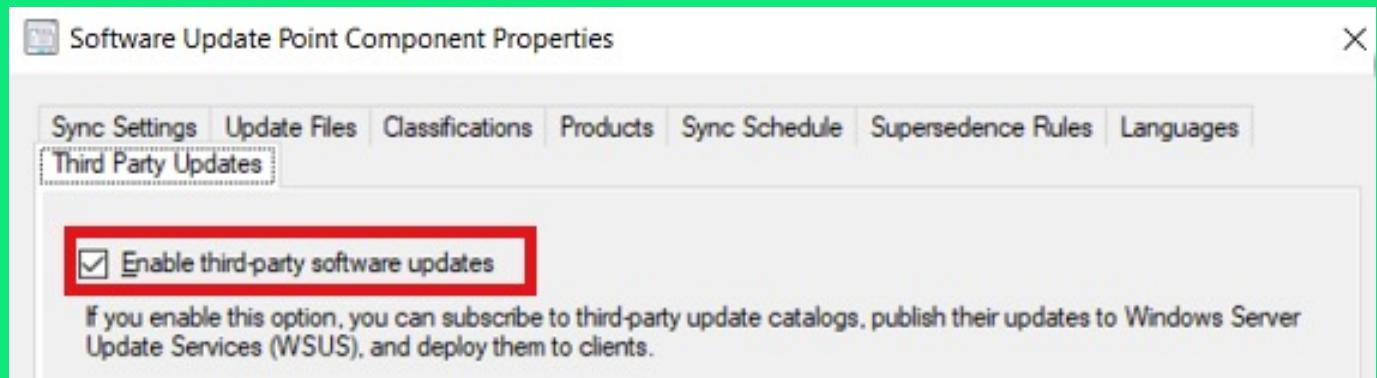


# 2. Patch Applications Third Party Updates

---

Managing 3<sup>rd</sup> 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





# 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 ①, ②, ③

2021 Maturity Level ①, ②, ③



Privileged Access

① At request  
② At request  
③ + annually

① At request  
② At request  
③ + annually

② Validate >12 mths.  
③ OR 45 days inactive

(Interactive) Privileged Account: No internet, email, web services

① ② ③ ④ ⑤ ⑥

Separate privileged/unprivileged operating environments

② ③

Privileged OE not VM in unprivileged

③

Use jump servers; local admin & service account passwords 'tricky'

② ③

JIT Admin

③

Log use/change (③ central log, protected, monitor for compromise, action cyber events)

② ③

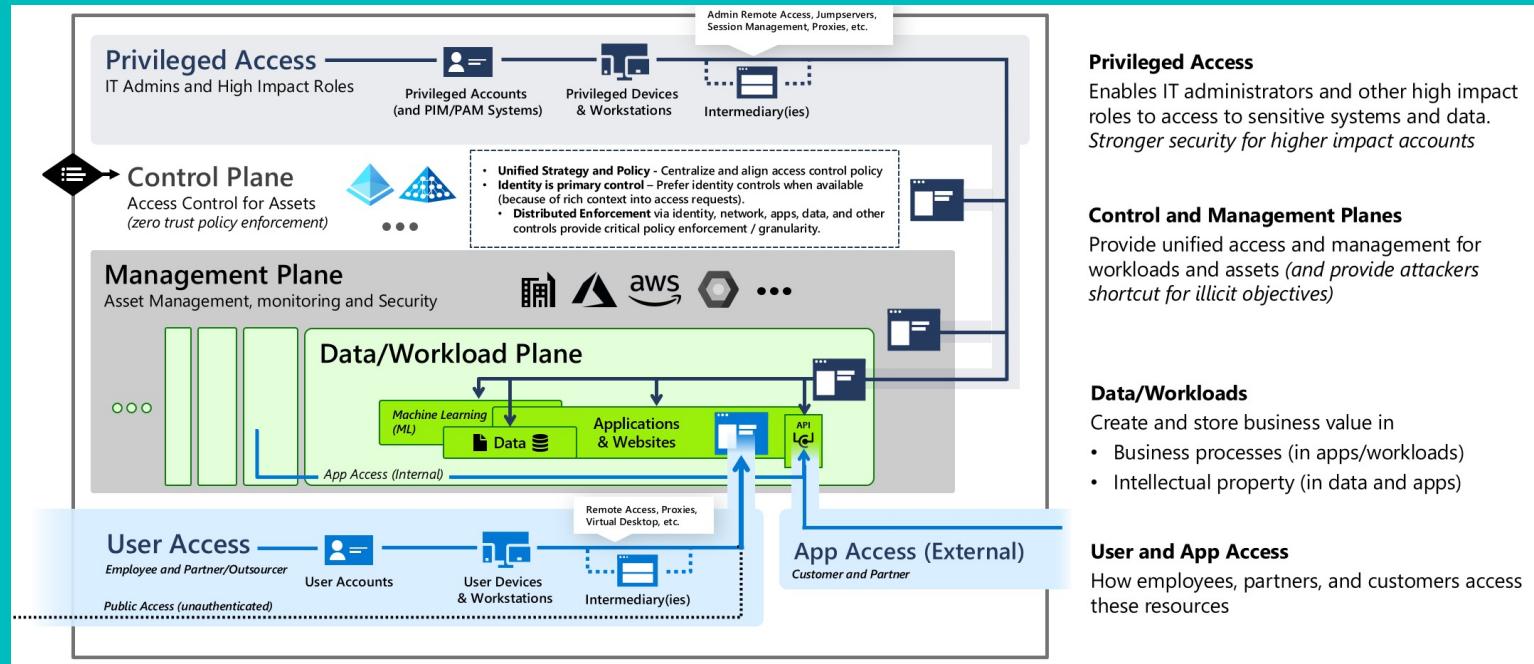
Windows Defender Credential Guard and Windows Defender Remote Credential Guard

③

# 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



# 5. Restrict Admin Privileges

## PIM

### Azure AD Privileged Identity Management (PIM)

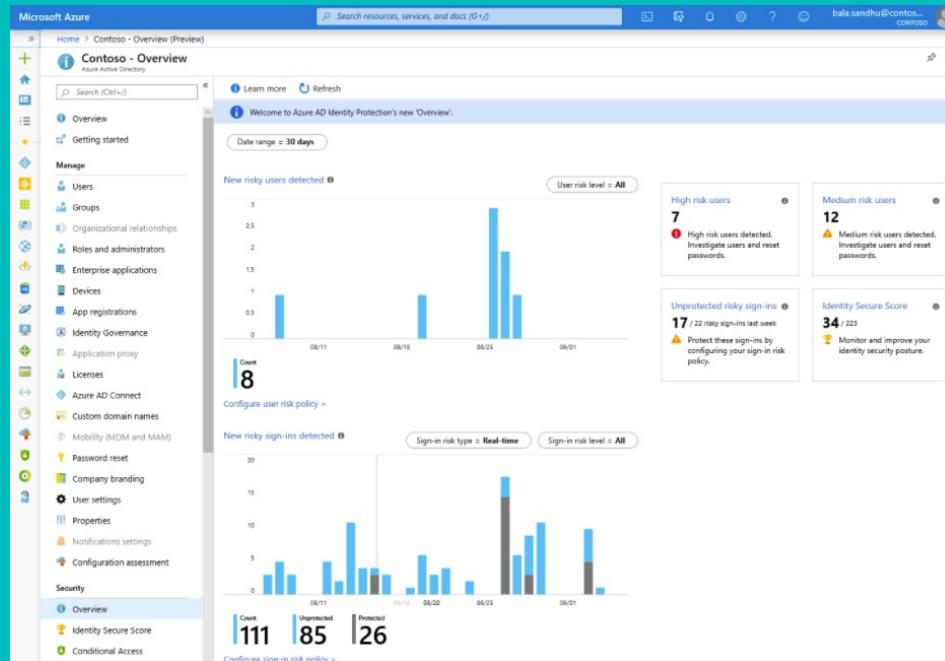
- Time-bound, just-in-time access
- Configure to require justifications, approval, and MFA enforcement
- Enables notifications, access reviews and audit history

The screenshot shows the Microsoft Azure PIM interface for the 'FIMDEV' tenant. The main title is 'FIMDEV | Approve requests'. Below it, there's a sub-header 'Privileged Identity Management | Azure AD roles'. On the left, a sidebar has tabs for 'Quick start', 'Overview', 'Tasks' (selected), 'My roles', 'Pending requests' (highlighted with a red box), and 'Approve requests' (also highlighted with a red box). Under 'Tasks', there's a table for 'Requests to renew or extend role assignments'. The table includes columns for Role (Application Administrator), Requestor (Dylan Price), Resource (FIMDEV), Resource type (Directory), Request type (Member extend), Assignment type (Eligible), Start time (8/16/2021, 12:23:38 PM), End time (8/17/2021, 12:23:04 PM), and Action (button labeled 'Approve | Deny'). At the bottom of the table, there are buttons for 'Approve' and 'Deny'. Below the table, there's another section for 'Requests for role activations' with a note 'No requests pending approval'. The top of the page has a standard Microsoft Azure header with a search bar and various navigation icons.

# 5. Restrict Admin Privileges Identity Protection

## Azure AD Identity Protection

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



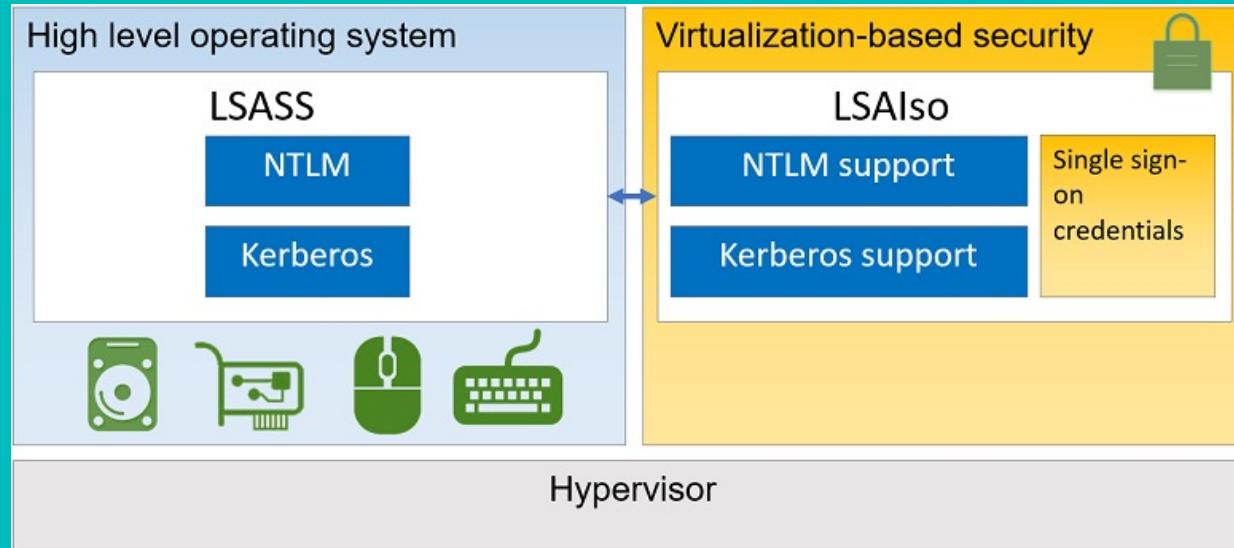
The screenshot shows the configuration interface for a new sign-in risk policy. The policy is titled 'Device compliance app policy' and is set to 'Not configured' for all conditions.  
**Conditions:** The policy applies to 'Sign-in risk' (Not configured) across all device platforms, locations, client apps, and device states.  
**Sign-in risk:** The policy is configured to 'Yes' (selected). A note says: 'Select the sign-in risk level this policy will apply to'. Options include: High, Medium, Low, and No risk.

# 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





# E8 Maturity Model Updates - Recover

---

Recover Data and System Availability:

8. Regular Backups



# 8. Regular Backups Maturity Levels

2020 Maturity Level ①, ②, ③

2021 Maturity Level ①, ②, ③



Perform  
Backup



Retain  
Backup



Test Restore  
(Full/Partial)

Backup important info, software and config

① monthly ① Per BC  
② weekly ② Per BC  
③ daily ③ Per BC

① monthly ① Per BC ① NA/partial  
② weekly ② Per BC ② 1 / bi-annual  
③ daily ③ Per BC ③ Big changes /quarterly ① Per DR  
② Per DR  
③ Per DR

Unprivileged  
Users

Backup  
Admins

Other Privileged  
Users

Block backup delete/modify (③ or backup offline)

①  
②  
③  
④

②  
③

②  
③  
④

Access backups

① Only own  
② Only own  
③ None

② Only own  
③ None

# 8. Regular Backups - Integrity

## Protect Backup Integrity

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

The screenshot shows the 'wormtestcontainer1 - Access policy' blade in the Azure portal. Under the 'SETTINGS' section, 'Access policy' is selected. In the 'Immutable blob storage' section, the 'Policy type' dropdown is set to 'Time-based retention'. The 'Time-based retention' option is highlighted with a red box. Below it, 'Legal hold' is listed. The 'RETENTION INTERVAL' field shows 'days' and has a dropdown menu open with '1000 days' selected. At the bottom are 'OK' and 'Cancel' buttons.

The screenshot shows the 'softdelrsv | Properties' blade in the Azure portal. On the left, 'Properties' is selected. On the right, the 'Security Settings' section is expanded. The 'Soft Delete (For eligible Backup Management Types)' switch is highlighted with a red box and is set to 'Enabled'. Other settings like 'Security PIN Generate' and 'Recovery Services Agent Download' are also visible.

# 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



# 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!)



# Q&A Discussion

---



[www.zetta.com.au](http://www.zetta.com.au)



[linkedin.com/company/zetta-group](https://linkedin.com/company/zetta-group)