Take Control of The ASD Essential Eight Cyber Security Guidelines with Continuous Security

Validate your maturity level and stay in front of regulatory compliance with Qualys

Qualys.

Executive Summary

Qualys enables you to analyse threats and misconfigurations in real time, which helps you validate your compliance with the Australian Cyber Security Centre (ACSC) Essential Eight at the pace required to mitigate threats.

Summary of the ASD Essential Eight guideline	How Qualys helps meet and validate the recommendations
Application control covers restrictions on code and applications being executed on workstations and servers outside an approved set.	Qualys can define approved or disallowed software and can automatically apply or uninstall packages, including any required end-point agents.
Patch applications recommends vendor patches and updates for internet-facing services, including office productivity suites, web browsers to be applied promptly.	Qualys can identify missing patches on a machine and can deploy patches either automatically or manually.
The Essential Eight recommends Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Qualys Policy Compliance has a number of controls that can access and validate whether macros are appropriately configured and running from appropriate locations.
Application hardening focuses on reducing the likelihood of end-user applications running malicious code.	Qualys helps assess the user application policy and can flag and remediate controls which compromise policy.
Restrict administrative privileges recommendations for privileged access management to systems and applications, which should be validated, limited to specific duties and automatically disabled.	Qualys can report on administration privileges, and can validate if proposed changes are needed.
Patch operating systems focuses on applying patches, updates, or vendor mitigations in operating systems of workstations and internet-facing services in a timely manner.	Qualys has market-leading vulnerability scanning which can discover vulnerabilities and then patch operating systems.
It is recommended multi-factor authentication (MFA) is used by staff for internet-facing services for both sensitive and non-sensitive organisational data; and generally, cannot be impersonated.	Qualys can validate MFA, which is a setting on both Mac and Windows, and also discover if MFA is enforced on a range of popular internet-facing services and third-party SaaS and PaaS platforms.
Backups of important data, software and configuration settings should be performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.	Qualys can validate whether backups have been taken and if the appropriate backup software or agent is running on the target machines.

Solutions exist to help meet the Essential Eight guidelines, but few, if any, validate compliance in an automated way.

Introduction

Australian enterprise and government organisations have numerous reporting and regulatory compliance requirements.

In additional to financial and workplace compliance, the Australia Government has recommendations for improving information security management practices through the Australian Cyber Security Centre (ACSC), the lead agency for cyber security.

The ACSC is part of the Australian Signals Directorate and is tasked with organising national cyber security operations and resources, including developing mitigation strategies to help organisations protect themselves against various cyber threats.

One of these mitigation strategies is the Essential Eight, which comprises of eight general recommendations designed to protect Microsoft Windows-based systems.

This report, *Take Control of The ASD Essential Eight Cyber Security Guidelines with Continuous Security,* is an IT and business leader's guide to ensuring their organisation is continuously meeting the best practice recommendations.

Organisations have access to numerous solutions to meet the Essential Eight guidelines, but what is less prevalent is the capability to validate whether operational systems are compliant in an automated way.

Being proactive with the Essential Eight can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

ACSC Australian Cyber Security Centre

The ACSC's Strategies to Mitigate Cyber Security Incidents publications now recommend the use of more continuous security tactics.

The Need for Continuous Cyber Security

As threats become more sophisticated and automated, Australian organisations will increasingly face continuous attacks which cannot be mitigated without better, more real time responses.

Tradition security techniques are always playing catch up with new threats, or undiagnosed exploits. This game of "cat and mouse" is not sufficient to protect enterprise and government organisations from the growing pace of attacks.

In fact, the ACSC's Strategies to Mitigate Cyber Security Incidents publications recommend the use of more continuous security tactics, including: Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions to log, protect, monitor and action cyber security events.

An organisation cannot secure what it cannot see or does not know about, and real time security solutions are invaluable for helping identify potential weak links at scale.

"Malicious attacks are growing in sophistication and volume year over year and security teams need a combination of proactive protection against known malware and the ability to identify and respond to new unknown threats quickly."

Michael Suby
Vice President of Research, IDC

Real time security from Qualys

Qualys is a market leader in continuous security. The Qualys Cloud Platform delivers an always-on assessment of your global IT, security, and compliance posture, with two second visibility across all your IT assets, wherever they reside. And with automated, built-in threat prioritization, patching and other response capabilities, it is a complete, end-to-end security solution.

Qualys enables you to analyse threats and misconfigurations in real time, with six sigma accuracy. Continuously and automatically detect vulnerabilities and critical misconfigurations across your global hybrid environment. And get real-time alerts on zero-day vulnerabilities, compromised assets and network irregularities.

Qualys platform now available in Australia

Australia's government agencies, and organisations with data sovereignty controls, now have the option to use a local Qualys cloud. The on-shore platform keeps data in Australia and demonstrates commitment to Australian businesses which can use the cloud platform without their data ever leaving Australian shores.

Our growing suite of more than 20 fully integrated apps protects digital transformation efforts and meets the needs of all security teams. Consolidate your security and compliance stacks with Qualys apps for: Asset Management; IT Security; Cloud and Container Security; Web Application Security; and Compliance. The benefits of Qualys include:

- ✓ Get a complete and continuously updated view of all your IT assets – from a single-pane-of-glass UI
- ✓ Eliminate information silos via shared data collection and use
- ✓ Easily access all apps from a central, common web interface
- ✓ Conveniently provision more apps by simply checking a box
- ✓ Forget about software maintenance with self-updating, cloud-hosted apps
- ✓ Save time and money with an all-in-one, cloud-based solution

The ASD Essential Eight

The Australian Cyber Security Centre (ACSC), part of the Australian Signals Directorate (ASD), is the Australian Government's lead agency for improving cyber security.

The ACSC's cyber security mission is supported by ASD's wider organisation and provide mitigation strategies to help organisations protect themselves against various cyber threats. The lead mitigation strategies are included in what is known as the Essential Eight.

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC as a baseline. By adhering to the Essential Eight, it is more difficult for attackers to compromise systems.

The mitigation strategies that constitute the Essential Eight are: application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication and regular backups.

To assist organisations with their implementation of the Essential Eight, four maturity levels have been defined, from Maturity Level Zero through to Maturity Level Three.

The Essential Eight Maturity Model is designed to assist organisations to implement the Essential Eight in a graduated manner based upon different levels of threats.

The different maturity levels can also be used to provide a high-level indication of an organisation's cyber security maturity, and generally, there are:

- **Maturity Level Zero:** There are weaknesses in an organisation's overall cyber security posture.
- **Maturity Level One:** The organisation is exposed to adversaries who are content to simply leverage widely available exploits.
- **Maturity Level Two:** The organisation might be exposed to attackers with slightly higher capability from the previous maturity level, including more targeted attacks.
- **Maturity Level Three:** Is aimed at protecting against attackers who are more adaptive and much less reliant on public tools and techniques.

Maturity Level Three is the benchmark for Australian enterprise and government, including for critical infrastructure providers and other organisations that operate in high threat environments.

2021 updates to the Essential Eight Maturity Model

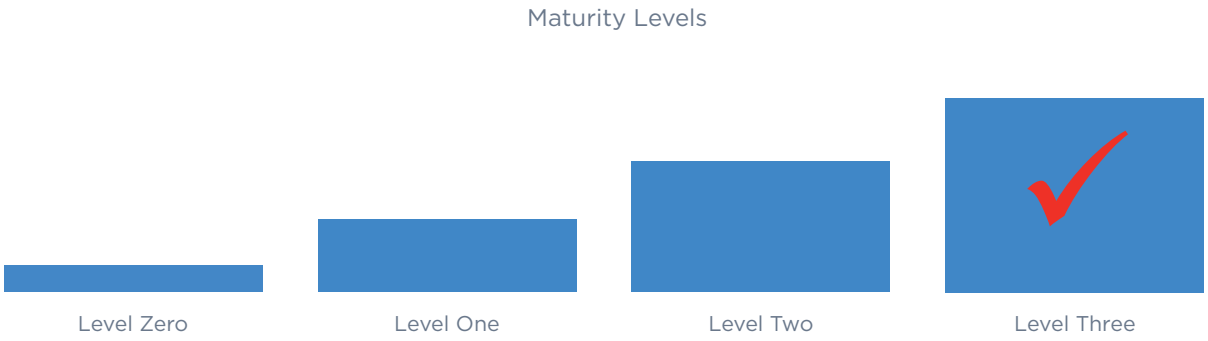
In July 2021 the ACSC published updates to the Essential Eight Maturity Model.

According to the ACSC, this update focused on using the maturity levels to counter the sophistication of different levels of adversary tradecraft and targeting rather than being aligned to the intent of a mitigation strategy, including:

- Redefining the number of maturity levels and what they represent.
- Moving to a stronger risk-based approach to implementation.
- Implementing the mitigation strategies as a package.

The update also introduces monitoring to support identification and response to cyber security events as a general Maturity Level Three capability. This is an important vindication of, and step towards, real time security.

With real time security, organisations can more confidently meet the Essential Eight guidelines and quickly discover if improvements are needed to their security posture.



How Qualys Helps Meet the Essential Eight

Qualys enables you to analyse threats and misconfigurations in real time, which helps you validate your compliance with the Essential Eight at the pace required to mitigate threats.

In this report we will focus on Maturity Level Three, the highest maturity level and indicative of the capability Australian enterprise and government organisations must work towards achieving.

1. Application control

Application control covers restrictions on code and applications being executed on workstations and servers outside an approved set. At the highest maturity level, this includes the ability to:

- Restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set.
- Microsoft's 'recommended block rules' and 'recommended driver block rules' are implemented.
- Application control rulesets are validated on an annual or more frequent basis and allowed and blocked executions are centrally logged and protected from unauthorised modification and actioned when cyber security events are detected.

July 2021 updates

- Additional executable content types (i.e. compiled HTML, HTML applications and control panel applets) were introduced for all maturity levels.

How Qualys helps

- ✓ Qualys delivers Cyber Security Asset Management, which puts a security lens on your assets. It tells you about the asset and how secure it is.
- ✓ Qualys can define approved or disallowed software and can automatically apply or uninstall packages, including any required end-point agents
- ✓ Anything approved can be run and Qualys can tell you what unauthorised packages you have
- ✓ If an organisation aspires to become Essential Eight complaint, then application control is a first step and Qualys can identify what software people are using, and if it is approved

2. Patch applications

At number two is patch applications, which recommends vendor patches and updates for internet-facing services, including office productivity suites, web browsers and their extensions, email clients, PDF software, and security products, are applied within two weeks of release, or within 48 hours if an exploit exists.

At the highest maturity level:

- Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month.
- A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services and browsers and productivity apps.
- A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.
- Applications that are no longer supported by vendors are removed.

July 2021 updates

- Patching requirements were updated for all maturity levels to remove the need for every security vulnerability to be individually risk-assessed to determine patching timeframes.
- Maturity Level Three introduced patching office productivity suites, web browsers and their extensions, email clients, PDF software, and security products within 48 hours if an exploit exists, otherwise within two weeks.

How Qualys helps

- ✓ Qualys supports Maturity Level Three in its entirety
- ✓ Qualys can identify (every 4 hours) missing patches on the machine and can deploy patches either automatically or manually
- ✓ There is support for Office productivity and web browser extensions and Qualys can discover and report on end-of-life (EOL) software and hardware
- ✓ Qualys has industry leading vulnerability scanning and patching, which enables you to patch and validate
- ✓ When you deploy a patch has it been properly deployed? Qualys can check.

3. Configure Microsoft Office macro settings

Microsoft Office macros can be used to automate tasks across the office productivity suite, but can also be used for malicious purposes.

At the highest maturity level, the Essential Eight recommends Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. In addition:

- Only Microsoft Office macros running from within a sandboxed environment, a trusted location or that are digitally signed by a trusted publisher are allowed to execute. Untrusted macros cannot be enabled via the Message Bar or Backstage View.
- Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within trusted locations.
- Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis. Microsoft Office macros in files originating from the internet are blocked, and macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users.
- Microsoft Office macro antivirus scanning is enabled and allowed and blocked Microsoft Office macro executions are centrally logged and protected from unauthorised modification.

July 2021 updates

- To lower an organisation's attack surface, all maturity levels were updated to recommend that macros are disabled for all users who do not have a requirement for their use.
- Maturity Level Three was updated to allow for either macros running from within a sandboxed environment, a trusted location or that that are digitally signed by a trusted publisher to execute. Preventing digitally signed macros signed by an untrusted publisher from being enabled via the Message Bar or Backstage View in Microsoft Office applications is also new.
- Maturity Level Three introduced an annual (or more frequent) validation of trusted publishers and monitoring to support identification and response to cyber security events.

How Qualys helps

- ✓ Qualys validates changes. To disable macros a registry change needs to be made, and often that is not validated
- ✓ Qualys Policy Compliance has a number of controls that can access and validate whether macros are appropriately configured and running from appropriate locations
- ✓ Qualys can also check of you have other agents running which are designed to make specific changes with Office macros
- ✓ The July 2021 update adds validation and Qualys can validate whether an organisation has gone through Maturity Level Three and if settings are in place or not

4. User application hardening

At number four is application hardening which focuses on reducing the likelihood of end-user applications running malicious code.

The highest maturity level recommends:

- Web browsers do not process Java or web advertisements from the internet and Internet Explorer 11 is disabled or removed. Web browser, Microsoft Office and PDF software security settings cannot be changed by users.
- Microsoft Office is blocked from creating child processes; from creating executable content; from injecting code into other processes; and configured to prevent activation of OLE packages.
- ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented, and PDF software is blocked from creating child processes.
- NET Framework 3.5 (including .NET 2.0 and 3.0) is disabled or removed. Windows PowerShell 2.0 is disabled or removed, and PowerShell is configured to use Constrained Language Mode. Blocked PowerShell script executions are centrally logged and protected from unauthorised modification.

July 2021 updates

- As Adobe Flash Player reached end of life on 31 December 2020, it is now considered an unsupported application and addressed by the 'patch applications' mitigation strategy instead.
- Maturity Level Three introduced disabling or removing Internet Explorer 11, .NET Framework 3.5 (including .NET 2.0 and 3.0), and Windows PowerShell 2.0 features from Microsoft Windows.
- Maturity Level Three introduced the use of PowerShell in Constrained Language Mode and monitoring to support identification and response to cyber security events.

How Qualys helps

- ✓ Qualys helps assess the user application policy and can flag and remediate controls which compromise policy
- ✓ Qualys can identify and remove the risk of a machine either has not received changes, or if someone has done it locally
- ✓ Qualys can help validate and report on the level of user application hardening compliance

5. Restrict administrative privileges

Restricting administrative privileges is an ideal first step in preventing accidental or malicious system compromise and data breaches. This guideline has general recommendations for privileged access management to systems and applications. Privileged access should be validated, limited to specific duties and automatically disabled after periods of inactivity.

Privileged accounts should be prevented from accessing the internet, email and web services, and use separate privileged and unprivileged operating environments. The Highest maturity level also recommends:

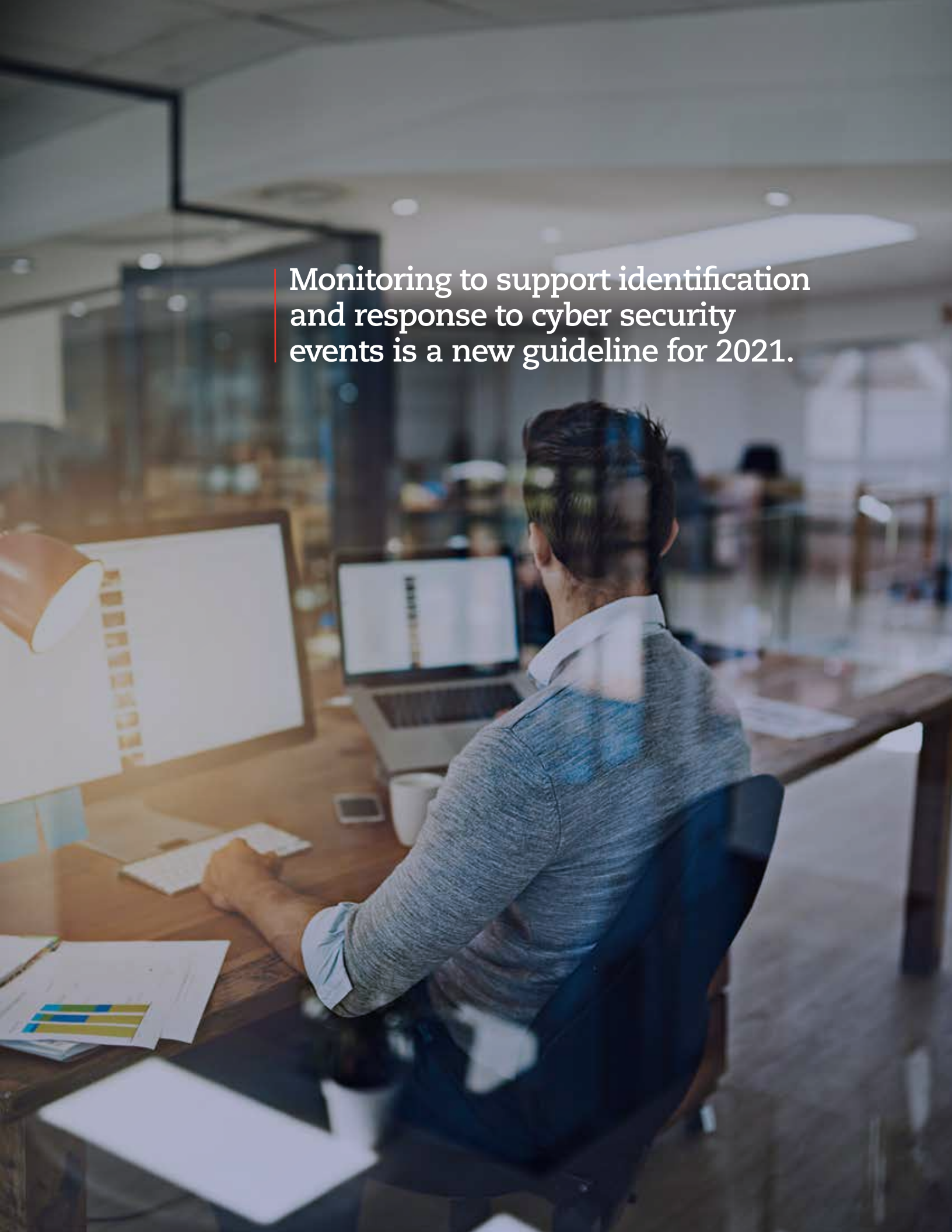
- Just-in-time administration is used for administering systems and applications. Administrative activities are conducted through jump servers.
- Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.
- Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.
- Use, and changes to, privileged access accounts is centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

July 2021 updates

- Requirements relating to policy controls were removed and emphasis was placed on separating privileged and unprivileged operating environments, and the accounts associated with them, for all maturity levels.
- Maturity Level Three introduced the use of just-in-time administration for administering systems and applications and the use of Windows Defender Credential Guard and Windows Defender Remote Credential Guard. Monitoring to support identification and response to cyber security events is also new.

How Qualys helps

- ✓ Qualys can report on administration privileges, and can validate if proposed changes are needed
- ✓ Qualys can identify and remove the risk of a machine either has not received changes, or if someone has done it locally
- ✓ Qualys can help validate and report on the level of administrative privilege compliance



Monitoring to support identification and response to cyber security events is a new guideline for 2021.

6. Patch operating systems

At number six is patch operating systems which focuses on applying patches, updates, or vendor mitigations for security vulnerabilities in operating systems of workstations and internet-facing services in a timely manner, including within 48 hours if an exploit exists.

The highest maturity level recommends:

- A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services, and at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices.
- The latest release, or the previous release, of operating systems are used for workstations, servers and network devices, and operating systems that are no longer supported by vendors are replaced.

July 2021 updates

- Patching requirements were updated for all maturity levels to remove the need for every security vulnerability to be individually risk-assessed to determine patching timeframes.
- Maturity Level Three introduced patching operating systems of workstations, servers and network devices within 48 hours if an exploit exists, otherwise within two weeks.
- Maturity Level Three introduced using the latest release, or the previous release, of operating systems for workstations, servers and network devices.

How Qualys helps

✓ Qualys has market-leading vulnerability scanning which can discover vulnerabilities and then patch operating systems

✓ Qualys can report on things that are either becoming specifically end-of-life or end-of-support

✓ Qualys helps plan for upgrades or help with planning a different approach to keeping systems patched. Such data might not be included in a typical vulnerability scan

7. Multi-factor authentication

Multi-factor authentication (MFA) is becoming a standard to improve access to systems and services that rely on a single password. In number seven of the Essential Eight, it is recommended multi-factor authentication is used by staff for internet-facing services; third-party internet-facing services for both sensitive and non-sensitive organisational data; and generally, cannot be impersonated.

The Highest maturity level also recommends:

- Multi-factor authentication is enabled by default for non-staff (with opt out) if they authenticate to an organisation's internet-facing services.
- Multi-factor authentication is used to authenticate privileged users of systems and users accessing important data repositories.
- Successful and unsuccessful multi-factor authentications are centrally logged and protected from unauthorised modification and actioned when cyber security events are detected.

July 2021 updates

- Multi-factor authentication requirements were updated to focus on the use of different types of authentication factors (e.g. something you know, something you have and something you are) rather than specific authentication factors (e.g. password, smartcard and fingerprint).
- Maturity Level Three was updated to focus on the use of cryptography to protect against real-time phishing attacks and machine-in-the-middle attacks, and also introduced monitoring to support identification and response to cyber security events.

How Qualys helps

✓ Qualys can validate MFA, which is a setting on both Mac and Windows, and also discover if MFA is enforced on a range of popular internet-facing services and third-party SaaS and PaaS platforms

✓ Qualys also has partnerships with industry-leading MFA vendors

✓ The Qualys Cloud Platform supports MFA for access control

Scanning should be done at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

8. Regular backups

The final Essential Eight is a set of guidelines for backups and data protection.

Backups of important data, software and configuration settings should be performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Additionally, restoration of systems, software and important data from backups should be tested in a coordinated manner as part of disaster recovery (DR) exercises.

The highest maturity level also recommends:

- Unprivileged accounts, and privileged accounts (excluding backup administrators), cannot access backups.
- Unprivileged accounts, and privileged accounts (excluding backup break glass accounts), are prevented from modifying or deleting backups.

July 2021 updates

- Backup requirements were updated to focus on performing and retaining backups in accordance with an organisation's own business continuity requirements, as opposed to specifying backup frequencies and backup retention timeframes.
- Maturity Level Three introduced preventing unprivileged accounts and privileged accounts (excluding backup administrators or break glass accounts) from accessing, modifying or deleting any backups.

How Qualys helps

✓ Qualys can validate whether backups have been taken and if the appropriate backup software or agent is running on the target machines

✓ Qualys can also check for backup settings on the local machine

Conclusion

The Australian Cyber Security Centre (ACSC) Essential Eight is now a benchmark for an improved security posture that is more resilient to the growing pace of cyber-attacks.

The 2021 updates to the Essential Eight call for more routine vulnerability scanning, in addition to ACSC's recommend the use of more continuous security tactics.

Being proactive with the Essential Eight can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

Organisations have access to numerous solutions to meet the Essential Eight guidelines, however, many organisations are not able to validate whether they are meeting or exceeding the guidelines in an automated way.

The Qualys Cloud Platform brings industry-leading real time security capability to your organisation. Qualys helps IT and business leaders confidently meet the ASD Essential Eight by giving them the visibility they need into compliance and an appropriate course of action.

Take control of the ASD Essential Eight cyber security guidelines with continuous security from Qualys.


Born in the cloud, with a fresh approach to security
Qualys.

About Qualys.

The leading provider of IT security and compliance solutions at your fingertips.

The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

Request a full trial (unlimited scope) at qualys.com/trial

Qualys is easy to implement, easy to use, fully scalable – and requires NO infrastructure or software to maintain.

Trusted globally

More than 10,300 global businesses in more than 130 countries trust Qualys to underpin digital transformation for greater agility, better business outcomes, and substantial cost savings.

74% of the Forbes Global 50 rely on Qualys and:

- **9 of the top 10 in Technology**
- **9 of the top 10 in Retail**
- **9 of the top 10 in Biotech**
- **7 of the top 10 in Chemical**
- **7 of the top 10 in Banking**

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 10,300 customers in more than 130 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and consolidate their security and compliance solutions in a single platform and build security into digital transformation initiatives for greater agility, better business outcomes and substantial cost savings. The Qualys Cloud Platform and its integrated Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds.

For more information, please visit **qualys.com**

Qualys, Inc. (APAC)
39/2 Park Street
Sydney NSW 2000
Australia

tel: 1800 233 647

sales_anz@qualys.com