Insight Frequently Asked Questions (FAQs)

How do I access the new customer portal?

You may access the Insight portal by going to https://insight.silversky.com/

How do I add more users to the Insight customer portal?

SilverSky will provide your company with user credentials to access the Insight customer portal. During the installation process, at least one member of your company will be given credentials to add new users to the Insight portal.

How does the Insight portal scan my assets?

There are a few scanning options that can be used to make sure your entire attack surface is covered:

Agent-based Scanner: This agent can be deployed to MacOS or Windows OS workstations and servers. Once installed, the agent can scan either the local machine or be configured to scan the Active Directory.

Super-agent Scanner: This scanner is deployed onto physical hardware. This allows for network discovery scans and scanning of headless devices.

Agentless Scanner: This scanner is deployed to a VM to scan your internal network. This allows headless devices to be scanned as well as to check for devices that are added. Agentless can also be in your cloud environment (Azure, GCP, AWS) to scan your subnets in the cloud.

Cloud Scanner: This is a preinstalled scanner that can scan external IPs and FQDNs.

How seamless is the installation? Do I need to plan for reboots?

The installation process is designed to allow any size business to easily integrate into the Insight platform. The Knowledge Base articles and videos are posted at Vulnerability Scanning Migrations and include step-by-step methods and pictures to assist with the onboarding. Once the agent is installed there is no need for a machine reboot. The agents will be updated automatically, so there is no need to worry about pulling in the latest version.

Are there any technical prerequisites?

- The Agent-Based Scanner has the requirements: Windows 7 SP1/Windows Server 2008 R2 SP1, 500 MB of Disk, Windows Management Instrumentation running.
- The Super Agent has a hardware requirement of: 2 CPUs, 12 GB of RAM, 90 GB of Disk
- The Agentless Internal Scanner supports Hyper-V and VMWare.

Can I use my RMM tool?

Yes! The following RMM tools are supported:

- Active Directory GPO [using MSI+MST]
- Active Directory GPO [using batch startup script]
- KASEYA VSA
- Itarian Endpoint Manager
- Connectwise Automate

How does the scanner communicate with the Insight portal?

Each customer portal has a unique Footprint Agent Token; this token along with the portal URL is added to the scanner, allowing the traffic to reach your portal securely.

Do I need to whitelist an IP for External Scanning?

Yes. The External Scanner will be scanning from 34.73.183.250 and you will need to whitelist that IP.

Will I need to implement any firewall rules for Insight?

Yes. There are changes for if you are using the Agentless Internal Scanner or if you are using the Agent-based scanner.

Agentless Internal Scanner Rules				
Destination	Port	Protocol	Encrypted	Purpose
https://update.codacloud.net	443	HTTPS	Yes	Footprint IS Automated Updates (optional, highly recommended)
https://sentry.codacloud.net	443	HTTPS	Yes	Footprint IS Alerting Service (optional, highly recommended)
https://insight.silversky.com	443	HTTPS	Yes	Footprint IS - Console Connectivity (mandatory)
https://insight.silversky.com	5671	SSL	Yes	Footprint IS - Console Connectivity (mandatory)

Agent-Based Scanner Rules				
Destination	Port	Protocol	Encrypted	Purpose
https://update.codacloud.net	443	HTTPS	Yes	Footprint Automated Updates (mandatory)
https://sentry.codacloud.net	443	HTTPS	Yes	Footprint Agent Alerting Service (optional, highly recommended)
https://insight.silversky.com	443	HTTPS	Yes	Footprint IS - Console Connectivity (mandatory)

If we only subscribe to only External or only Internal scanning today, can we add the other scanning as well?

Yes, customers can add either External or Internal vulnerability scanning to their existing services by

- Adding in the External IPs to implement External scanning.
- Adding either agent-based or agentless scanning to allow the Internal scanning.

Please note that in the Insight service, we bill based on the IPs that are being scanned in the system. We do not make the distinction between External or Internal IPs like in your current

Vulnerability Scanning service. We also reserve the right to adjust billing to market-based rates if necessary.

Can I have my findings or reports emailed to me?

No, due to security policies, the report will be available in the Portal. If you select the option to mail a weekly report, you will receive an email with the link to login into your scanning portal.