SECURING EMPLOYEE DEVICES DURING REMOTE WORK

Remote work has rapidly become the new default for most organizations, and early studies indicate that for many, the changes will be permanent. However, the rush to support remote workers creates new challenges with profound impacts on organizational security models. Users are no longer protected by the many layers of security found on-premise in the corporate network. Organizations must adapt security policies to support a massive influx of inbound connections. Security teams must consider how to adapt core security concepts like Zero Trust to include remote work environments that include corporate laptops, BYOD devices, and home networking gear.

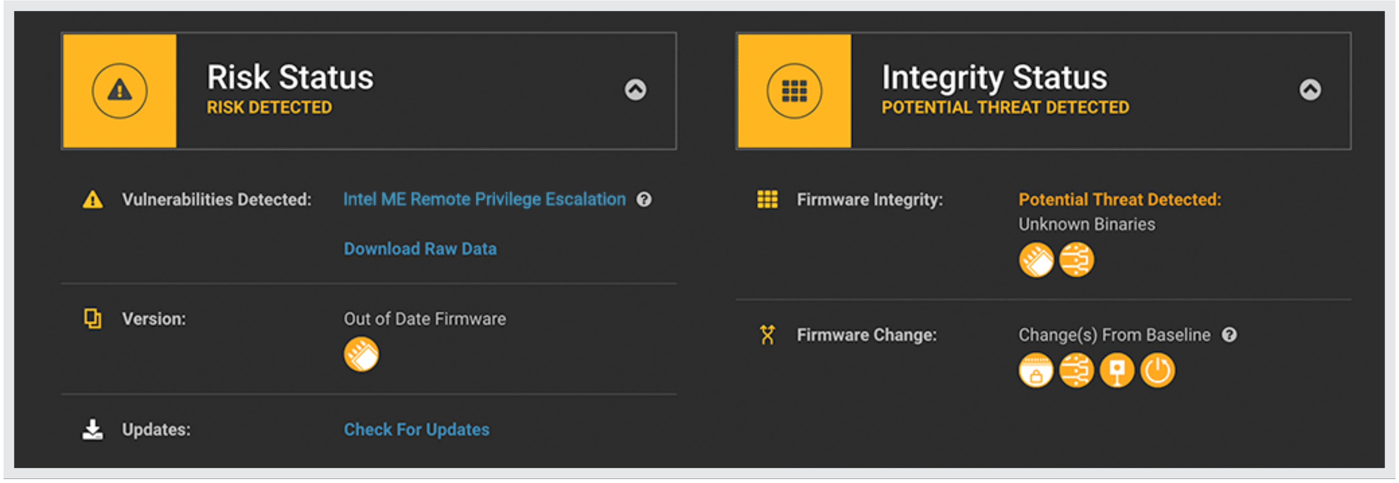
Eclypsium® helps organizations manage this all-important change. The Eclypsium platform provides security teams with complete visibility into the security and integrity of remote devices, protecting you from threats that are invisible to traditional endpoint security such as antivirus and EDR software. Eclypsium ensures the integrity and health of the devices that remotely access corporate resources over VPN and other secure remote access mechanisms.

> Eclypsium lets you assess the risk and trust level of any device and alert for any breaches or changes in device integrity that could impact the security of a remote access.

As remote work becomes the default, attackers are setting their sights on end user devices and the ways that users connect back to the enterprise. For example, a recent alert from the DHS CISA and the FBI reported that the most commonly exploited vulnerabilities in 2020 were affecting VPN appliances. Malicious actors such as APT41 have consistently targeted both remote end user devices and VPN and other network infrastructure devices with persistent backdoors, while a number of botnets have been compromising home office networking gear.

THE ECLYPSIUM SOLUTION FOR REMOTE WORKERS

The Eclypsium cloud-based device security solution gives teams full visibility into remote devices to ensure they are in a secure state and have not been compromised. When problems are found, Eclypsium can remotely patch or update devices to get them back into a safe state. The solution likewise extends this protection to networking and VPN infrastructure to secure the inbound connections that remote workers rely on in order to be productive.



Risk Status
RISK DETECTED

Vulnerabilities Detected: Intel ME Remote Privilege Escalation
Download Raw Data

Version: Out of Date Firmware

Updates: Check For Updates

Integrity Status
POTENTIAL THREAT DETECTED

Firmware Integrity: Potential Threat Detected:
Unknown Binaries

Firmware Change: Change(s) From Baseline

Audit Device Health and Patch Level—Check corporate and BYOD devices used remotely for vulnerabilities and misconfigurations that can put the device at risk. For example, ensure that all devices including BYOD devices are configured to use Secure Boot.

Cloud-Based Remote Updates and Patching—Keep devices in a secure state by remotely patching or updating out-of-date or vulnerable device firmware.

Verify Device Integrity—Ensure devices have not been tampered with or compromised and are free from implants and backdoors. Receive automated alerts to changes in any integrity changes.

Verify Inbound VPN Connections—Integrate Eclypsium with VPNs such as Cisco AnyConnect, and verify device integrity before allowing remote access into the enterprise.

Protect VPN Infrastructure—Ensure remote access network gear including VPN appliances are up to date and free from backdoors and implants.

Verify New Devices—Directly ship new devices to remote workers, while validating that new devices are safe and were not compromised in the supply chain. Allow workers to use BYOD or personal devices, while ensuring they meet organizational security requirements.

Ready to close your device security gap? Eclypsium can help. **Contact us**.