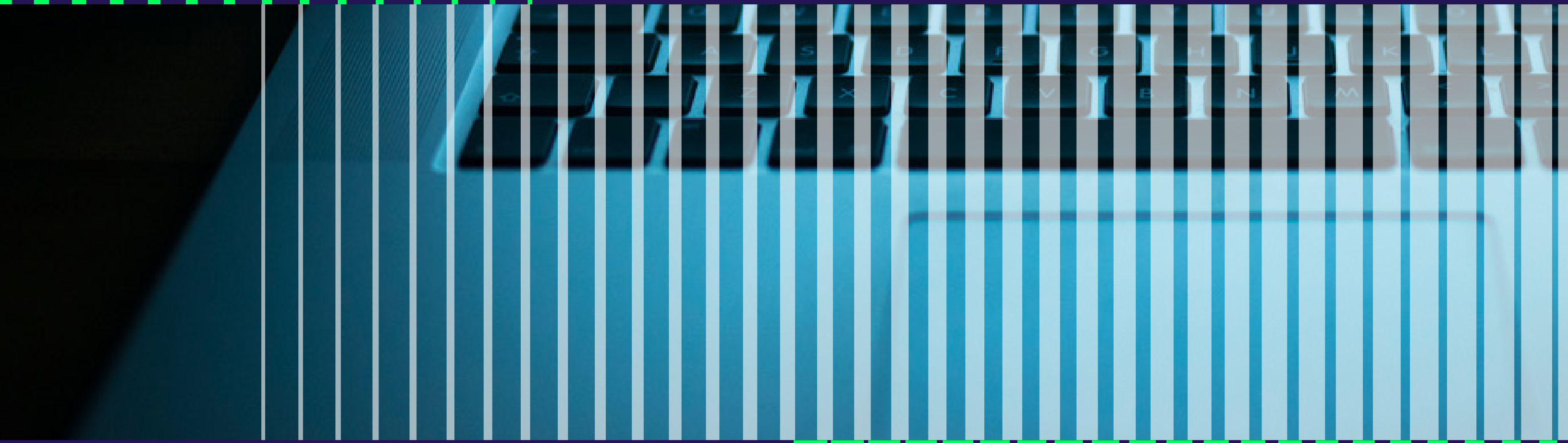
Delinea

Implementing Privileged Access Management solutions to meet Essential Eight requirements



WHITEPAPER

Implementing Privileged Access Management solutions to meet Essential Eight requirements

The Australian Cyber Security Centre (ACSC) introduced Essential Eight in 2017 as cybersecurity guidance to provide a set of mitigation strategies and defensive measures against threats affecting Australian organisations. Learn the requirements of Essential Eight and how Delinea's Privileged Access Management (PAM) solutions help you meet them.

What is Essential Eight?

Essential Eight measures are designed to prevent and contain cyberthreats like malware, phishing, ransomware, and data breaches. Implementing Essential Eight security measures is much less expensive than dealing with the consequences of a cyberattack, according to ACSC.

Although ACSC doesn't require an independent party certification, you might be asked to provide evidence of Essential Eight compliance by a government directive or policy, regulatory authority, or as part of contractual arrangements with vendors, partners, or customers.

Eight Security Strategies and PAM solutions

The Essential Eight framework consists of the following mitigation strategies:

1. Implementing application control
2. Patching applications
3. Configuring Microsoft Office macro settings
4. Hardening user applications
5. Restricting administrative privileges
6. Patching operating systems
7. Implementing Multi-Factor Authentication
8. Ensuring regular backups

In developing the Essential Eight, one of the goals of ACSC was to correct an imbalance in how organisations implement cybersecurity strategies. Their model for Essential Eight implementation is organised according to the four stages of a maturity model so that organizations know where to start and how to progress systematically. They suggest implementing Level One requirements for all Eight controls before progressing to the higher levels rather than leaving any of the controls unaddressed.

ACSC suggests Level One fits smaller organisations, Level Two fits medium-sized organisations, and Level Three fits organisations that manage critical infrastructure or experience a high volume of malicious activity.

Organisations that are on Level Zero and haven't yet achieved Level One aren't sufficiently prepared to deal with an attack. They're vulnerable to significant risk when breached, which can result in great financial loss and severely affect their reputation.

PAM solutions are organised in a similar maturity model to the Essential Eight and cover areas like governance, risk and compliance, privilege administration, and Identity Access Management.

Privileged Access Management is a set of security solutions that help companies protect their digital assets by ensuring only authorised individuals can access them. PAM products reduce the risk of insider and external threats by minimising the number of identities, whether human or machine, who have access to sensitive data and systems by facilitating their access privileges.

Access audits enabled by the PAM platform are necessary for confirming that the organisation stays compliant with Essential Eight requirements.

When implementing the Essential Eight, you should evaluate your level of maturity, industry sector, and risk tolerance to create a roadmap that's right for you.

How Privileged Access Management solutions can help you on the path to success with the Essential Eight

Based on your size, risk, and level of maturity, you can identify gaps in your current strategies and prioritize your next steps. Learn how Delinea PAM aligns with each strategy suggested in the Essential Eight, according to each maturity level.

1 | Application control

Essential Eight requirements

At Level One, basic protection rules should be implemented so that users can access devices and systems in a controlled and protected manner. The execution of applications, software libraries, scripts, installers, compiled HTML, HTML applications, and control panel applets should be prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers, and email clients.

At Level Two, application controls should be implemented on workstations and internet-facing servers. Allowed and blocked executions (workstations and internet-facing servers) should be logged.

At Level Three, event logs should be stored and protected from unauthorised modification and deletion and monitored for signs of compromise. Application control should be added to non-internet-facing servers. Allowed and blocked execution on non-internet-facing servers must be logged.

Delinea capabilities

Rules and policies that govern execution of applications or commands according to the best practice of least privilege can be established in Delinea Privilege Manager for workstations and Delinea Server PAM for servers. Administrators can request temporary roles just-in-time to complete privileged tasks. Privilege Manager and Delinea Server PAM have reporting, auditing, and host-level session recording capabilities to track and record users' activity. Privilege Manager enables you to establish allow and deny lists to control execution of known applications on workstations. Unknown applications can be sandboxed for further investigation.

Server PAM supports fine-grained elevation to protect access to privileged applications and commands on Windows and Linux servers. Server PAM can also control application execution by placing users in a restricted Windows Desktop or Linux shell environment.

2 | Patch applications

At Level One, organisations must monitor employees' tools daily to detect vulnerabilities so that patches can be implemented. Software no longer supported with patches supplied by vendors should be removed from the organisation.

At Levels Two and beyond, the requirement specifies the frequency of vulnerability scans: weekly for Office productivity suites, web browsers and their extensions, email clients, PDF software, and security products, and fortnightly for other applications.

Delinea capabilities

To get a comprehensive scan on every endpoint, including servers and workstations, vulnerability scanners must log into the endpoint with a suitable credential that provides the necessary access.

Instead of hard-coding credentials within the scanner, they can be fetched from Delinea Secret Server via custom integration or API calls. Benefits of this approach include reduced risk of credential exposure and reduced administrative overhead. Also, since the scanner is assured that the credential is always current, there's less risk of a scanner-initiated login failure that could leave a server in an unresolved state of compromise.

Delinea enables authenticated scans to run systematically, always having the correct credentials while keeping those credentials secure.

3 | Configuring Microsoft Office macro settings

At Level One, organisations should disable Microsoft Office macros for users that don't have a business requirement. Macros' security settings cannot be changed by users. Additionally, Microsoft Office macros in files originating from the internet must be blocked and Microsoft Office macro antivirus scanning must be enabled.

At Level Two, organisations should have capabilities to log blocked and enabled macros. Microsoft Office macros should be blocked from making Win32 API calls.

At Level Three, it is further specified that Microsoft Office macros are allowed to execute if running from within a sandboxed environment, a trusted location, or that are digitally signed by a trusted publisher. Those that were digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. A list of trusted publishers should be validated at least on annual basis. Only privileged users responsible for macro validation can write and modify content within Trusted Locations.

Logging requirements are further expanded. Allowed and blocked Microsoft Office macro executions should be centrally logged and protected from unauthorised modification and deletion. Organisations should frequently monitor them and action when cybersecurity events occur.

Delinea capabilities

Not covered by Delinea Privileged Access Management solutions.

4 | User application hardening

At Level One, organisations should restrict web browsers from processing Java and web advertisements on the internet. Security settings of web browsers cannot be changed by the users.

At Level Two, Microsoft Office and PDF software must be blocked from running child processes. Additionally, blocked PowerShell script executions must be logged.

Level Three emphasises logging PowerShell events and requires that logs be centrally stored and protected from unauthorised modification and deletions well as monitored for signs of compromise. When cybersecurity events are detected in the logs, action must be taken.

Delinea capabilities

Privilege Manager and Server PAM allow you to restrict or prohibit the execution of scripts and child processes.

Through session monitoring and recording, Delinea automatically logs all privileged behaviour, including activities of privileged users such as updating scripts or running restricted executables. Logs are stored securely and can be easily analysed for reporting and forensics. Further, Delinea Privileged Behavior Analytics can detect and alert anomalous behaviour not accounted for in static policies and rules.

5 | Restrict admin privileges

At Level One, the control requires organisations to identify privileged users and establish policies defining their access to IT systems.

At Levels Two and Three, the control recommends just-in-time access controls rather than standing access left open to be exploited. There is also a greater focus on preventing unauthorised modification and deletion of privileged accounts through monitoring and logging.

Delinea capabilities

Secret Server helps you manage access for privileged users of all types, including domain administrators, developers, business users, service accounts, and machine identities. Policy-based controls establish who can access which systems and under what conditions. Once logged in, Server PAM control the actions the user can take on servers. Avoiding the risks associated with broad, standing access, Delinea's solutions enforce the Principle of Least Privilege to ensure that every privileged user has only the access they need, at the time they need it, for a limited time.

Automated, continuous discovery ensures you have visibility over all endpoints, users, and privileges, plus centralised management of policies. All privileged user behaviour can be recorded and logged, including remote users and third parties, whether in the cloud or on-premise.

6 | Patch Operating Systems

Organisations must ensure that patches, updates, or vendor mitigations for security vulnerabilities are updated regularly or within a specific time frame. Frequency of updates and patches application increases with each maturity level.

Vulnerability scanning must be conducted daily for operating systems with internet-facing services and weekly for workstations, servers, and network devices operating systems.

Delinea capabilities

To get a comprehensive scan on every endpoint, including servers and workstations, vulnerability scanners must run an authenticated scan, sometimes called a credentialed scan.

Delinea enables authenticated scans to run systematically, always having the correct credentials while keeping those credentials secure.

Delinea can act as an external provider of credentials to the third-party tools that are required to log in and access operating systems and applications.

7 | Multi-Factor Authentication

Level One requires organisations to use Multi-Factor Authentication (MFA) when users authenticate to their organisation's internet-facing services or authenticate to third-party internet-facing services that process, store, or communicate their organisation's data.

Levels Two and Three place greater emphasis on event logging. MFA events should be protected from unauthorised modification and deletion. Logs should be monitored for signs of compromise.

Delinea capabilities

Delinea believes in a layered security approach, providing organisations with the means to enforce MFA at all significant access gates. Delinea's PAM solutions enable you to request additional proof of identity at endpoint login, during application or command execution and elevation, and when attempting to access vaulted secrets.

8 | Regular backups

Level One requires organisations to perform and retain backups and test them as part of a disaster recovery plan. It also specifies that unprivileged users can access backups but can't modify or delete them.

At Level Two, most privileged users (apart from designated backup admins in "break-glass" scenarios) are restricted from accessing, modifying, and deleting backups.

Delinea capabilities

Secret Server protects access to privileged accounts, ensuring that only approved users can access them in emergency break-glass scenarios. Protection is military-grade, and the vault can be replicated for disaster recovery.

Server PAM controls access to backup servers at the operating system level and ensures that only approved users can run backup management tools. Access request workflows enable users to request additional rights to perform these tasks.

Conclusion

Privileged Access Management is essential to meet Australia's Essential Eight requirements and demonstrate compliance. Delinea's suite of PAM solutions helps you get started with Level One and can accelerate your maturity to achieve Levels Two and Three.

Connect with Delinea for a free, 30-day trial and learn more about how we can help you align to the Essential Eight.

Delinea

Defining the boundaries of access

Delinea is a leading provider of privileged access management (PAM) solutions that make security seamless for the modern, hybrid enterprise. Our solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

Learn more about Delinea's solutions at **delinea.com.**