

CORE Insight for Vulnerability Management

Unify and Streamline Vulnerability Management with Enterprise Security Intelligence

CORE Insight™ is the first solution to truly unify and streamline network, endpoint and web vulnerability management initiatives enterprise-wide. An automated, end-to-end vulnerability management platform, Insight aggregates vulnerability data from every corner of your organization and adds predictive security intelligence to identify critical exposures and reveal business risks.

From web application weaknesses threatening backend network resources, to “low-level” endpoint malware exposures opening the door to advanced persistent threats, Insight reveals how actual attackers can traverse multiple vulnerabilities across layers of infrastructure to access your most valuable business assets.

Insight’s Automated Process for Continuous Vulnerability Management

1. Scan for Potential Vulnerabilities and Import Data

To begin a CORE Insight security assessment, you first import data on potential security exposures from your vulnerability scanners. Insight offers connectors for importing, validating and correlating results from any combination of network and web scanners, including:

Network Vulnerability Scanners:

- eEye Retina® Network Security Scanner
- McAfee® Vulnerability Manager
- GFI LANguard™
- nCircle IP360™
- IBM Internet Scanner®
- Qualys QualysGuard®
- Lumension® Scan
- SAINTscanner®
- Tenable Nessus®

Web Application Vulnerability Scanners:

- Cenzic Hailstorm™
- NTO Spider™
- HP WebInspect®
- WhiteHat Sentinel
- IBM AppScan®

2. Plan and Simulate Threats

Insight leverages imported scanner data to model attacks and identify where exploit-based testing might be necessary.

- **Discover** and profile network, web and endpoint targets
- **Reveal** attack paths that expose business assets
- **Identify** exploits that could be used by attackers

You can also begin assessments at this stage, since Insight can identify and profile targets to select appropriate tests independently of scanners.

Get meaningful, actionable information

- Validate vulnerability data from multiple, disparate sources
- Pinpoint critical exposures and eliminate false positives

Correlate vulnerabilities to business risk

- Reveal specific assets and resources exposed to breaches
- Report risk in context of your organizational structure, processes and compliance mandates

Trace attack paths across multiple vectors

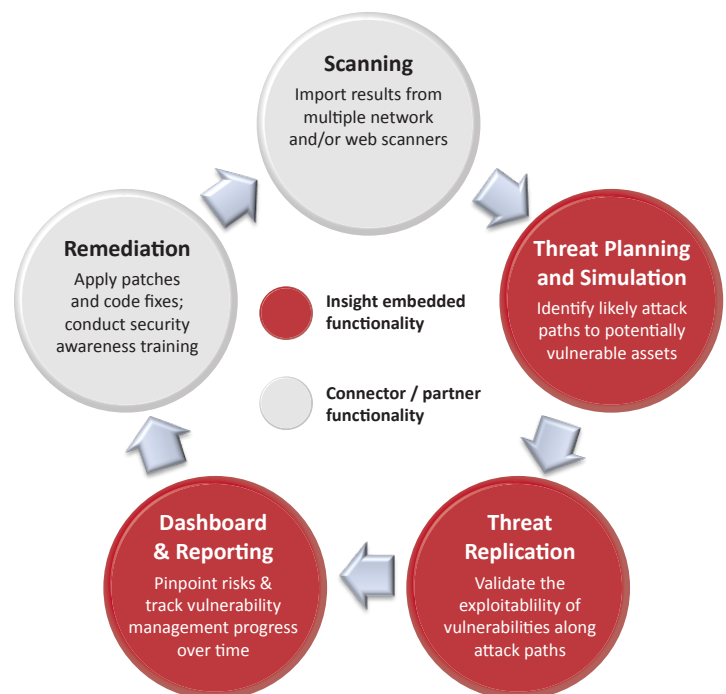
- Demonstrate how attackers can chain vulnerabilities across vectors to move through your environment

Increase team efficiency and effectiveness

- Focus resources on addressing the most critical risks
- Increase the scope and frequency of security assessments

Demonstrate continuous improvement

- Measure the impact of remediation efforts
- Compare and track results over time



The CORE Insight unified vulnerability management workflow.

3. Replicate Threats

Insight enables you to validate if critical assets could be breached and understand the risk to your business – with no false positives.

- **Network:** Exploit vulnerabilities and weak passwords
- **Web:** Verify SQL injection and cross-site scripting exposures both before and after applications go live
- **Endpoint:** Evaluate phishing awareness & endpoint defenses

4. Dashboards and Reporting

Insight Dashboards

- **Executive:** Monitor overall security posture and drill-down for actionable details to inform decision making
- **Tester:** Configure and execute security assessment campaigns
- **Campaign:** Gain in-depth information about the status and results of specific campaigns

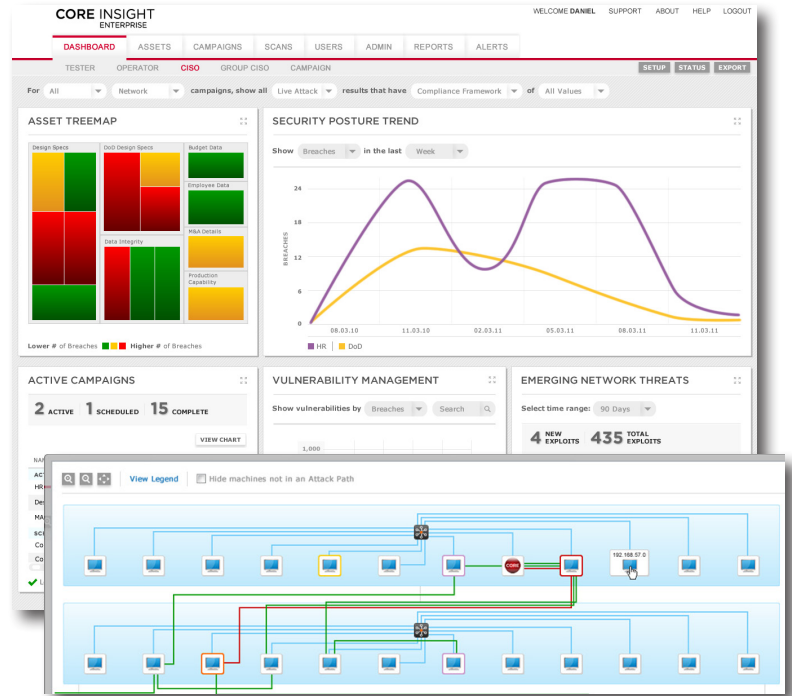
Insight Reports

- **Executive:** Identify key exposures, see changes in risk posture, and determine where to focus resources
- **Vulnerability Validation:** Pinpoint exploitable vulnerabilities from imported scan results
- **Campaign:** Get complete details on attack paths identified, assets tested, and vulnerabilities confirmed – plus audit trails of assessment activities
- **Delta:** Compare results before and after remediation
- **Trend:** Track security assessments over time

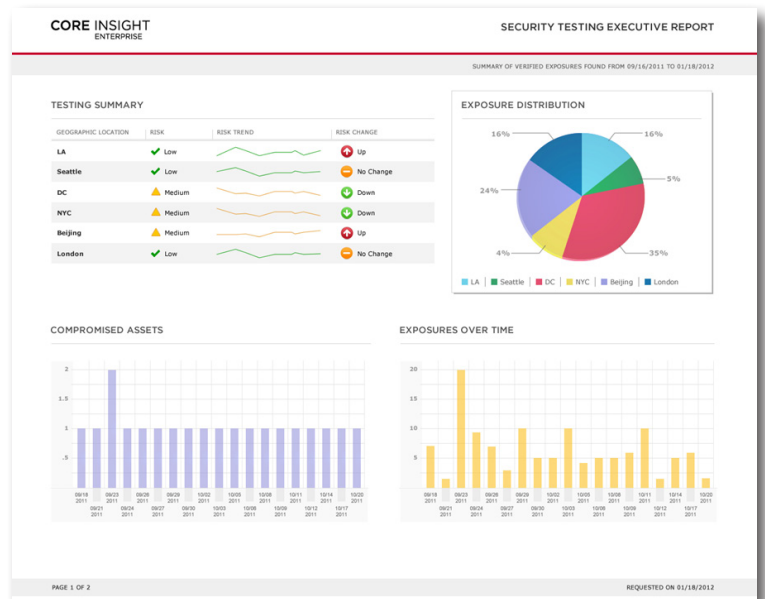
5. Remediate Vulnerabilities and Repeat Testing

Insight provides the information you need to quickly address exposures – and makes it easy to confirm that fixes are effective.

- Get actionable information for efficient remediation
- Prioritize exposures and optimize resource allocation
- Repeat testing to confirm that fixes are effective and do not introduce new exposures



The CORE Insight Executive Dashboard enables you to track vulnerability management effectiveness throughout your organization. Drill-down capabilities include visualizations of how attacks could leverage multiple vulnerabilities to reach critical assets.



The Executive Report provides key metrics about your real-world security posture.