GFI GUIDE

Understanding Essential Eight compliance and why it matters

GFI Software™

Contents

Essential Eight

The Essential Eight is a robust cybersecurity framework developed by the Australian Cyber Security Centre (ACSC) to empower organizations in safeguarding their digital assets and sensitive information from prevalent cyber threats. This comprehensive set of strategies focuses on addressing common attack vectors exploited by malicious actors to gain unauthorized access, exfiltrate data, or disrupt operations.

Key strategies of Essential Eight

1 Application whitelisting

Guarantee that only approved applications are allowed to run on systems, preventing unauthorized or malicious software from executing.

2 Patch applications

Consistently update applications to eliminate vulnerabilities and shield against known exploits.

3 Configure Microsoft Office macro settings

Regulate the execution of macros in Microsoft Office to thwart the exploitation of malicious macros.

4 User application hardening

Establish secure settings in web browsers and email clients to minimize the risk of malware delivery and exploitation.

5 Restrict administrative privileges

Restrict administrative access to authorized personnel, mitigating unauthorized system changes.

6 Multi-Factor Authentication (MFA)

Integrate MFA to enhance user authentication and minimize the likelihood of unauthorized access.

7 Patch operating systems

Regularly update operating systems to resolve security vulnerabilities and avert potential exploitation.

8 Daily Backups

Execute daily backups of critical data to facilitate recovery in the event of a cyber incident.

Implementation of Essential Eight

Attaining Essential Eight compliance requires organizations to effectively implement the recommended security controls associated with each strategy. Which means, adopting best practices such as application whitelisting, frequent patching, user education, and secure configurations.

Benefits of Essential Eight

- Enhanced cyber resilience

  The Essential Eight establishes a formidable defense against common cyber threats, thereby decreasing the susceptibility to successful attacks.

- Mitigated data breach risks

  The implementation of these strategies significantly diminishes the likelihood of data breaches and unauthorized access to sensitive information.

- Improved incident response

  The presence of these security controls enhances an organization's capacity to efficiently detect and respond to cyber incidents.

- Regulatory compliance

  Essential Eight compliance signifies an organization's dedication to cybersecurity and aligns with regulatory requisites.

- Business continuity

  By securing critical data and systems, the Essential Eight framework contributes to the seamless continuation of business operations.

Essential Eight certification

Unlike a traditional certification process, Essential Eight compliance is demonstrated through the effective implementation of the security strategies. However, Essential Eight implementations may need to be assessed by an independent party if required by a government directive or policy, by a regulatory authority, or as part of contractual arrangements.

Organizations can engage with the ACSC for guidance and assistance in aligning their cybersecurity practices with the framework.

Significance of Essential Eight for Australian organizations

As cyber threats persistently evolve, Australian organizations are not immune to these risks. The adoption of Essential Eight strategies is imperative for safeguarding sensitive data, upholding customer trust, and averting potentially costly breaches.

GFI LanGuard and Essential Eight controls

As cyber threats persistently evolve, Australian organizations are not immune to these risks. The adoption of Essential Eight strategies is imperative for safeguarding sensitive data, upholding customer trust, and averting potentially costly breaches.

Requirements under Control #2 Patch Applications & Control #7 Patch Operating Systems

The requirements within both controls are the same. Furthermore, the Essential Eight encompasses three “maturity” levels, with requirements becoming more stringent as the levels increase. Nevertheless, the operational requisites remain the same. It's primarily the frequency of these operations that intensifies, meaning you can achieve even the highest level (3) through more frequent scheduled scans and patch deployment operations through GFI LanGuard. More details about maturity levels here. Let's have a look at the requirements:

- An automated method of **asset discovery** is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
- A **vulnerability scanner with an up-to-date vulnerability database** is used for vulnerability scanning activities.
- A vulnerability scanner is used at least daily to **identify missing patches or updates** for vulnerabilities in internet-facing services.
- A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in **office productivity suites, web browsers, and their extensions, email clients, PDF software, and security products.**
- Patches, updates, or other vendor mitigations for vulnerabilities in internet-facing services are applied within two weeks of release, or 48 hours if an exploit exists.
- Patches, updates, or other vendor mitigations for vulnerabilities in office productivity suites, web browsers, and their extensions, email clients, PDF software, and security products are applied within one month of release.

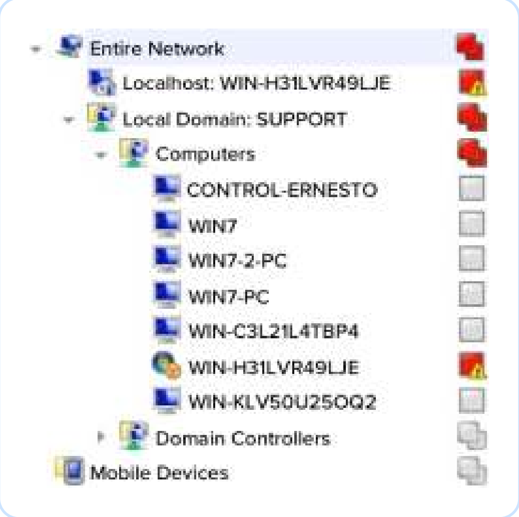
- Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security **products that are no longer supported by vendors are removed.**

How GFI LanGuard can help

GFI LanGuard enables you to manage and maintain end-point protection across your network. It provides visibility into all the elements in your network, helps you assess where there may be potential vulnerabilities, and enables you to patch them. The patch management and network auditing solution is easy to use and easy to deploy. To aid in maintaining Control #2 and Control #7 in Essential Eight, consider leveraging GFI LanGuard, a comprehensive solution designed to streamline and enhance your cybersecurity efforts.

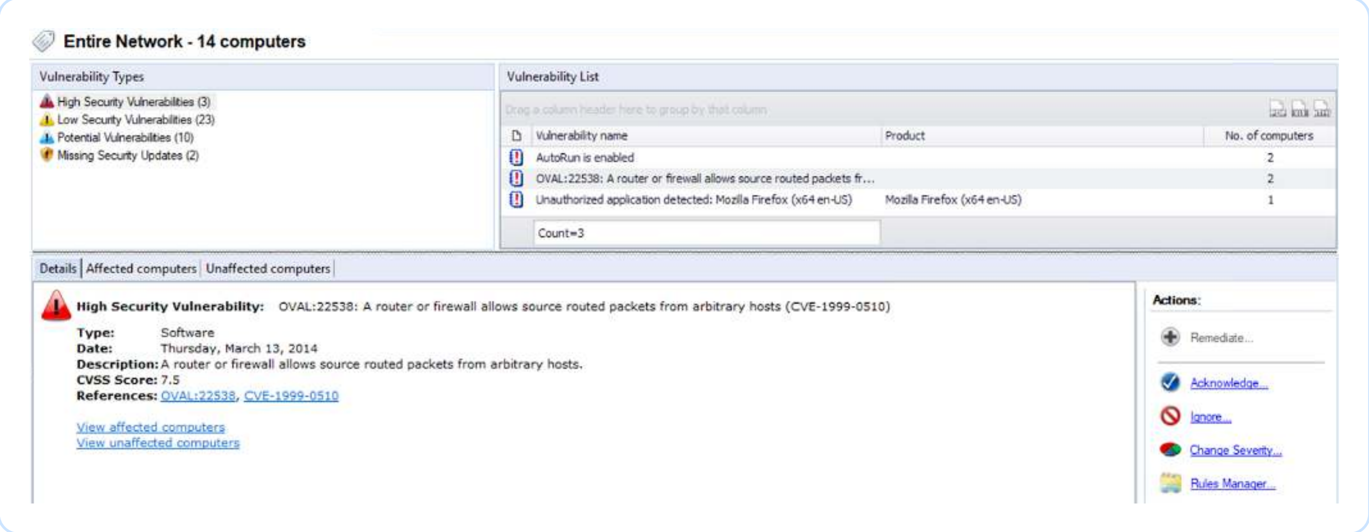
Asset discovery

GFI LanGuard facilitates the automatic discovery of all elements within your network, spanning computers, laptops, mobile devices, printers, servers, virtual machines, routers, and switches.



Vulnerability scanning

Benefit from GFI LanGuard's extensive vulnerability assessment database, boasting over 60,000 checks from established standards like OVAL (11,500+ checks) and SANS Top 20. The database receives regular updates, incorporating information from sources like BugTraq, SANS Corporation, OVAL, and CVE.



Entire Network - 14 computers

Vulnerability Types

- High Security Vulnerabilities (3)
- Low Security Vulnerabilities (23)
- Potential Vulnerabilities (10)
- Missing Security Updates (2)

Vulnerability List

Drag a column header here to group by that column

	Vulnerability name	Product	No. of computers
ⓘ	AutoRun is enabled		2
ⓘ	OVAL:22538: A router or firewall allows source routed packets fr...		2
ⓘ	Unauthorized application detected: Mozilla Firefox (x64 en-US)	Mozilla Firefox (x64 en-US)	1
	Count=3		

Details | Affected computers | Unaffected computers

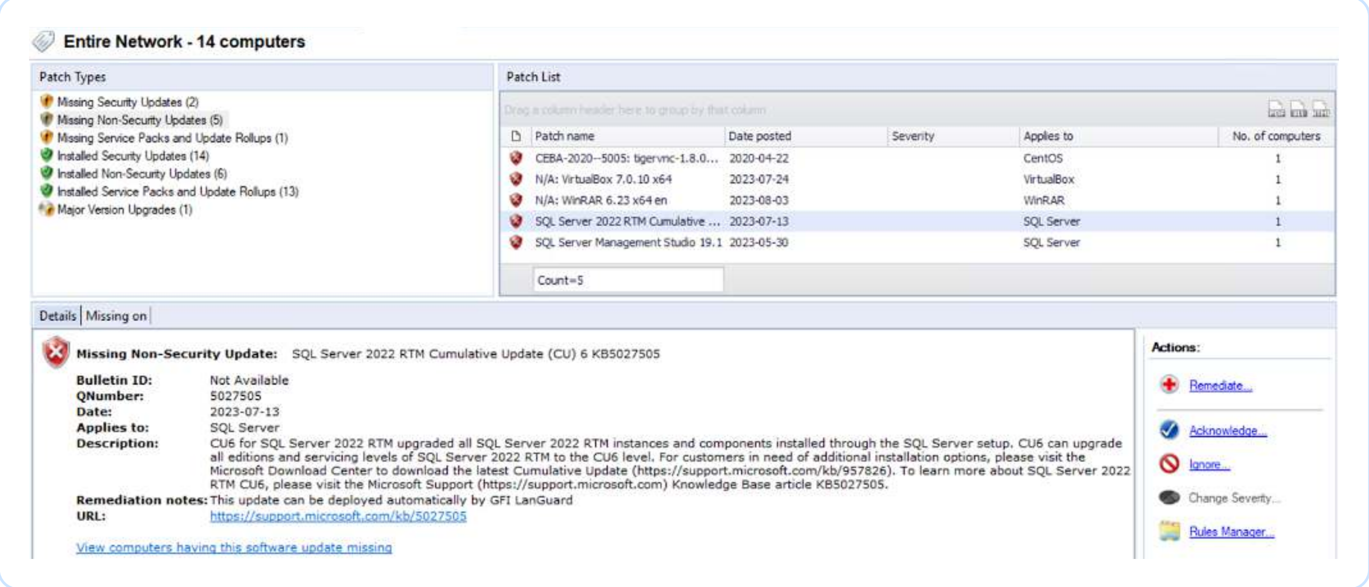
High Security Vulnerability: OVAL:22538: A router or firewall allows source routed packets from arbitrary hosts (CVE-1999-0510)

Type: Software
Date: Thursday, March 13, 2014
Description: A router or firewall allows source routed packets from arbitrary hosts.
CVSS Score: 7.5
References: OVAL:22538, CVE-1999-0510

View affected computers
View unaffected computers

Identifying missing patches or updates

GFI LanGuard automates patch management to maintain up-to-date software. It conducts network scans to identify absent updates in applications, operating systems, web browsers, and third-party software such as Adobe and Java.



Entire Network - 14 computers

Patch Types
Missing Security Updates (2)
Missing Non-Security Updates (5)
Missing Service Packs and Update Rollups (1)
Installed Security Updates (14)
Installed Non-Security Updates (6)
Installed Service Packs and Update Rollups (13)
Major Version Upgrades (1)
Patch List
Drag a column header here to group by that column

Patch name	Date posted	Severity	Applies to	No. of computers
CEBA-2020--5005: tigervnc-1.8.0...	2020-04-22		CentOS	1
N/A: VirtualBox 7.0.10 x64	2023-07-24		VirtualBox	1
N/A: WinRAR 6.23 x64 en	2023-08-03		WinRAR	1
SQL Server 2022 RTM Cumulative ...	2023-07-13		SQL Server	1
SQL Server Management Studio 19.1	2023-05-30		SQL Server	1

Count=5

Missing Non-Security Update: SQL Server 2022 RTM Cumulative Update (CU) 6 KB5027505

Bulletin ID: Not Available
QNumber: 5027505
Date: 2023-07-13
Applies to: SQL Server
Description: CU6 for SQL Server 2022 RTM upgraded all SQL Server 2022 RTM instances and components installed through the SQL Server setup. CU6 can upgrade all editions and servicing levels of SQL Server 2022 RTM to the CU6 level. For customers in need of additional installation options, please visit the Microsoft Download Center to download the latest Cumulative Update (https://support.microsoft.com/kb/957826). To learn more about SQL Server 2022 RTM CU6, please visit the Microsoft Support (https://support.microsoft.com) Knowledge Base article KB5027505.
Remediation notes: This update can be deployed automatically by GFI LanGuard
URL: https://support.microsoft.com/kb/5027505

View computers having this software update missing

Automated patch deployment

Ease the burden of manual updates with GFI LanGuard's automated patch deployment feature. Updates can be deployed across the system or on specific machines using agents for regular updates. Additionally, you have control over which patches to install and can roll back changes if needed.

Integration with third-party security applications

GFI LanGuard integrates with over 4,000 security applications, including antivirus, firewalls, backup clients, and more. It provides insights into installed applications and resolves issues requiring attention, such as triggering antivirus or anti-spyware updates.

Compliance with other regulations

GFI LanGuard generates automated network security reports that assist in demonstrating compliance with various regulations such as ISO 27001/27002, PCI DSS, HIPAA, and SOX. By embracing GFI LanGuard, organizations can efficiently manage and fortify endpoint protection throughout their network. The solution's user-friendly interface and deployment ease make it a powerful asset in enhancing cybersecurity measures and Essential Eight compliance.