

# CA Vulnerability Manager r8.3

CA VULNERABILITY MANAGER PROTECTS ENTERPRISE SYSTEMS AND BUSINESS OPERATIONS BY IDENTIFYING VULNERABILITIES, LINKING THEM TO CRITICAL BUSINESS ASSETS AND PROVIDING STEPS FOR REMEDIATION.

## Overview

Today's enterprise security organization needs to mitigate the risk that threatens critical business operations. CA Vulnerability Manager enables you to identify vulnerabilities, link them to the business assets they affect and remedy them.

## Benefits

CA Vulnerability Manager enables you to simplify and streamline the complex process of risk mitigation, work with up-to-date vulnerability information, control costs and meet compliance obligations. By managing and mitigating risk, you protect critical business systems and help ensure ongoing business operations.

## CA Advantage

The distinctive, asset-based vulnerability management approach employed by CA Vulnerability Manager addresses every aspect of system vulnerabilities with a single tool. As the vulnerability management component in the CA Security Information Management solution, CA Vulnerability Manager contributes to the larger CA vision of Enterprise IT Management (EITM). Its goal: to simplify and unify IT management across the enterprise.

---

## CA Vulnerability Manager Uses Asset-Based Vulnerability Assessment to Secure Your Enterprise

Vast — and increasing — numbers of vulnerabilities in your software open the door to malicious attacks that can disrupt critical business systems. To prevent such disruptions means finding and fixing vulnerabilities before someone exploits them.

To achieve this herculean feat requires knowledge:

- **Know Your Assets** Identify the technologies running on them and how critical those assets are to business continuity
- **Know Your Vulnerabilities** Identify, research and validate vulnerabilities and determine their relationship to business-critical assets
- **Know Your Organization's Security Risk Posture** Identify those assets that must be protected immediately
- **Know the Remedy** Establish the best practice for protecting your systems from a given vulnerability
- **Know Whether the Vulnerability Has, in Fact, Been Fixed** Determine if the remediation was implemented, if it worked, and preserve this information for compliance records

You can gain the knowledge you need with a single, comprehensive tool — CA Vulnerability Manager. Its unique, asset-based vulnerability assessment approach gives you visibility into every platform and application in your IT infrastructure. This visibility, along with key features, enables you to mitigate risk and helps ensure business continuity.

### Key Features

**ASSET-BASED VULNERABILITY ASSESSMENT** Using asset-based vulnerability assessment, you gain a comprehensive picture of your assets, new and existing. You can find new assets with Asset Discovery, by non-intrusively scanning within a specified IP range and gathering high-level information, such as the IP address, host name and operating system. The discovery process can be run on an ad-hoc or scheduled basis.

Asset Inventory enables you to perform either a scheduled or an on-demand inventory, identifying the technologies running on your asset down to a patch level. You can then group the assets, classify their risk level and assign administrative privileges.

**RISK-PRIORITIZED TASK MANAGEMENT** System administrators can prioritize tasks according to risk, helping to ensure that the most critical vulnerabilities are handled first. They can determine how a known vulnerability will affect any given asset with vulnerability-to-asset correlation, which automatically compares your asset inventory data to a validated vulnerability database provided by CA.

Once vulnerability is established, remediation instructions define the correct action to take — apply a patch, change a configuration setting, implement a shielding tactic or apply a complex patch fix. The instructions also provide manual remediation instructions when automated patch delivery is not feasible. You can assign status and track manual remediation.

After remediation occurs for an asset, you can review the disposition status of the remedy with tracking methods provided by CA Vulnerability Manager. This includes administrative notes that detail remediation progress and verify completion of the work — essential for audit and compliance purposes.

**VALIDATED SECURITY INFORMATION** You can further secure your assets by leveraging the abilities of the CA Security Advisory team, a global network that researches, assembles and validates security risks through a patent-pending process that supports proactive risk management. This process reduces or eliminates false positives, enabling your administrators to focus on the real threats to your IT environment.

The content and code in the vulnerability database are updated automatically. As new vulnerabilities are downloaded, the data is correlated and the risk-prioritized task list is dynamically updated. The latest code enhancements are automatically applied during a user-defined maintenance window, creating hands-off software maintenance.

**REPORTING CAPABILITIES** Through a variety of reports, you gain a comprehensive understanding of your security posture and can measure risk.

- **Enterprise-Wide Reporting** reports risk exposure in real time and details progress toward mitigation
- **Top 10 Reports** lists the Top 10 assets most at risk according to their protection rating
- **On Demand Queries** you define the queries through an easy-to-use query wizard. Results can be exported to CSV-compatible tools.

**ADMINISTRATIVE MANAGEMENT CAPABILITIES** You simplify administering assets and managing their risks with CA Vulnerability Manager. You can group assets, which can be automatically defined based on parameters such as location, role in the network, or value to the enterprise. You can then assign a protection rating to each asset group, based on its importance to your business.

You can further protect assets with pre-defined user roles and permissions. Each user can be assigned to a specific asset group, giving them access only to those assets and task lists they manage.

Global updates enable you to make a single administrative change to multiple assets, such as changing an asset group designation or deleting a group of assets. System administrators can close tasks across multiple asset groups, creating efficiencies in the daily routine. You can also define a global status for a specific vulnerability across the enterprise.

### **The Bigger Security Picture**

The information gained by knowing your assets and vulnerabilities — and the relationships between them — is put to good use in more ways than one. You can view the data and reports generated by CA Vulnerability Manager — along with information from other security products, events and processes — through the CA Security Command Center (CA SCC). CA SCC also accepts event notifications and correlates them with security incidents discovered by other real-time devices. This comprehensive view of disparate security data enables you to take corrective action and run investigations through a single, centralized command and control center.

## How CA Vulnerability Manager Works

CA Vulnerability Manager facilitates risk mitigation by initially conducting a scheduled asset inventory where system data is collected. The data is then correlated with known vulnerabilities and compiled into a prioritized task list that defines your most critical vulnerabilities. Remediation instructions detail the appropriate corrective action and verification is provided to measure progress toward enterprise risk mitigation.

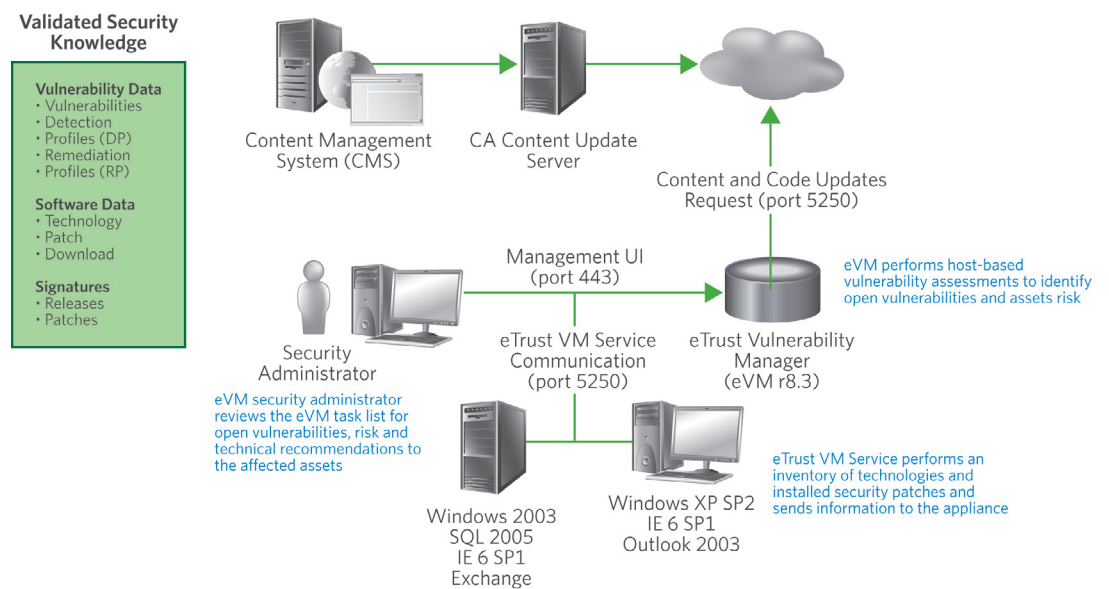
CA Vulnerability Manager displays information through a home page dashboard and user interface. It highlights the Top 10 high-risk assets, new vulnerabilities and a summary of your organization's overall security risk. A task list search feature enables you to drill down to more detailed information.

CA Vulnerability Manager supports Windows operating systems, embedded applications, UNIX and Linux.

FIGURE A

CA Vulnerability Manager correlates data from your software with known vulnerabilities.

## THE CA VULNERABILITY MANAGER PROCESS



---

## Vulnerability Mitigation Helps Ensure Business Operations

CA Vulnerability Manager enables you to: simplify and streamline the mitigation process, from data collection through reporting; work with up-to-date information when dealing with emerging and evolving vulnerabilities; control costs; and meet compliance requirements. Most importantly, you acquire the knowledge you need about system assets and vulnerabilities that enables you to mitigate risk and help ensure business operations.

### **Simplify and Streamline**

CA Vulnerability Manager enables you to simplify the complex and time-consuming processes required to mitigate risk. Automated asset discovery and inventory, correlation to vulnerabilities and prioritization of tasks help you streamline daily routines. Your security personnel can focus on other critical duties — a valuable commodity given the demands on today's IT organizations.

### **Up-to-Date Information**

Because vulnerabilities evolve and new threats constantly emerge, up-to-date information is critical to successful mitigation. Based on hourly or daily updates, IT is aware of new threats to enterprise operations and can take the correct action to remedy the situation.

### **Control Costs**

You can control costs by off-loading to the CA Security Advisory Team the task of researching and validating new vulnerabilities. Once those vulnerabilities are in your database, CA Vulnerability Manager automatically determines which machines are vulnerable and prioritizes fixes based on your business priorities.

### **Meet Compliance Requirements**

You can provide auditors solid documentation to help meet compliance and regulatory requirements with CA Vulnerability Manager tracking and reporting capabilities. You can prove that you know what your risks are and show that steps have been taken to mitigate them.

---

## CA Advantage

CA Vulnerability Manager enables you to manage vulnerabilities before they can be exploited. As an integral part of the CA Security Information Management (CA SIM) solution, CA Vulnerability Manager integrates easily with other security products, including CA SCC, moving you closer to comprehensive IT management across the enterprise.

CA Vulnerability Manager is an integral part of CA's Security Information Management solution, and an important part of EITM — CA's overall approach to transforming IT management. CA unifies and simplifies IT management across the enterprise for greater business results.

CA Technology Services™ and our partners can help you assess your current IT situation, define your goals and implement solutions to gain measurable results. To keep your CA solutions operating at peak performance, CA support delivers unparalleled technical and customer support worldwide, and we offer training and certification through CA Education.

---

## Next Steps

CA Vulnerability Manager, with its distinctive asset-based vulnerability assessment approach, simplifies the complex process of managing vulnerability and ensures the continuity of business operations while controlling costs and contributing to compliance efforts.

---

To learn more, and see how CA software solutions enable organizations to unify and simplify IT management for better business results, visit [ca.com/products](http://ca.com/products).