THREATLOCKER®
ZERO TRUST PLATFORM

DEFENSE AGAINST CONFIGURATIONS

DAC REPORT

SAMPLE

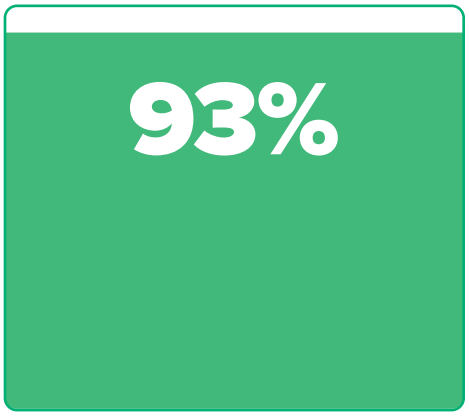
PREPARED FOR

CLIENT COMPANY

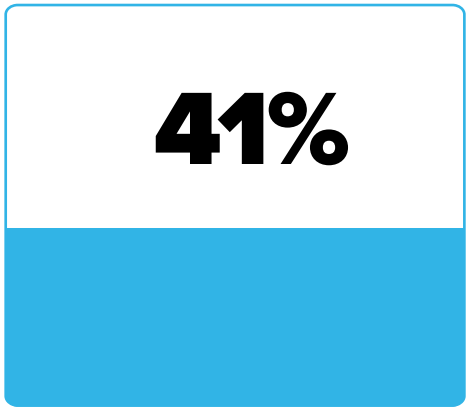
EXECUTIVE SUMMARY - LAST 7 DAYS

During the reporting period, a total of 26 configurations were analyzed on 558 computers. This resulted in **651** critical impact failures, **812** high impact failures, **543** moderate impact failures, and **431** low impact failures, with a potential for **2,437** compliance violations.

Compared to the previous reporting period, critical impact failures have not increased, high impact failures have not increased, moderate impact failures have **not increased**, low impact failures have **not increased** and potential compliance violations have not increased.



93% of your environment is free from misconfigurations, tested across 558 endpoints.



Since your last report, you have reduced your misconfigurations by 41%.

Out of 200 unqiue analyses, 36 of them had no impacted computers.

Criticality Summary

Below are the criticality results of endpoints within your organization. Categorized by risk level, the total number of reported risks across all endpoints is summarized from Critical to Low Risk. High counts of Critical and High-Risk findings warrant evaluation due to potential concerns with non-compliance and misconfiguration.

651	812	543	431
Critical Risk	High Risk	Moderate Risk	Low Risk

85

Analyses Passed

The total number of DAC analyses that found all computers in the environment free of misconfiguration within the report period.

36

Analyses Failed

The total number of DAC analyses that revealed at least 1 computer in the environment has misconfigurations that could expose the organization to security and compliance gaps.

ORGANIZATION GRADESHEET

This gradesheet evaluates a rating based on all categories analyzed, signifying the organization's overall security rating over the analysis period. The graphic depicted below shows the organization's "Environment Security Rating", the cumulative rating after evaluating all categories and parameters.

93% Out of **200** unique analyses, your organization's overall security grade sits at **93%.**

23% Since your last report, your organization's overall security grade has **improved 23%.**

Each category shows an evaluation below. Identifying underperforming categories with scores that indicate significant amounts of misconfiguration can assist organizations in identifying specific areas that are necessary to address.

Account and Authentication	Advanced Audit Configuration
85 ↓	90 ↑

Account and Authentication

Controls in this category govern user account creation, management, and authentication. Emphasis is placed on password lockout policies and configurations to protect user credentials. Proper configuration is essential for preventing brute-force attacks, credential stuffing, insider misuse, and lateral movement.

Advanced Audit Configuration

Windows-specific settings that allow for granular tracking and monitoring of system events, such as logon attempts, object access, and privilege use. These events support continuous monitoring, aid in incident response, and are key in assisting in forensics and threat detection.

Local Security	Network
95 ↑	100 ↑

Local Security

These policies are housed in the system's group policy, local security, or registry settings and enforce centralized security settings over domain-joined endpoints. By standardizing policy implementation, these settings ensure consistent policy implementation over multiple machines and reduce the threat of misconfiguration.

Network

Policies relating to Network Control and enforcing boundary protection and transmission security. This includes configuring Network Control policies to prevent untrusted IPs from connecting to the SMB port, helping protect against data exfiltration, lateral movement, and credential theft.

Patch Management
88 ↑

Patch Management

Assist in verifying that software is up to date. Checks contained here will alert users to the presence of outdated third-party applications on their systems. Proper Patch Management eliminates the threat of vulnerabilities in outdated software.

Application Control
92 ↑

Application Control

Focuses on managing applications and configuring Ringfencing™ control within a system to prevent unnecessary elevated permissions, unauthorized application interaction, and the use of unwanted software. Examples include ensuring CMD is not permanently elevated and preventing web browsers from interacting with PowerShell to prevent exploitation.

Registry
96

Registry

Registry Policies enforce security at the registry level; Registry analyses will check security baselines to ensure they are consistent with compliance standards to meet security best practices such as disabling “Remote Shell” and “UPnP.”

Remote Desktop and Access Control
98 ↑

Remote Desktop and Access Control

Focusing on security settings and policies for RDP and other remote access services, this category has a focus on disabling RDP where not needed, and locking down RDP connections and privileges where applicable.

Storage
91

Storage

Storage policies will control access, encryption, and retention of data on disks, removable media, and cloud storage. Vital for protecting data at rest, or in transit—this category focuses on Storage Control policies that will block access to unauthorized USB drives or access to components such as VHDs.

Detection and Response
94 ↑

Detection and Response

This category examines ThreatLocker® Detect settings to ensure organizations have policies in place to detect and respond to common endpoint anomalies. This includes monitoring for large amounts of file changes on a system, or mismatches of exploitable files such as sethc.exe (Sticky Keys).

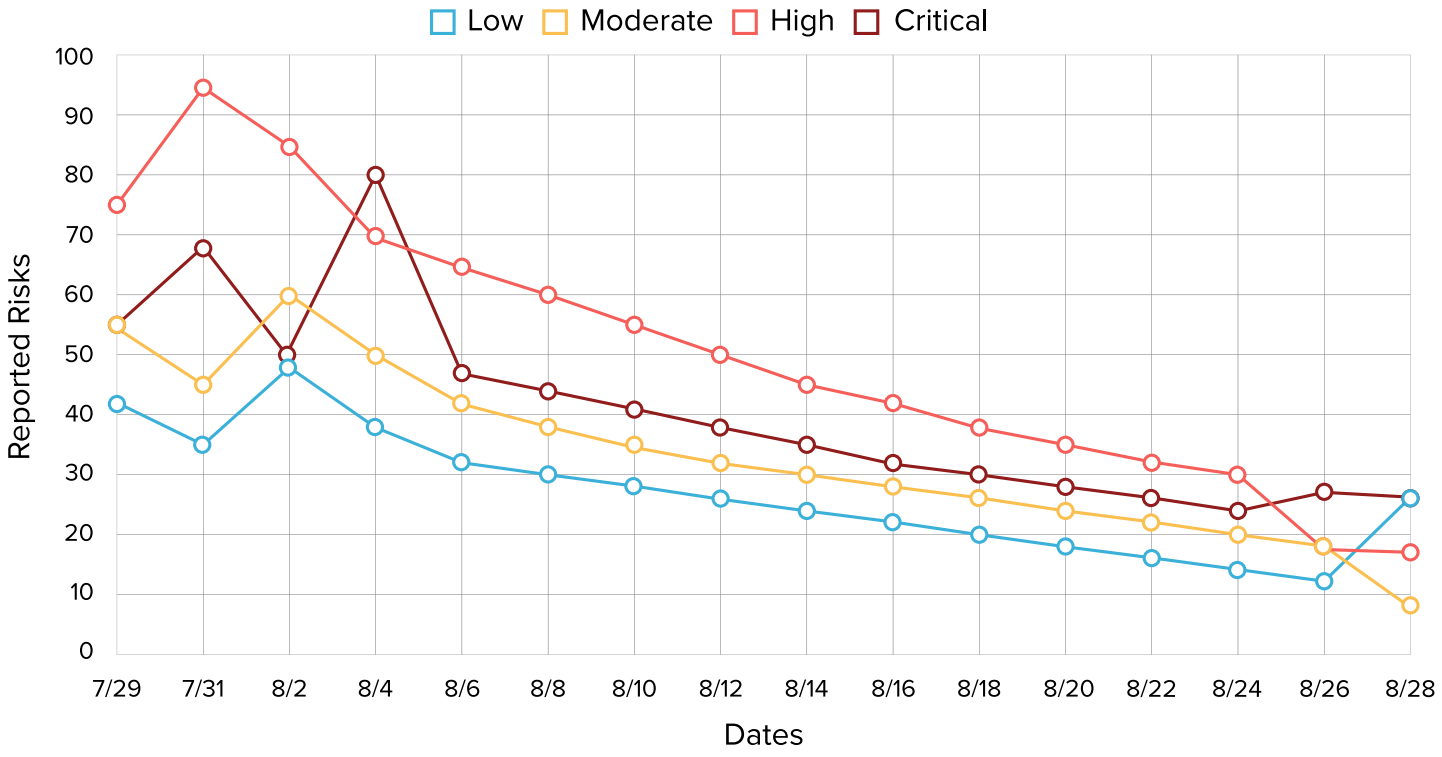
User Rights Assignment
100 ↑

User Rights Assignment

Policies defining which user/groups can perform specific actions within an endpoint, such as shutting down the system or using debug programs. This limits insider threat and enforces least privilege in user environments.

Criticality Trend

The graph below depicts the trending results of all criticality levels within the analysis period. Failed compliance checks, categorized by criticality level, can be observed daily to identify configuration points of failure on a granular level.



Potential Compliance Violations Breakdown

The graphic below highlights the organization's number of failed configuration checks within each compliance framework. Higher quantities within a framework indicate the need for additional evaluation if compliance is required.

23 NYCRR 500	CAN/DGSI 104	CCPA	CIS Controls	CMMC	COBIT	Cyber Essentials
10	6	7	10	10	6	8

Essential 8	FedRAMP	FISMA	GDPR	HIPAA	ISO IEC 27001	ITIL
10	9	6	10	7	8	10

NIS2	NIST 800-171	NIST 800-53	NIST CSF	PCI DSS	SOC2	SOX
6	10	7	10	8	8	10

Security Issue:

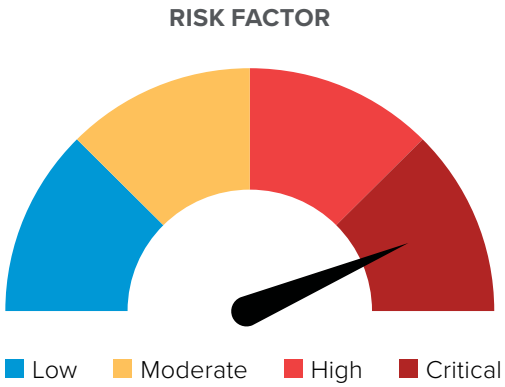
UNTRUSTED RDP IS BLOCKED | Critical

Related Frameworks

CIS_Controls | CMMC | Essential 8 | HIPAA | ISO_IEC_27001 | NIST 800-171 | NIST 800-53 | NIST_CSF

72%

435 out of 558 endpoints, didn't pass this analysis. Compared to your last report, this is down 12%.



What This Means for Your Environment

Blocking untrusted sources from RDP (Remote Desktop Protocol) restricts unauthorized connections from accessing systems remotely. RDP is a common entry point for ransomware/malware attacks, with around 90% of cyber-attacks showing RDP exploitation.

Why This Is a Potential Risk

Once breached, a system can become a victim of DOS/DDOS, brute-force, and credential stuffing attacks. Attacks via RDP may also result in decreased logging of system events, making it more challenging for forensic teams to investigate potential breaches. This is particularly true when threats can move laterally through systems, stealing sensitive data and escalating privileges to dangerous entities.

How to Resolve This Issue

Utilizing Network Control policies to outright restrict the use of RDP is the ideal method to prevent attacks through remote connections. For example, the ThreatLocker Community policy "Deny RDP – Inbound" will restrict the port (3389) associated with RDP connections.

Even having RDP exposed on a local network is dangerous; attackers can gain access to a single machine and move laterally through the network. Ensure Administrative privileges for RDP are reserved for personnel who require access.

Comprehensive logging of remote sessions can help detect anomalies that may emerge from suspicious RDP use. The ThreatLocker® Detect policy "TL.EV.1013 - RDP login from a public IP" assists in alerting to any public IP connections through Remote Protocol.

Real World Example

In 2019, a vulnerability named "BlueKeep (CVE-2019-0708)" affected Windows systems by exploiting a weakness in Remote Desktop Services. The threat was classified as "wormable," because it could spread between systems without any user interaction.

According to Microsoft, CVE-2019-0708 is a critical vulnerability in Remote Desktop Services that allowed remote code execution. Attackers could send a specially crafted packet to an operating system with RDP enabled, allowing them to install programs, modify or delete data, and create user accounts with full user rights.

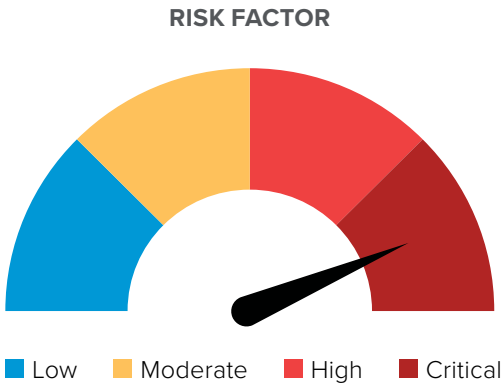
Security Issue:

MSHTA BLOCKED OR RESTRICTED | Critical

Related Frameworks

CIS_Controls | CMM | Essential 8 | FedRAMP | FISMA | GDPR | HIPAA | ISO_IEC_27001 | NIST 800-171 | NIST 800-53 | NIST_CSF | PCI_DSS | SOC2

58% **324 out of 558 endpoints,** didn't pass this analysis. Compared to your last report, this is up 8%.



What This Means for Your Environment

MSHTA is a legitimate Microsoft binary used to execute HTML Application files. Since mshta.exe is a trusted component of Windows systems, it is commonly utilized by attackers to execute malicious scripts remotely. Blocking the file outright can prevent living-off-the-land attacks.

Why This Is a Potential Risk

Without proper allowlisting tools, security systems may inadvertently permit MSHTA activity, facilitating malware spread. MSHTA attacks can run code via URLs on external servers, conducting fileless attacks that leave minimal traces for antivirus detection. Additionally, MSHTA can be embedded in scheduled tasks, providing persistent access and further network propagation.

How to Resolve This Issue

Creating an Allowlisting policy to deny mshta.exe can ensure that the Windows binary is not permitted on the system. Unless the program has a designed business need, the ThreatLocker Community policy "Block mshta (Built-In)" can prevent MSHTA from running on an endpoint entirely.

Otherwise, restricting MSHTA from accessing additional directories and applying rules to isolate the executable can prevent malicious use of the binary.

Real World Example

Remcos RAT uses mshta.exe to execute disguised LNK files through PowerShell to decode and reconstruct a shellcode loader into system memory. For corporations, forms like tax documents that might be commonly issued as LNK file extensions make the restriction of MSHTA even more vital.

According to Jason Soroko of Sectigo, during an interview with CSOonline,

"Tax season forces enterprises to relax their tightest content-filtering rules so employees can exchange government templates, PDF forms, and yes, zipped LNK shortcuts that many payroll systems still ship by default. Attackers are exploiting that mandated soft spot. The very policies intended to keep auditors happy become the opening gambit for a fileless breach."

Security Issue:

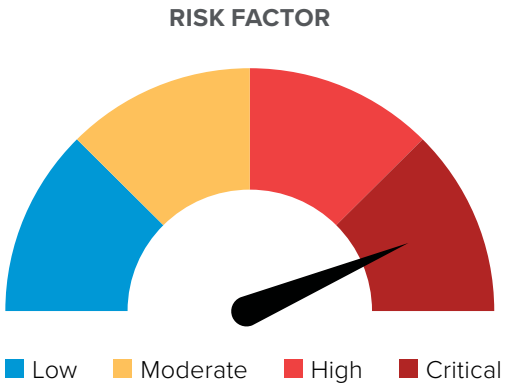
BLOCK UNTRUSTED SOFTWARE | Critical

Related Frameworks

CIS_Controls | CMM | Essential 8 | FedRAMP | FISMA | GDPR | HIPAA | ISO_IEC_27001 | NIST 800-171 | NIST 800-53 | NIST_CSF | PCI_DSS | SOC2

32%

179 out of 558 endpoints, didn't pass this analysis. Compared to your last report, this is down 27%.



What This Means for Your Environment

Essential in Zero Trust principles, block untrusted software in order to prevent execution of applications, scripts, or binaries that are not verified and explicitly allowed to run in an environment. Implement application allowlisting to prevent malware, ransomware, and other unauthorized tools and programs.

Why This Is a Potential Risk

Failing to block untrusted software opens your environment to malware, insider threats, data breaches, regulatory non-compliance, and system instability. It's essentially leaving the "front door" open to attackers and unvetted software.

How to Resolve This Issue

By implementing and maintaining a robust and comprehensive catalog of verified and approved applications, and by using deny-by-default principles, administrators can prepare their environments to block all other programs on a Zero Trust basis. Application allowlisting programs, such as Application Control from ThreatLocker®, can facilitate this process by providing pre-vetted and verified applications.

Incorporating services like third-party software patch management and application approvals can enhance allowlisting security, ensuring that software remains current and relevant.

Real World Example

In 2021, attackers modified Codecov's Bash Uploader script, allowing unverified code to run automatically in developers' CI/CD environments and exfiltrate sensitive credentials. This incident highlights why blocking untrusted software is critical: the breach occurred solely because altered, unverified software was allowed to be executed. If proper controls had been implemented, such as the enforcement of allowlisting, the breach could have been prevented.

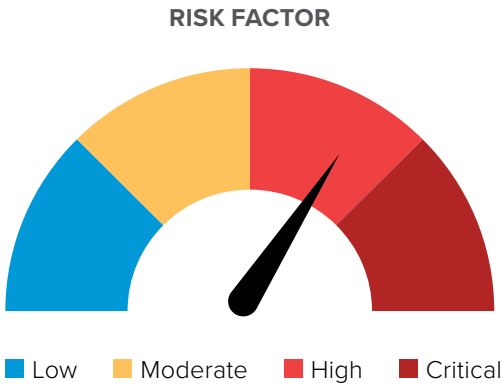
Security Issue:

BITLOCKER ENABLED ON C DRIVE | High Risk

Related Frameworks

CIS_Controls | CMMC | Essential 8 | FedRAMP | FISMA | GDPR | HIPAA | ISO_IEC_27001 | NIST 800-171 | NIST 800-53 | NIST_CSF | PCI_DSS | SOC2

21% **117 out of 558 endpoints,** didn't pass this analysis. Compared to your last report, this is down 16%.



What This Means for Your Environment

BitLocker is a native Windows feature that allows users and administrators to encrypt an entire drive on an endpoint device. BitLocker uses AES encryption to protect sensitive data and utilizes Trusted Platform Modules (TPM) to store a key that ensures only users authorized on a system can access the device drive.

BitLocker is vital because it will protect against attacks on data at rest. Additionally, if physical security is compromised, data theft can be minimized or prevented due to heightened protections on storage drives.

Why This Is a Potential Risk

Without enabling BitLocker on the C Drive, when the physical security of an asset is compromised, threat actors can access all data and files stored on the system. Many system credentials are stored on the system drive; not encrypting the C Drive leaves these credentials exposed.

Additionally, without BitLocker encryption, an attacker can boot into a device using external media. Alternatively, if an attacker gains access to your hypervisor, it allows them to mount the drive into the hypervisor, bypassing security and allowing them to tamper with security and configuration settings.

How to Resolve This Issue

Enable BitLocker to prevent the compromise of the system drive by encrypting all data on the drive. BitLocker is enabled in Settings ➔ Privacy & Security ➔ Device Encryption or Control Panel ➔ BitLocker Drive Encryption. Use TPM (if available) and a PIN for extra security and remember to save your BitLocker Recovery Key.

Updating to the latest Windows Security Updates can assist in additional security.

Real World Example

Whether company assets are stolen or misplaced by an employee, lapses in physical security can compromise sensitive data and content if not properly secured. The encryption provided by BitLocker assists in securing these files in the case of malicious threats attempting to access sensitive information.

Security Issue:

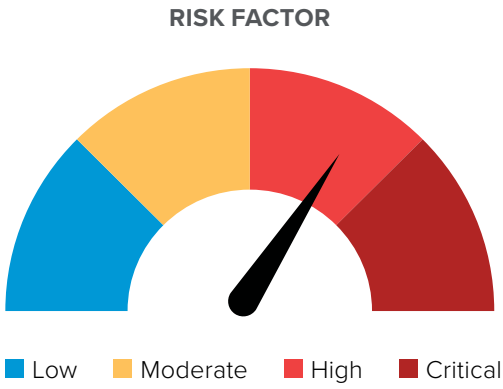
OPERATING SYSTEM PAST END OF SERVICING | High Risk

Related Frameworks

CIS_Controls | CMMC | Essential 8 | FedRAMP | FISMA | GDPR | HIPAA | ISO_IEC_27001 | NIST 800-171 | NIST 800-53 | NIST_CSF | PCI_DSS | SOC2

87%

485 out of 558 endpoints, didn't pass this analysis. Compared to your last report, this is up 14%.



What This Means for Your Environment

Running an operating system past its end of servicing is a critical failure point in cybersecurity and compliance. Updating an operating system to a supported build will provide the system with key vulnerability security patches that may not otherwise be available or provided on older versions of the OS.

Why This Is a Potential Risk

Unsupported platforms are at risk because they do not receive security patches, making them prime targets for threat actors who exploit outdated systems to deploy malware and ransomware. Older systems lack modern defenses, which allow attackers to deliver threats more easily.

How to Resolve This Issue

Upgrading systems to a supported operating system version is ideal for preventing misconfiguration and securing systems from attacks on vulnerabilities attached to legacy systems. Refer to the operating system documentation for information regarding versions still receiving vendor support.

Consider implementing OS Patching software to ensure systems are updated with the latest security updates. OS Patching can assist administrators in keeping key system processes fully updated and monitoring new operating system updates securely and simply. With Microsoft announcing the end of support for Windows 10 in October 2025, ThreatLocker® users with Patch Management enabled can upgrade to Windows 11 through the DAC interface in the ThreatLocker Health Center module.

Updating to the latest Windows Security Updates can assist in additional security.

Real World Example

The 2017 WannaCry ransomware attack targeted and exploited a known vulnerability in outdated Windows systems. Users who had not updated their operating systems were missing a crucial security patch that could have prevented the infection. The vulnerability, known as "EternalBlue" (Microsoft Security Bulletin MS17-010), was disclosed before the attack spread; however, many affected machines had not installed the latest updates. Enterprise systems that remained on Windows 7 and had not upgraded to a newer operating system were particularly vulnerable to the ransomware attack.

Security Issue:

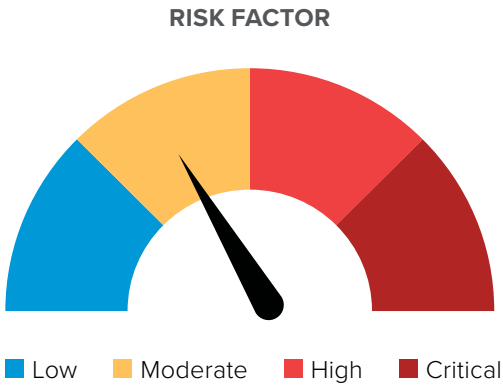
SECURE BOOT ENABLED | Moderate

Related Frameworks

CIS_Controls | CMMC | Essential 8 | FedRAMP | FISMA | GDPR | HIPAA | ISO_IEC_27001 | NIST 800-171 | NIST 800-53 | NIST_CSF | PCI_DSS | SOC2

63%

352 out of 558 endpoints, didn't pass this analysis. Compared to your last report, this is down 12%.



What This Means for Your Environment

With Secure Boot enabled, your system firmware enforces a security policy that only allows trusted, signed code to run during the boot process. This provides protection against malware and unauthorized operating system manipulation and enhances system integrity at the boot chain.

Why This Is a Potential Risk

Without Secure Boot, the risk for malicious code exposure increases before the OS loads. Attackers manipulate boot components to deploy Bootkits or Rootkits that remain undetected while operating with elevated privileges. Boot chain attacks can also compromise disk encryption controls, making them ineffective.

How to Resolve This Issue

Manufacturers typically enable Secure Boot by default on Windows machines. However, you can enable Secure Boot when starting an endpoint by inputting the correct key (typically Delete, F2, F10, F12, or ESC) to open the BIOS menu. You can also enter the UEFI by navigating to Settings, ➔ Update & Security ➔ Recovery, then clicking "Restart Now" under Advanced startup.

From there, navigate to your system's "Boot" or "Security" settings. The name of this setting may vary between vendors. Look for a setting for "Secure Boot" and set it to "Enabled."

Real World Example

The LoJax rootkit is a notorious example of a malicious bootloader. It begins as a Trojan, delivering payloads to a system and then escalating privileges to the kernel or system level. Once it gains privileged access to the endpoint, it checks for Secure Boot and boot chain protections.

If these protections do not exist, the rootkit injects code directly into the system's flash memory, where the system firmware is stored. At this stage, the infection will load before the operating system bootloader and persistently reinstall additional malware payloads each time the system boots. Furthermore, the malware remains even if you format the hard drive, replace the operating system, or wipe the partitions, threats attempting to access sensitive information.