

# Vulnerability Risk Management in Higher Education

Secure your dynamic IT environment with Rapid7 InsightVM

Colleges and universities have become enticing targets for threat actors given the wealth of staff and student data, intellectual property, and payment information housed in their IT systems. Simultaneously, these environments also pose a unique security challenge given the volume and diversity of devices that join and leave the network by the minute, and the difficulty of managing various segments of the environment with different needs and priorities. If compromised, the fallout isn't limited to reputational damage—the loss of sensitive information could have rippling enrollment and financial impact for years to come.

To stay protected in the face of these threats, you need a vulnerability risk management solution that can adapt to your dynamic environment, maximize visibility and communication across widely distributed sites and stakeholders, and keep you on track towards your risk reduction and compliance goals. Rapid7 InsightVM is designed specifically with these kinds of challenges and the modern IT environment in mind; learn what makes it the ideal solution for higher education institutions below.

## Visibility into every layer of your infrastructure

You can't comprehensively manage risk in your environment unless you know exactly what's there. InsightVM is the only solution of its kind able to identify all of your assets whether they be local, remote, or virtualized, including those you may not have even known about; its **Attack Surface Monitoring with Project Sonar** capability scans the public internet to help you identify your externally-facing, internet connected assets, and DHCP discovery connections dynamically uncover new assets as they join the network.

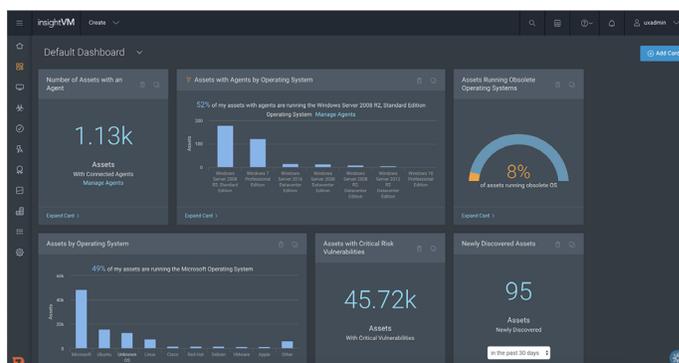
Plus, coverage isn't limited to just your data centers and most critical infrastructure—InsightVM scans and assesses your complete modern infrastructure, including cloud-based assets and containers. That said, we know not all assets are created equal: the **Real Risk** score in InsightVM allows you to factor in business criticality in the way risk is prioritized in your environment.

Once you've identified and prioritized the risk across your attack surface, **Live Dashboards** enable you to create the most efficient views for vulnerability analysis in your unique environment. These dashboard views can be customized to offer everything from a bird's eye view of your whole institution's risk posture to the remediation progress of a named vulnerability in a satellite campus.



InsightVM earned the highest possible scores in the criteria of Vulnerability Enumeration and Risk-Based Prioritization.

—The Forrester Wave™: Vulnerability Risk Management, Q4 2019



## Confidence in compliance

Beyond your own internal security goals, we know that higher education institutions are also accountable for compliance to numerous policies and standards. InsightVM eases this process by offering pre-built scan templates for common compliance requirements such as HIPAA, SOX, USGCB (a base requirement of FISMA), and PCI DSS. Additionally, Rapid7 is a PCI Approved Scanning Vendor (ASV).

For further data protection measures, such as those required by GDPR, InsightVM can automatically audit systems for compliance with secure configurations, password policies, and access control requirements.

## A centralized home for your operations

Managing a widely dispersed IT environment can be cumbersome, to say the least. From different campuses spread out geographically to different schools or offices under the university name, InsightVM offers a single source of truth for your operations.

To start, InsightVM enables you to create individual sites for scanning based on what makes most sense for your organization. While you still retain the ability to push out and hold teams accountable for policies and goals set by central IT, you can also drill into more specific use cases like zero-day impact on your primary data center. InsightVM also offers granular, easy-to-set-up role based access control (RBAC) for different types of users across your IT and security teams—these roles can be customized for varying permissions related to sites, asset groups, ticketing, reporting, and more.

When it comes time for patching and containment, Remediation Projects make it easy to assign and track remediation duties in real time, providing continuous visibility into how well issues are being fixed across the organization or within certain parts of your network; this includes your most efficient remediators, past-due projects, remaining work, and more. **Remediation Projects** also integrate with popular ticketing systems like Atlassian Jira and ServiceNow, so teams are working seamlessly within IT's existing workflows.

---

**The big difference was in the prioritization of vulnerability remediation. Rapid7's prioritization is automatic, which saves me almost 140 hours of work compared to prioritizing it manually... Rapid7 security solutions allow me to automate the scanning and reporting features, which saves me at least 10 hours in asset discovery and reporting.**

—Allen Basey, Senior Security Analyst at MCPHS University

---

## Easy integration into your existing operations

InsightVM will help you tangibly reduce risk from the start, but we know that improving your overall security posture is an effort that reaches beyond one solution—that's why InsightVM is designed to maximize impact with the other parts of your security stack. With out-of-the-box integrations with Microsoft, ServiceNow, McAfee, Palo Alto Networks, and (many) more, InsightVM empowers you with more efficient, more comprehensive end-to-endpoint coverage even across vendors.

Within the Rapid7 Insight cloud platform, InsightVM shares a lightweight agent with InsightIDR, a Leader in the 2020 Gartner Magic Quadrant for SIEM. **The Insight Agent** automatically collects data from all your endpoints, even from remote assets or users and sensitive assets that can't be actively scanned or that rarely join the corporate network. This shared dataset can then be leveraged for vulnerability analysis, as well as threat detection and user behavior analytics (UBA) activities for a more unified view of your network. To extend your risk protection to the application layer, go beyond application discovery in InsightVM to test and remediate with InsightAppSec, our leading dynamic application security testing (DAST) solution.

Need even more flexibility for the way you secure your environment? InsightVM also features an open, **RESTful API** that allows you to automate virtually any aspect of your vulnerability risk management process.



InsightVM received the highest possible scores for its extensibility and Partner Ecosystem.

—The Forrester Wave™: Vulnerability Risk Management, Q4 2019

## Tracking shared progress

To bring your operations full circle, you need an efficient way to measure and track progress across your program, then communicate the efficacy of your efforts to those who need the information most. InsightVM makes this painless with **Goals and SLAs**. Goals and SLAs ensure you're making (and tracking) progress at an appropriate pace, and maintaining compliance with the standards you've set for your program at an institutional or more granular level.

Performance against these metrics can then be visualized through dashboards unique to different stakeholders—from technical remediation teams to your Executive Board—or reported on with our highly customizable reporting templates. This ensures that every stakeholder gets the information they need that's most relevant to them quickly and at scale.

---

**“[Role based access] gives system administrators around the campus a sense of empowerment.”**

—Randy Marcheny,  
Chief Information  
Security Officer at  
Virginia Tech University

---

## Get started today:

Dive deeper into how InsightVM can help secure your modern environment at [www.rapid7.com/insightVM](http://www.rapid7.com/insightVM).