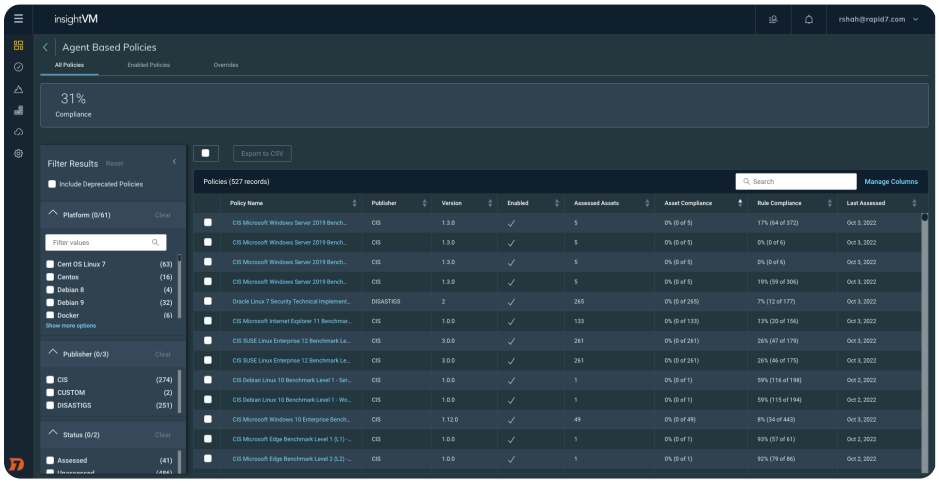
Security Configuration Assessment with InsightVM

Assess configuration of enterprise IT assets to proactively secure your environment and meet compliance mandates.

Incorrectly configured enterprise assets increase the attack surface and make your IT environment more vulnerable to breaches. These poor or default configurations may include weak password policies, unsecured ports and services, multiple root accounts, unmonitored guest access, and more that expose your systems and data for an attacker to exploit.

A robust vulnerability management (VM) program should assess for security configurations in addition to vulnerabilities. However, identifying insecure configurations can be overwhelming for security teams. Many teams lack visibility into their environment to monitor configurations and are unsure of what "secure" looks like for each system.

Our Policy Assessment feature — part of InsightVM, Rapid7's vulnerability management solution — provides organizations the ability to conduct Secure Configuration Assessments of IT assets against widely used industry benchmarks such as Center for Internet Security (CIS) and Security Technical Implementation Guides (STIG) or custom internal policies. InsightVM's configuration assessment capability gives you the flexibility to deploy Insight Agents or Scan Engine to assess configuration of remote and on-prem enterprise assets.



Key Benefits

- Mature your VM program to harden your systems against breaches
- Secure remote endpoints
- Leverage expert knowledge from CIS benchmarks and DISA STIGs
- Stay compliant with industry regulations or internal policies

Features

- Flexible deployment
- Out-of-the-box coverage for CIS benchmarks and DISA STIGs
- Custom policy builder
- Visualize policy compliance
- Built-in to InsightVM

Secure configuration assessment with InsightVM | How it works

Define:

Select the benchmarks or define custom policies and assets that need to be assessed

Collect:

Collect configuration settings of remote and on-prem IT assets using Insight Agents and/or Scan Engine

Assess:

Compare the asset(s) configuration information against each enabled benchmark or custom policy

Secure:

Use the configuration assessment results including the remediation information to harden the systems

Key benefits

Mature your VM program to harden your systems against breaches

As modern networks evolve, your risk exposure changes by the minute. It's easy for organizations to rush through business with default system settings that increase the attack surface. In such a risk landscape, security configuration assessment is critical not only for compliance in regulated industries but for any organization that wants to mature its VM program. Use the built-in configuration assessment capability of InsightVM to harden the systems and proactively secure the IT environment.

Secure remote endpoints

With the shift to remote work and an increase in digitalization, today's security teams have to protect a fast growing environment. Ensure coverage and secure configurations for your remote endpoints by leveraging Insight Agents for configuration assessment.

Leverage expert knowledge from CIS benchmarks and DISA STIGs

Know what secure configurations look like with guidelines from CIS and DISA. CIS is consensus-based, best-practice security configuration that is widely accepted by government, business, and industry. While DISA STIG encompasses US Government requirements. These benchmarks outline secure configuration settings for software, OS, network devices, desktops and more.

Stay compliant with industry regulations or internal policies

Meet requirements of compliance framework under industry regulations like PCI-DSS, HIPAA, DFARS, NIST, CMMC, FISMA and more that prescribe configuration assessment as one of its key requirements; Also ensure compliance with your company's own internal policies/baselines.

Features that make it possible

Flexible deployment

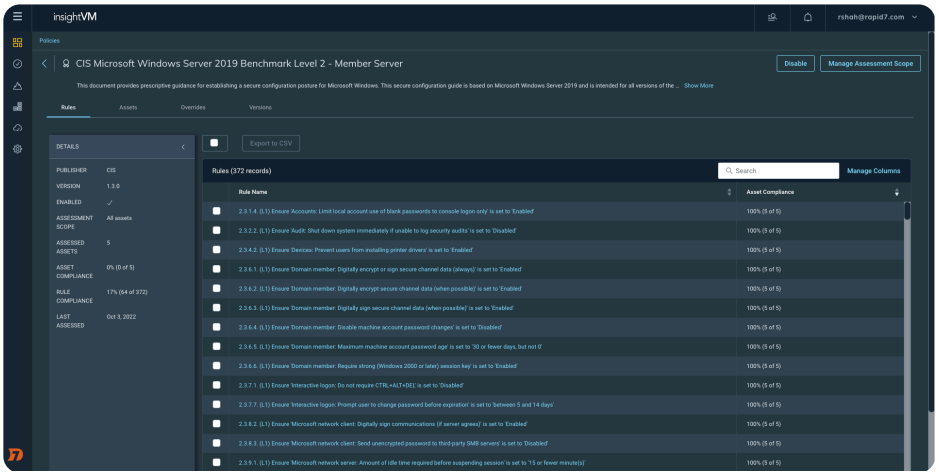
With hybrid or remote work, your IT assets are no longer in a single network but rather distributed across various environments. Using the same foundational technology as InsightVM, our secure configuration assessments can be flexibly performed either through Insight Agents or the Scan Engine to ensure your remote and on-prem assets are protected. The universal Insight Agent is a piece of lightweight software you can install on various types of endpoint devices, with Windows, Linux, or Mac operating systems to collect data from across your IT environment. Scan Engines can be deployed centrally in your environment to perform active network scans, providing device discovery and configuration assessment capabilities.

Out-of-the-box coverage for CIS benchmarks and DISA STIGs

Organizations look to CIS and DISA for guidance on security configuration best-practices. CIS benchmarks and DISA STIGs are built into InsightVM's configuration assessment capability; so you can quickly and easily begin scanning configuration for

- Operating Systems
- Network Devices
- and more
- Server Software
- Desktop and Endpoint Software

As CIS and DISA make updates to the benchmarks/guidelines or publish a new version, Rapid7 will update the product to ensure you're working with the latest guidance.



Custom policy builder

A benchmark or guideline as-is may not meet the unique needs of your business. With our tool you can modify existing policies or create new policies from scratch to align with the needs of your operating environment. You can modify an existing policy for use on a newer OS before an official benchmark is available from CIS or DISA STIG.

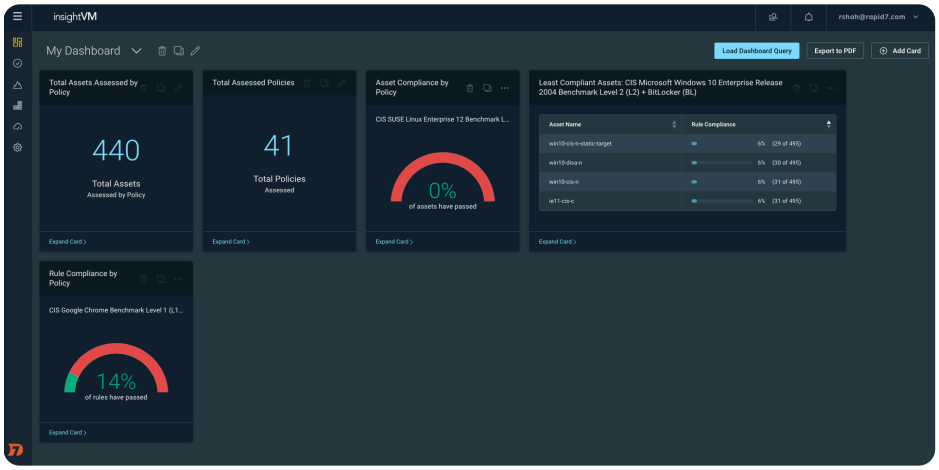
> **An effective system hardening program can drastically reduce the attack surface from threats, while achieving compliance objectives.**
>
> Gartner

Visualize policy compliance

Understand how well the assets in your environment comply with individual policies. Once you've assessed your risk posture, you can take clear, actionable steps toward compliance and securing the systems configurations.

Get compliance data, visibility, and reporting on the platform with dashboard cards like

- Total Assessed Policies
- Total Assets Assessed by Policy
- Asset Compliance by Policy
- Least Compliant Assets by Policy
- Rule Compliance by Policy



Built-in to InsightVM

InsightVM supports a robust vulnerability management program that assesses configurations along with vulnerabilities in your IT environment. The configuration assessment capability is built into InsightVM; this means you can start scanning enterprise assets for configurations in a few clicks without the need to integrate an additional module or a paid add-on.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/