How Cisco Vulnerability Management Works

A Peek "Under the Hood" of Risk-Based Vulnerability Management

When the first vulnerability scanner appeared on the market, organizations were provided with tangible evidence of security holes in their networks. Since then, many vendors followed suit, and soon organizations would have access to data on weaknesses or flaws within their infrastructure, applications, and eventually, connected devices. It's immensely valuable data, but complications arose as the volume of the data spiraled out of control. Suddenly, an organization might have thousands of vulnerabilities but not nearly enough resources to patch every single one. The question becomes, "How can I possibly patch everything?"

The reality is that you can't patch everything. Most organizations simply do not have the manpower or time to patch every vulnerability identified by their scanner. And even if they had the time, trying to patch everything wouldn't be an efficient use of that time. Why not? Because every vulnerability doesn't result in a breach.

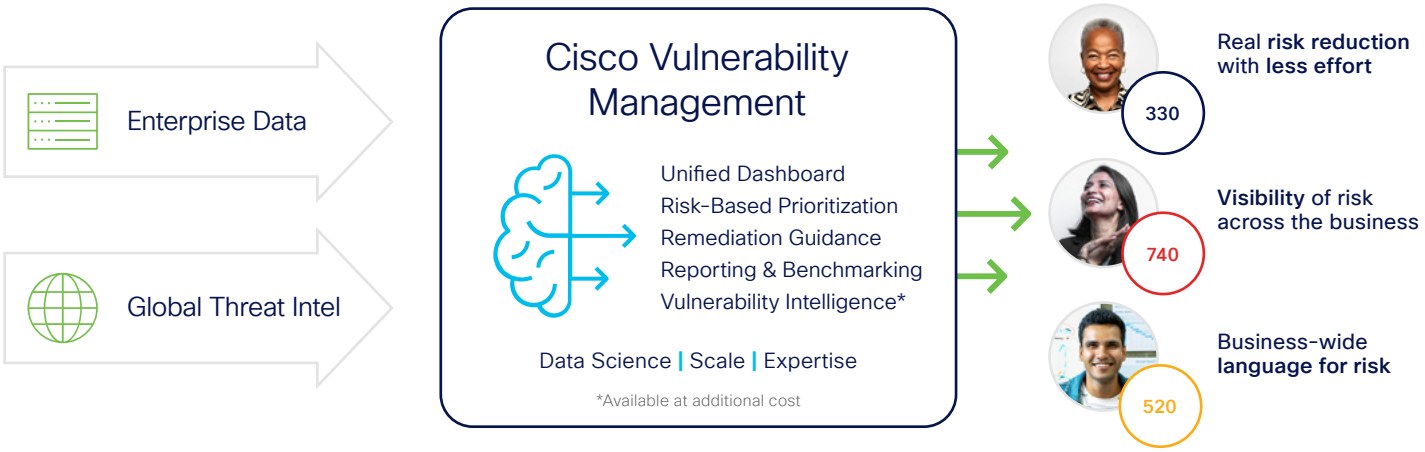
Cisco Vulnerability Management (formerly Kenna.VM) was founded to address this exact problem—to extract the signal from the noise of security data and identify the vulnerabilities that pose real risk to an organization so that it can focus their limited resources. Most security companies create new security data, but Cisco Vulnerability Management helps you make sense of that deluge of data.

Which Vulnerabilities Really Matter?

- 2%–5% of published vulnerabilities have observed exploits in the wild
- 23% of published vulnerabilities have associated exploit code
- The chance of a vulnerability being exploited in the wild is 7 times higher when exploit code exists
- 50% half of exploits are released within two weeks of the CVE publication date

Kenna Security (now Cisco) and the Cyentia Institute, Prioritization to Prediction – Volume 1: Analyzing Vulnerability Remediation Strategies

Kenna Security (now Cisco) and the Cyentia Institute, Prioritization to Prediction – Volume 3: Winning the Remediation Race



The Right Data Provides the Right Context

The best place to start this conversation is the data that Cisco Vulnerability Management uses to help organizations prioritize their vulnerability remediation efforts. There are two datasets that provide the framework for decision making: 1) enterprise data from every available source across the customer's infrastructure, applications, and the Internet of Things (IoT), and 2) global threat intelligence, which includes custom-curated exploit and threat intelligence feeds. This data is analyzed by proven data science algorithms to deliver an accurate, granular, and quantifiable risk score for every vulnerability within seconds.

To understand what attackers are doing in real time and evaluate which vulnerabilities are likely to pose a threat to the organization's specific environment, Cisco Vulnerability Management analyzes the following internal and external data sources:

<table>
<tr><th colspan="2">Ground Truth Telemetry</th><th>Internal Security Data Sources</th></tr>
<tr><td colspan="2">19+ exploit and threat intelligence feeds
15+ billion security events
12.7+ billion managed vulnerabilities</td><td rowspan="2">· Any vulnerability scanner
· Asset- and network-specific data from configuration management database (CMDB) tools
· Penetration testing
· Bug bounty programs
· Static application testing
· Dynamic application testing
· Open source tools
· Custom data sources in JSON format</td></tr>
<tr><th>Exploit Intelligence:</th><th>Threat Intelligence:</th></tr>
<tr><td>· Metasploit
· Exploit DB
· ReversingLabs
· Proofpoint
· Secureworks CTU
· D2 Elliot
· Contagio
· Black Hat Kits on rotation (AlphaPack, Blackhole, Phoenix, more)
· Canvas Exploitation Framework
· CISA Known Exploited Vulnerabilities
· Github Exploit Feed: Cyentia Institute</td><td>· AlienVault OTX
· AlienVault Reputation
· Secureworks CTU
· Emerging Threats
· ReversingLabs
· Sans Internet Storm Centre
· X-Force Exchange
· Cisco Talos
· Silobreaker</td></tr>
</table>

Cisco Vulnerability Management uses all of this data to get a full view into the potential impact of each vulnerability, as well as how critical each threat could be given your specific environment, and then translates that context into actionable security intelligence to guide remediation efforts and resource allocation.

Volume and Velocity

- Processes and analyzes threat and exploit data from more than 19 intelligence feeds to determine the volume and velocity with which attackers are exploiting vulnerabilities in the wild.

Easily Exploitable

- Analyzes data from exploit toolkits in the commercial space and dark web to determine which ones have weaponized capabilities.

Malware Exploitability

- Determines which malware strains exploit vulnerabilities and determine the prevalence of that malware.

Zero Day

- Analyzes all available zero-day information and determine whether a customer is susceptible.

Using Data Science to Understand Risk

Again, not every vulnerability will result in a breach. The wide range of internal and external data can help us to understand which vulnerabilities are most likely to result in a breach—that is, which vulnerabilities pose a real risk. Cisco Vulnerability Management uses proven data science techniques, including machine learning, natural language processing, and predictive modeling to assess, prioritize, and even predict risk. These approaches allow us to dynamically calculate the risk of every vulnerability to enable security and IT teams to embrace risk-based vulnerability management.

Using predictive modeling, Cisco Vulnerability Management can calculate the risk of a vulnerability as soon as it is revealed. Advanced predictive modeling forecasts the weaponization of new vulnerabilities with a confirmed 94 percent accuracy rate, and then prioritizes remediation based on the risk of exploitation. This gives your organization the foresight needed to remediate high-risk vulnerabilities before attackers can mount an attack.

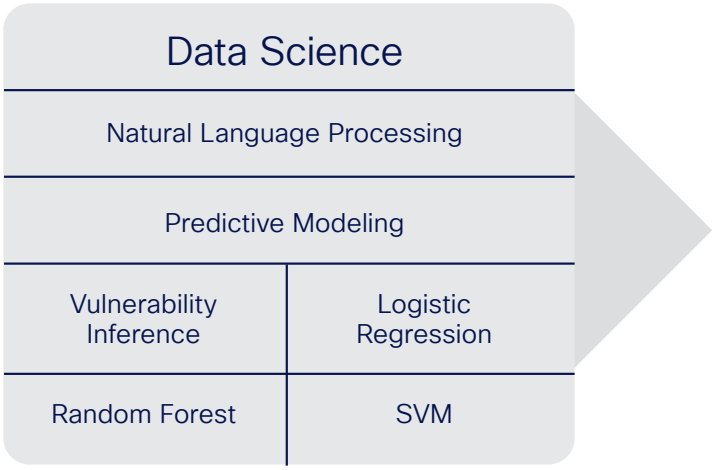
Natural language processing—a branch of artificial intelligence aimed at making sense of "natural" human language—investigates social media sites, the dark web, and other places where vulnerabilities are discussed, and extracts the language associated with vulnerabilities to assist in risk assessment. Natural language processing is also used to help score vulnerabilities that do not have a Common Vulnerability Scoring System (CVSS) score by analyzing various text keywords and phrases that are shown to be high indicators of risk.

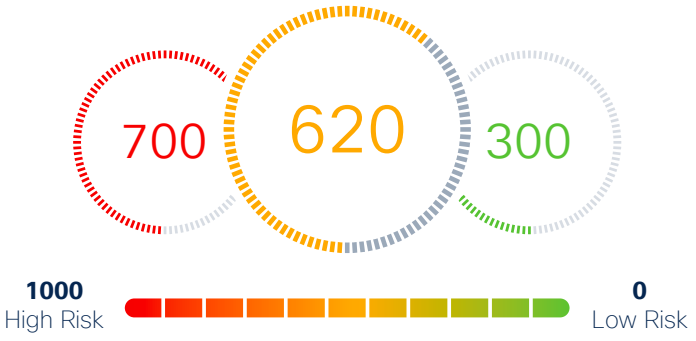
Cisco Vulnerability Management then analyzes the data using a number of predictive technologies, including support-vector machines (SVM), random forest, logistic regression, and vulnerability inference. The data from the predictive models is then used by the Risk Scoring Engine to produce an actionable risk score for every vulnerability.

Actionable Risk Scoring

Leveraging ground truth telemetry and an extensive amount of internal security data, the Kenna Risk Scoring Engine ties into Cisco Vulnerability Management's predictive model to algorithmically determine risk scores for each unique vulnerability and in concert with asset criticality scores, determines an actionable risk score for each asset and group of assets that ranges from zero (no risk) to 1000 (highest risk).

The risk score takes into account all of the internal and external variables used in the predictive model that are high indicators of risk. Internal risk calculations factor in the number of instances of each vulnerability in your environment, their potential severity, and the criticality of the assets that are threatened as a result of each vulnerability. External risk calculations factor in the CVSS score of the vulnerability, threat intelligence information such as whether or not an exploit kit is available for the vulnerability, the volume and velocity of exploits that take advantage of the vulnerability, and the prevalence of the vulnerability seen throughout customer environments. With accurate and quantifiable risk scores, you will understand your organizations' current risk posture and identify the actions you can take to reduce the greatest amount of risk.

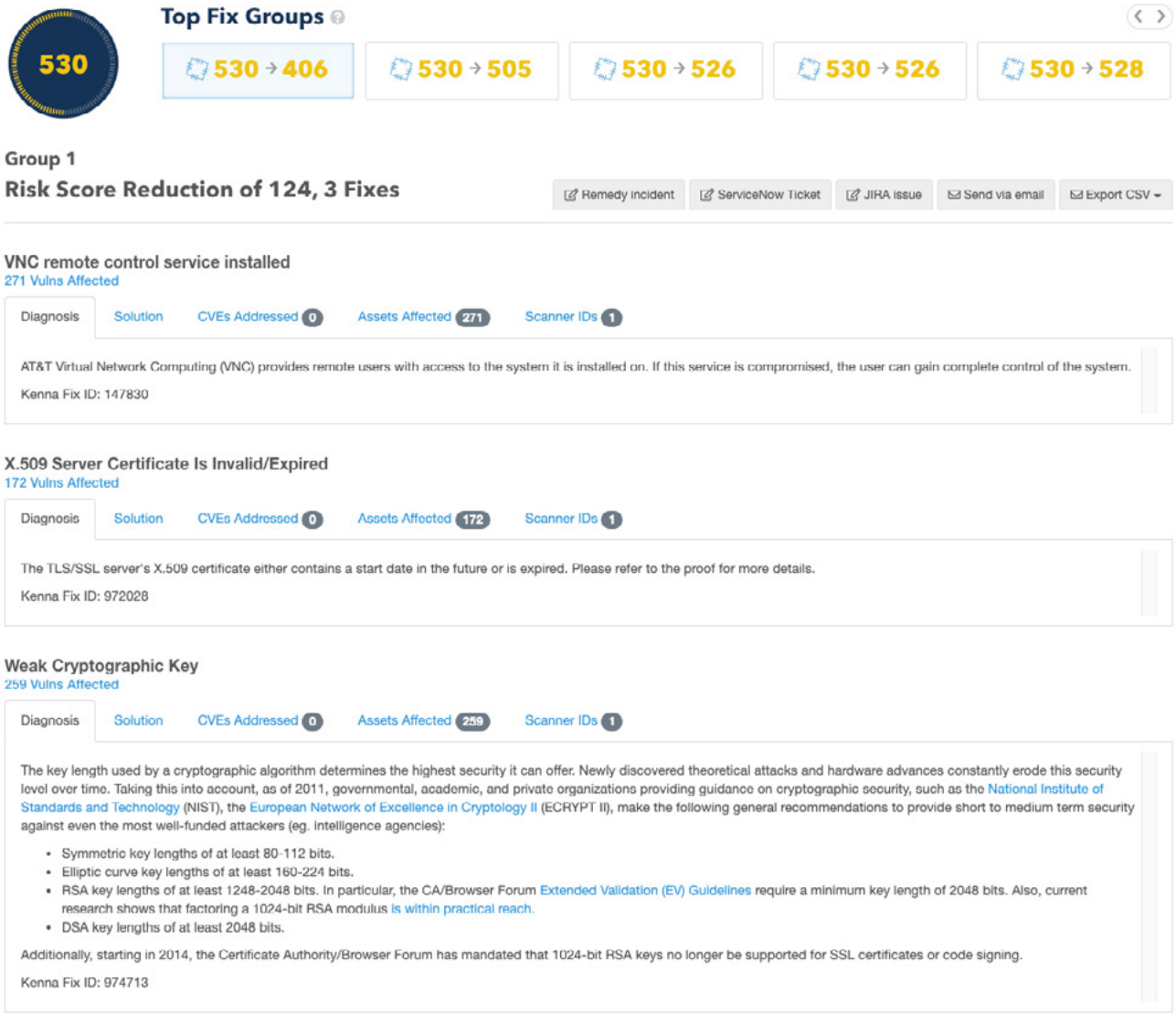




Remediation Intelligence to Guide the Reduction of Risk

The Cisco Vulnerability Management Remediation Intelligence Engine prioritizes the vulnerabilities that, if remediated, will have the greatest impact on risk score reduction. The Remediation Intelligence Engine clearly identifies which vulnerabilities should be remediated first and articulates the specific impact each action will have on your organization's risk posture using a mechanism called "Top Fix Groups". Top Fix Groups are ranked collections of fixes that, when implemented, make the highest impact on reducing the organization's risk posture with the least amount of effort. Top Fix Groups can be used with a ticketing system as part of an optimal workflow process that optimizes vulnerability risk reduction for the organization.

Thanks to Cisco Vulnerability Management's integration with popular ticketing systems like Remedy, Jira, ServiceNow, and Cherwell, Security and IT teams have the same level of actionable intelligence, and IT knows what to fix, how to fix it, and why the fix is a priority. The ticketing system integrations are bi-directional in nature, and automated tracking keeps security teams informed and synchronized regarding the progress against all tickets. This tight coupling with ticketing systems saves the IT teams valuable time by promoting close collaboration with security teams, with the common mission of optimizing the organization's risk reduction–as quickly and efficiently as possible.



The Bottom Line

When the rubber meets the road, Cisco Vulnerability Management's approach not only helps reduce and manage risk, but it does so while saving money, resources, and time. Vulnerability management is a notoriously resource-heavy and friction-filled task. Security teams face a tidal wave of data on known vulnerabilities, while IT teams are being crushed by the demand to patch everything. Cisco Vulnerability Management shifts away from this unproductive and taxing status quo to embrace a risk-based approach to vulnerability management that is more appropriate for modern organizations. This approach helps organizations focus on the vulnerabilities that matter, remediate faster, and align the entire business around a common objective. Ultimately, Cisco Vulnerability Management allows you to do more with less.

To learn more about Cisco Vulnerability Management, visit

https://www.cisco.com/go/vulnerability-management

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands