KENNA Security

eclypsium®

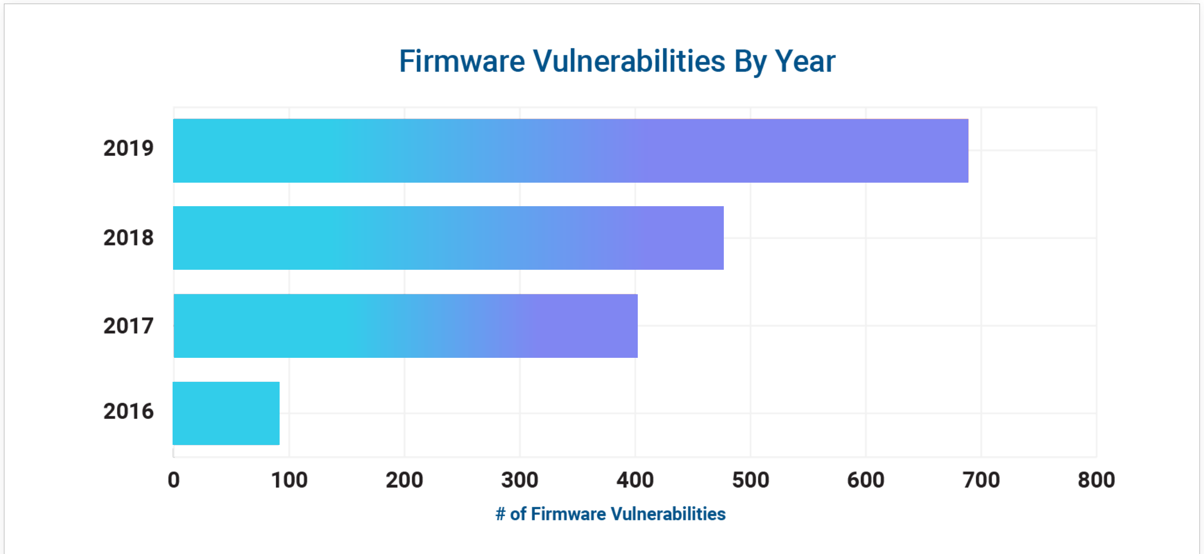
SOLUTION BRIEF

Extending Risk-Based Vulnerability Management to Firmware With Eclypsium® and Kenna.VM

New Challenges Require New Solutions

Modern IT and Security teams are facing a cybersecurity landscape that is both expansive and sophisticated. In recent years, the rate of discovery of new vulnerabilities has more than doubled, making it virtually impossible for the majority of organizations to address all or even most of the vulnerabilities in their environment. On the other hand, attackers have become increasingly sophisticated by finding new ways to evade security tools, persist within compromised devices, and cause the greatest damage possible.

Unfortunately these two trends have converged at the spot where enterprise security is typically the weakest—the firmware and hardware layer of devices. 2019 was the busiest year on record for new firmware vulnerabilities and had over 7.5 times more CVEs than were seen just three years ago. Attackers have increasingly turned their sights on this often unguarded attack surface. Malware and ransomware have increasingly targeted vulnerabilities in firmware as a way to subvert security and cause debilitating damage to infected devices. Threat actor groups such as APT28, APT29, and APT41 have all targeted firmware in devices including laptops, servers, and networking gear.



Source: National Vulnerability Database December 31, 2019

Yet, many organizations lack insight into their firmware and hardware attack surface. Identifying and remediating vulnerabilities is often a highly manual and technical process that is only performed by exception, leading to longer dwell times when attacks do occur. The integration of the Eclypsium and Kenna solutions changes that.

Eclypsium gives organizations visibility and control over their firmware and hardware risk. Eclypsium scans devices at the levels that traditional vulnerability scanners and security tools miss to reveal device level vulnerabilities, misconfigurations, and threats. This includes visibility into the fundamental system UEFI/BIOS firmware that, if compromised, gives an attacker virtually complete control over a device including the ability to subvert the operating system and other security protections. The solution extends this same visibility to the many firmware and hardware components within a device such as network adapters, processors, hard drives, and more which can likewise provide attackers with the ability to hide, steal data, or cause damage.

> **By integrating with Kenna.VM, the combined solution ensures that organizations can seamlessly incorporate firmware security into the existing risk-based vulnerability management process.**

IT and security teams can now see a complete view of a device's risk, so that they can make smarter patching decisions based on all available information. For the first time, organizations can see a complete view of risk that spans the hardware, firmware, OS, and application layers of a device. The Kenna.VM dashboard brings all this information into a concise, actionable view that ensures that customers get the greatest security benefit from their time and effort.

The Eclypsium Solution

Eclypsium extends security to the fundamental layers of a device's firmware and hardware that are not covered by traditional security and vulnerability scanning tools. The solution automates the previously laborious and technical work of auditing device firmware and hardware configurations, and finding firmware threats such as implants, rootkits, and bootkits. When problems are found, Eclypsium helps customers manage their firmware updates to mitigate the key risks to the organization.

Key Eclypsium capabilities include:

- **Detection of Outdated and Vulnerable Firmware** - Vulnerabilities in firmware can allow attackers to take full control over a device and its operating system, while hiding from traditional security controls. Eclypsium's low-level scanning reveals vulnerabilities that are invisible to traditional vulnerability scanners.
- **Find Device Misconfigurations and Missing Protections** - Eclypsium audits the myriad detailed device settings needed to ensure a strong security posture such as Secure Boot settings, component settings, and more.
- **Verify Firmware Integrity and Detect Threats** - Eclypsium ensures that devices have not been tampered with or compromised by attackers or malware. The solution reveals both known and unknown threats including backdoors, implants, malicious bootloaders, rootkits and more.
- **Broad Coverage of an Organizations' Most Critical Devices** - Eclypsium protects a wide range of devices including laptops, servers, and networking infrastructure as well as the industry's most popular operating systems such as Windows, Linux, MacOS, and more.
- **Visibility Into Device Components** - In addition to auditing the system UEFI/BIOS firmware, Eclypsium analyzes and inspects all of the other major firmware components on a device; such as drives, processors, memory, drives, network adapters, and much more.

The Kenna Solution

Kenna.VM is a scalable, cloud-based solution that delivers the most informed and accurate risk prioritization available, enabling security and IT operations teams to take a risk-based approach to vulnerability management by prioritizing and proactively managing the vulnerabilities that matter most. The solution combines your organization's internal security data with contextual data from 15+ threat and exploit intelligence feeds and 7+ billion managed vulnerabilities to accurately track and measure real-world exploit activity across the enterprise's global attack surface.

Key Kenna.VM capabilities include:

- **Risk-based prioritization** - Provides risk prioritization that allows enterprises to focus on the 5% of the vulnerabilities that matter most.
- **Threat and Exploit Context** - Enriches vulnerability data with context information from 15+ threat and exploit intelligence feeds and extensive vulnerability volume and velocity data.
- **Full visibility** - Centralizes your risk management and determine risk and prioritize remediation efforts across a multi-vendor environment.
- **Evidence-based guidance** - Eliminates the guesswork and the friction between Security and IT about what to patch by providing authoritative risk prioritization and contextual data.
- **Predictive modeling technology** - Accurately forecasts the future risk of vulnerabilities the instant they're discovered, allowing organizations to proactively manage risk.

Combining the Power of Kenna and Eclypsium

With the integration of the Eclypsium and Kenna solutions, Security and IT teams are able to add a completely new perspective to the industry's leading risk-based vulnerability management solution.

> **Historically, organizations were limited to seeing vulnerabilities and risk at the level of software. Network-based vulnerability scans can discover vulnerabilities at the operating system or service level, but lack insights into the underlying device itself.**

Likewise, application security scans give visibility into the applications, but can not see details of the infrastructure those applications depend on.

The integration between Eclypsium and Kenna.VM provides customers with a consolidated, comprehensive view of vulnerability risk. With Eclypsium's ability to discover device and network infrastructure vulnerabilities and Kenna data science-based approach to prioritizing risk, IT and Security professionals now have a more comprehensive view on what they need to do to prioritize their remediation efforts and improve their risk posture.

Key Features:

- ✓ **View Risks From Firmware Vulnerabilities in Kenna.VM** - Manage firmware vulnerabilities, with rich threat context data from both Kenna and Eclypsium.
- ✓ **Risk Prioritization** - Leverage data science-based risk prioritization.
- ✓ **Consolidated Management of Risk** - Prioritize and manage firmware vulnerabilities in combination with infrastructure vulnerabilities.

Key Benefits:

- ✓ **A Total View of Risk** - With Eclypsium and Kenna, organizations are now able to see a complete, consolidated picture of a device's risk. For the first time, IT and Security teams can view any enterprise asset in the context of its hardware, firmware, and software for a more complete view of its security posture.
- ✓ **Maximize Staff Time and Effort** - Facing increasing volumes of vulnerabilities and limited resources, organizations need to make informed patching and risk mitigation decisions. With Eclypsium and Kenna.VM, IT teams don't need to patch arbitrarily, hoping that their efforts are improving the organization's risk posture. With evidence-based guidance on what to fix, how to fix it, and why, IT teams can focus their time on the vulnerabilities that pose the biggest risk to the organization.
- ✓ **Visibility Into Network Devices and Infrastructure** - In addition to seeing new perspectives on devices, organizations can also get visibility into networking devices that are often missed by traditional scanners. With visibility into switches, routers, VPN infrastructure and more, staff can ensure that vulnerabilities in networking gear don't leave the organization exposed to attacks.

How the Solution Works:

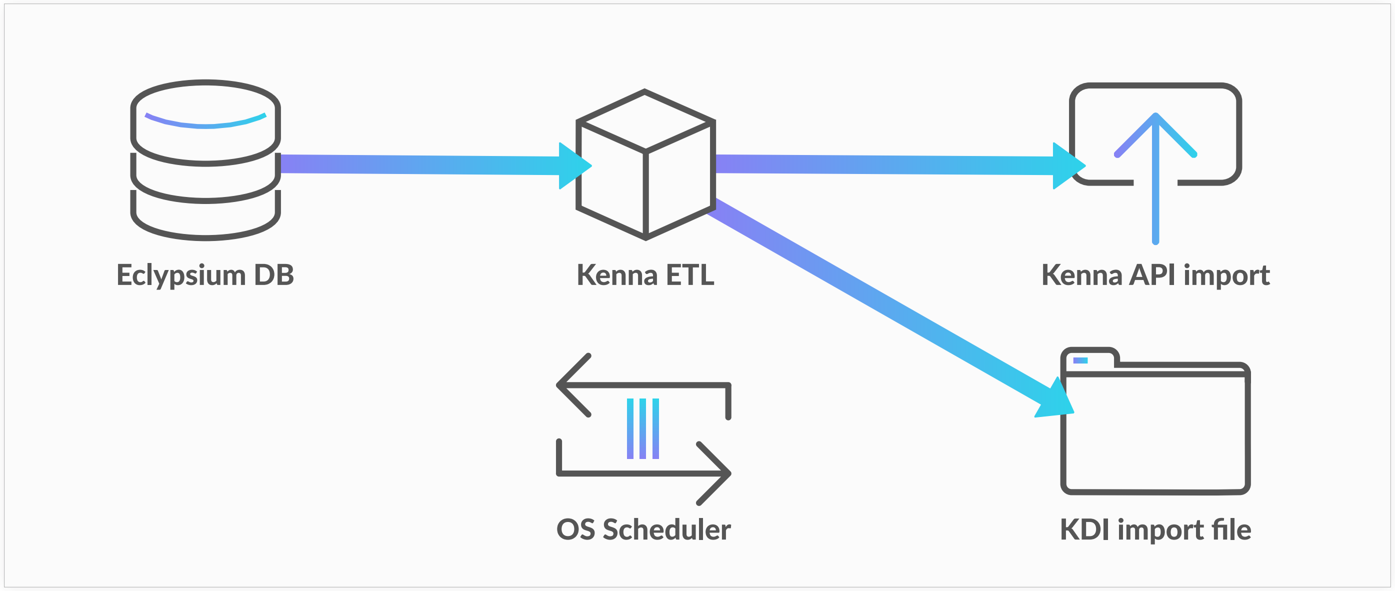
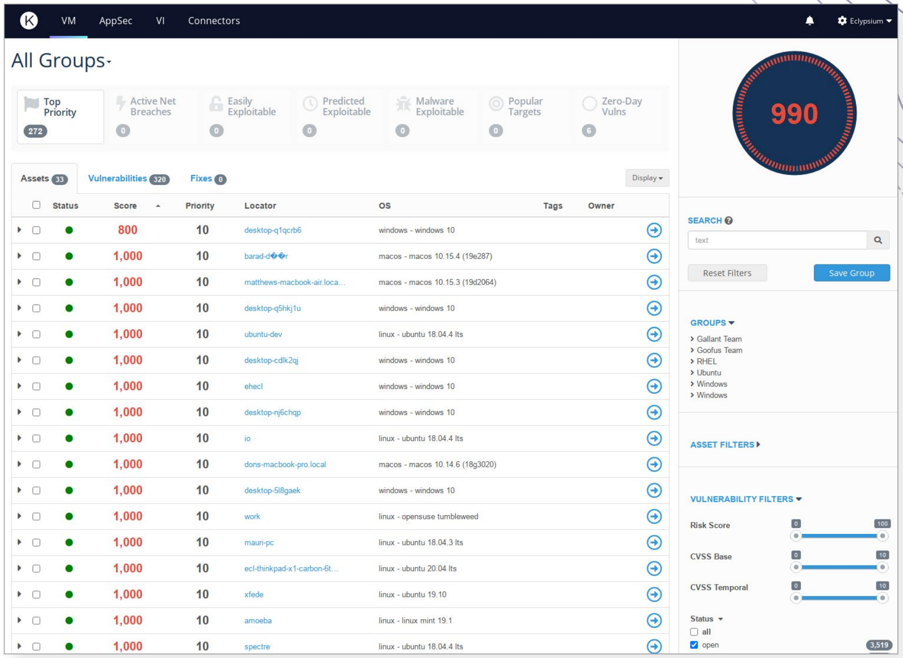


Figure 1. Kenna Security integration architecture

The Eclypsium-Kenna integration consists of an ETL (Extract-Transform-Load) process that, when executed, extracts summary information about all the hosts and the security tests from the Eclypsium scan database and transforms it into the JSON format compliant with the Kenna Data Importer. The Eclypsium scan data is imported automatically to Kenna via Kenna API or via the Kenna data file upload from a password protected page. The ETL process can be started directly on the system or scheduled via an OS scheduler like cron.

The scan results are visible in the Kenna Dashboard under “Explore” along with Kenna risk prioritization and threat context in a view similar to the one shown in Figure 2.



All Groups

Top Priority	Active Net Breaches	Easily Exploitable	Predicted Exploitable	Malware Exploitable	Popular Targets	Zero-Day Vulns
272	0	0	0	0	0	6

Assets 33 | Vulnerabilities 320 | Fixes 0

□	Status	Score	Priority	Locator	OS	Tags	Owner
□	●	800	10	desktop-q1qcrb6	windows - windows 10		
□	●	1,000	10	barad-d��r	macos - macos 10.15.4 (19e287)		
□	●	1,000	10	matthews-macbook-air.loca…	macos - macos 10.15.3 (19d2064)		
□	●	1,000	10	desktop-q5hkj1u	windows - windows 10		
□	●	1,000	10	ubuntu-dev	linux - ubuntu 18.04.4 lts		
□	●	1,000	10	desktop-cdlk2qj	windows - windows 10		
□	●	1,000	10	ehecl	windows - windows 10		
□	●	1,000	10	desktop-nj6chqp	windows - windows 10		
□	●	1,000	10	io	linux - ubuntu 18.04.4 lts		
□	●	1,000	10	dons-macbook-pro.local	macos - macos 10.14.6 (18g3020)		
□	●	1,000	10	desktop-5l8gaek	windows - windows 10		
□	●	1,000	10	work	linux - opensuse tumbleweed		
□	●	1,000	10	mauri-pc	linux - ubuntu 18.04.3 lts		
□	●	1,000	10	ecl-thinkpad-x1-carbon-6t…	linux - ubuntu 20.04 lts		
□	●	1,000	10	xfede	linux - ubuntu 19.10		
□	●	1,000	10	amoeba	linux - linux mint 19.1		
□	●	1,000	10	spectre	linux - ubuntu 18.04.4 lts		

GROUPS
- Gallant Team
- Goofus Team
- RHEL
- Ubuntu
- Windows
- Windows

ASSET FILTERS

VULNERABILITY FILTERS

Risk Score	0	100
CVSS Base	0	10
CVSS Temporal	0	10

Status
- □ all
- ☑ open 3,519

Figure 2. Kenna Dashboard with results from the Eclypsium solution

KENNA Security

eclypsium®

To learn more about aligning your organization around risk, visit **www.kennasecurity.com.** To protect your devices from threats down to the firmware level, visit **www.eclypsium.com.**