Extend Vulnerability Coverage with the Scan Assistant

Achieve the accuracy of authenticated scan results, without the hassle of credential management.

Historically, enterprises have had to rely on using administrative credentials for authenticated vulnerability management scans. This approach provides more accurate vulnerability detections, better reporting and analysis, and thorough asset vulnerability coverage when compared to unauthenticated scans.

However, traditional authenticated scanning comes with a considerable administrative burden for IT Administrators. It can be difficult to manage for a host of reasons, like jurisdictional boundaries, insufficient system access, password rotation policies, or credentials being managed in multiple locations across the organization. Finally, there is an ever-present risk of compromise, when using admin accounts that have privileged access to systems, for authenticated scans.

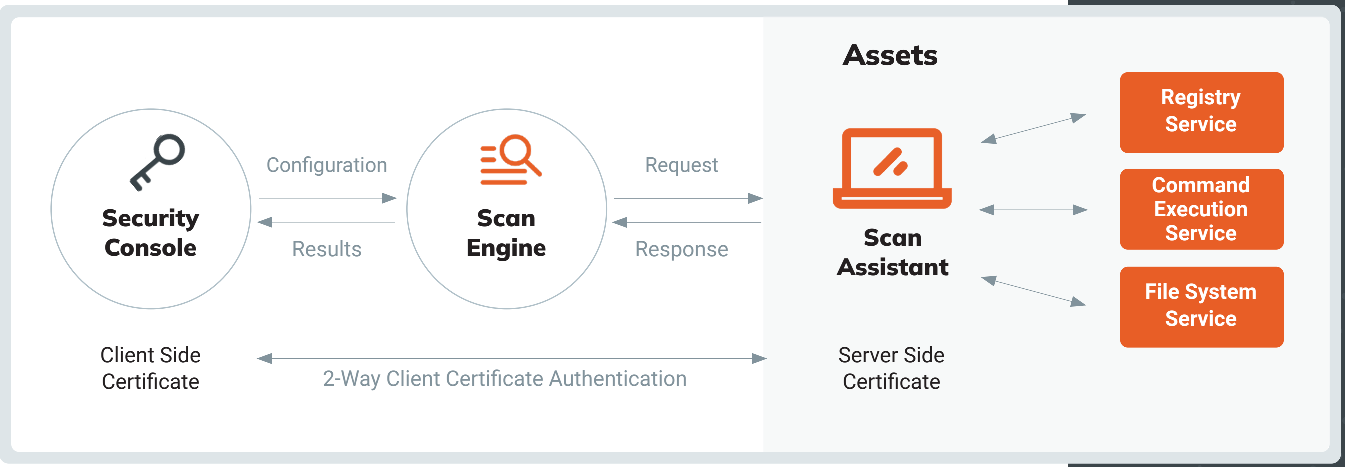
Introducing the InsightVM Scan Assistant

The Scan Assistant provides an innovative alternative to traditional credentialed scanning. Instead of account-based credentials, it uses digital certificates, which increases security and simplifies administration for authenticated scans. The Scan Assistant is a lightweight service deployed on the asset that executes scans in conjunction with the Scan Engine using Scan Templates.

Along with Insight Agents and Scan Engines, the Scan Assistant provides security teams an additional tool to extend enterprise vulnerability coverage. The Scan Assistant is available for Microsoft Windows and Linux assets. It is compatible with Nexpose and InsightVM, but does not require cloud connectivity.

Key Benefits

- Reduced risk
- Enhanced scan accuracy
- Simplified administration at scale
- Faster Microsoft Windows scan results



The Scan Assistant provides an ideal solution for the following vulnerability coverage scenarios:

- **Conduct authenticated scans without credential management.** The Scan Assistant uses digital certificates instead of traditional administrative credentials.
- **Operate in air-gapped networks with no or limited Internet access.** The Scan Assistant does not require internet connectivity.
- **Predict resource utilization for mission critical assets.** The Scan Assistant is only active during scans initiated by the Scan Engine.
- **Get granular control over asset assessment parameters.** The Scan Assistant responds to specific scan parameters defined via Security Console Scan Templates and performed by the Scan Engine.

Key Benefits

Reduced risk

Using privileged account-based credentials for authenticated scans carries inherent risk. The Scan Assistant uses public-private key encryption and digital certificates instead, greatly reducing the potential for a security compromise.

Enhanced scan accuracy

The Scan Assistant will automatically and securely ensure the access required to appropriately interrogate the asset for both vulnerabilities and policy compliance.

Simplified administration at scale

Account-based credential management is a never-ending task. Scan Assistant digital certificates can be automatically generated and administered for thousands of assets from the Security Console.

Faster Microsoft Windows scan results

Vulnerability scans of MS Windows Domain Controller servers and Windows policy scans using SMB2 or CIFS can be time consuming. The Scan Assistant will typically outperform traditional credentialed scans for vulnerability and policy scans on all Windows platforms.

> “
>
> **The Scan Assistant just works - flawlessly.**
>
> Financial Services Customer

Features that make it possible

Public-private key based authenticated scanning

The Scan Assistant uses TLS (Transport Layer Security), X.509 certificates and NIST (National Institute of Standards and Technology) CNSA (Commercial National Security Algorithm Suite) strength encryption rated for Top Secret data, to provide authenticated scans without the risk of shared administrative credentials.

Automatic Digital Certificate Generation

Scan Assistant X.509 certificates can be created automatically from the Security Console, greatly simplifying the certificate generation process.

Automatic Digital Certificate Rotation and Software Updates

Asset-based software will require updates as new versions are released. Digital certificates have a set validity period. Scan Assistant software updates and digital certificate rotation can be automated from the Security Console using Scan Templates, facilitating fleet management for customers with hundreds to thousands of assets.

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.

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/