Outpost24

Vulnerability Management made easy

HIAB Deployment Guide

Version: 2.5

2019-04-08

Table of Contents

About This Guide

The purpose of this document is to assist you in setting up the HIAB installation correctly within your environment and support you in reaching your security objectives. It provides you with instructions for performing key administration tasks such as planning a HIAB deployment within a distributed solution.

For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

1 Introduction

This guide will help you deploy your HIAB appliances strategically to meet your organizations security goals. If your organization has not defined these goals yet, this guide provides you with important questions that you should answer, so that you can determine what you want to achieve with vulnerability scanning.

1.1 Intended Audience

You should read this guide if you fit one or more of the following descriptions:

- You are responsible for planning how your organization will deploy the HIAB solution, whether you are the single employee in the IT department or a system administrator for a larger company.
- You have been assigned to be the installation owner for your company.

2 HIAB Deployment Planning

The configuration and deployment options that are available in HIAB allow you to address a wide variety of security issues, business models, and technical complexities. If you have a defined deployment strategy, you can be sure that the HIAB is used with maximum efficiency.

2.1 Product Description

The HIAB is a virtual image appliance with many features that allow you to set up the system in multiple ways to suit your organization.

Features include:

- **Scalable**: Multiple HIAB appliances can be connected to each other in a distributed architecture.
- **Scanning nodes**: Additional appliances can be placed in remote data centers, which allow you to perform scanning of all local services without exhausting the network bandwidth.
- **Storage:** All data is stored locally on the appliance.
- **External scanning**: The HIAB can be connected to the SaaS service OUTSCAN which allow you to perform scanning from an external location, transferring the result back to the appliance.

2.2 Understanding HIAB Key Concepts

HIAB is a vulnerability management solution that scans networks to identify available devices and probe them for vulnerabilities. Once the information is gathered, it stores it locally and process the data for report generation. You can then use the reports to help assess your network security at various levels of detail and remediate vulnerabilities quickly.

The HIAB scanner identifies vulnerabilities in all layers of a network-computing environment, including applications, databases, operating systems, and files. It can also detect suspicious programs, verify updates, and perform authenticated checks against company web services.

2.2.1 Schedulers and Scanners

Scheduler

A scheduler distributes scan jobs to one or more scanners and manages everything such as targets, findings, sending notification emails, reports, for example in one place.

Scanner

A scanner receives jobs from the scheduler, performs scans, and returns the data to the scheduler.

Scheduler - Scanner Communication

It can be defined as either push or pull, depending on requirements of how the traffic is allowed to flow between the different locations or network segments. It depends on the firewall setup.

If the scheduler is set to *only send information* to the scanner and the scanner is *not allowed to return data*, the scheduler must be set to push. If the scheduler is set to push, manual interaction with the scanner through the scheduler is needed.

Tasks such as, *Start a scan* or *Update now* from the distribution settings, is then sent to the scanner. It is possible to set up an automatic process for the Scan Jobs to run without interactions.

If the firewall allows the scanner to send traffic back to the scheduler, the scanner can be set to pull the information. The scanner then frequently (every third minute) asks the scheduler if it has something to do, such as: Updates, scan jobs and so on. It is highly recommended to have the scanners up to date at all time.

In a distributed solution, the HIAB is referred to as either a scanner or a scheduler. The scanner should be thought of as a scanning node that will not store any data if the scan is initiated from the scheduler.

Currently, the following set up options are available in a distributed scanning model:

- **HIAB Single**
  One HIAB performing scans against your network. Everything is managed from one appliance.

- **HIAB Scheduler, HIAB Scanner**
  HIAB scheduler uses one or multiple scanners to reach different network areas or to scale the solution to allow more scans to be executed during the same time period.

- **HIAB Scheduler, OUTSCAN Scanner**
  The HIAB can be set up to connect to the external OUTSCAN solution which allow you to perform external scanning against your outside perimeter, without the use of an additional external appliance. All data is securely stored on the HIAB appliance and removed from the OUTSCAN environment when the report has been successfully transferred.

- **HIAB Scheduler, HIAB Scanner(s), OUTSCAN Scanner**
  This solution will provide you with all the benefits of the HIAB distributed solution and allow you to both scale the solution and reach additional network areas, such as a subdivision of your company or any additional data center.
  This solution does not use any agents. It will perform all the scanning over the network with the use of commonly used protocols to gain access to target assets. Therefore, this solution makes it unnecessary for you to have to install and manage software agents on your targets which will lower your TCO (Total Cost of Ownership) and at the same time avoid security and stability issues which can occur with installed agents.

3 Define your Goals for HIAB

If you know in advance what security-related goals you would like to fulfill with the HIAB, it will help you when you design the most efficient and effective solution deployment for your company.

3.1 Do Not Limit Security for Compliance

Most companies have a very simple answer as to why they are acquiring a solution like the HIAB, which is that they need to comply with some security requirements imposed either by the government or by a private-sector entity that regulates their industry.

Compliance goals may help you to define your deployment strategy, but it is important to think beyond compliance alone to ensure security. For example, protecting a core set of network assets, such as credit card data servers in the case of Payment Card Industry (PCI) compliance is important but some aspects might not be considered in the compliance goals that your company might see as a risk.

Hackers will use any convenient point of entry to attack networks. A hacker may exploit an Internet Explorer vulnerability that makes it possible to install a malicious program on an employee computer when visiting web sites. The malware may be a remote execution program with which the hacker can access more sensitive network assets, including those defined as being critical for compliance.

A security plan that focuses only on the perimeter also has limitations. An inside user could be careless or a disgruntled IT employee with access to sensitive servers might be a risk. Compliance is not synonymous with security. On the other hand, a well implemented, comprehensive security plan will include among its benefits a greater likelihood of compliance.

3.2 Know Your Business Case to Know Your Goals

If you have not yet defined any goals for your HIAB deployment or if you are having difficulty doing so, start by looking at the technical environment and your business model to identify your security needs.
Factors to consider include network topology, technical resources (both hardware and bandwidth), human resources, time, and budget.

3.2.1 How Big is Your Enterprise?

How many networks, sub networks, and assets does your company have? The size of your company is a large factor when it comes to the number of appliances that you need to deploy.

3.2.2 What is the Geography of Your Enterprise?

How many physical locations is your network currently deployed over? Where are those locations (nearby or far away)? Where are firewalls and DMZs located?
These factors will affect how and where you need to deploy the HIAB appliances.

3.2.3 How is Your Network Segmented?

What are the ranges of IP addresses and sub networks within your organization?

3.2.4 What is Your Asset Inventory?

What kinds of assets are you using? What are their functions? What operating systems, applications, and services are running on them? Where are these different assets located related to firewalls and DMZs? What are your hidden network components that support other assets, such as Virtual Private Network (VPN) servers, LDAP servers, routers, switches, proxy servers, and firewalls? Does your asset inventory change infrequently? Or will today's spreadsheet listing all your assets be out of date in a month?

Answering these questions will help you determine not only the scope of your HIAB license but also the type of license you require. Additionally, asset inventory influences site planning and scan template selection.

Does your asset inventory include laptops that employees take home? Laptops open a whole new set of security issues that render firewalls useless. With laptops, your organization is essentially accepting external devices within your security perimeter. Network administrators sometimes unwittingly create back doors into the network by enabling users to connect laptops or home systems to a VPN. Additionally, laptop users working remotely can innocently create vulnerabilities in many ways, such as by surfing the Web without company-imposed controls or plugging in personal USB storage devices. An asset inventory that includes laptops may require you to create a special scan job that you scan during business hours, when laptops are connected to your local network.

3.2.5 Example Environment: My Company

Once you have answered the previous questions it might be wise to create a table that looks like the one shown below.

Network Segment	Address Space	# of Assets	Location	Asset Functions
London Sales	10.0.1.0/24	254	Building A Ground level	Workstations
London IT/Administration	10.0.2.0/23	50	Building A Floor 1	Workstations Servers
London Printers	10.0.3.0/24	16	Building A	Printers
London DMZ	172.18.0.0/25	30	Data center	Web server Mail server
Japan Sales	10.1.1.0/24	67	Building 1	Workstations
Japan Development	10.1.2.0/23	34	Building 1 Floor 2	Workstations Servers
Japan Printers	10.1.3.0/25	14	Building 1 Floor 1-2	Printers
Japan DMZ	172.18.1.0/25	21	Building 1 Basement	File server Mail server

3.2.6 What are the Key Areas in Your Organization?

What assets contain sensitive data? Which of the servers are on the perimeter of your network? Do you have any assets like web, e-mail or proxy servers located outside of your firewalls?
Any areas of specific concern may require a local scanner to be placed in that area.

3.2.7 What are Your Resources?

How much bandwidth do you have available? What is your security budget? How much time do you have to run the scans (are there any maintenance windows which need to be considered)? These considerations will affect both the placement and how many appliances you need to deploy.

3.2.8 What Exactly are the Security Risks for Your Organization?

How easy is it for hackers to penetrate your network remotely? Are there multiple logon challenges in place which might slow them down? How difficult is it for hackers to exploit vulnerabilities in your organization? What are the risks to data confidentiality, integrity, and availability?

The CIA triad (Confidentiality, Integrity, and Availability) is a good metric to quantify and categorize risks in your organization. The HIAB supports applying these kinds of details on a per host basis which will help you when you prioritize your vulnerabilities.

Confidentiality is the prevention of data disclosure to unauthorized individuals or systems. What happens if an attacker steals customer credit card data? What if a Trojan provides hacker access to your company's confidential product specifications, business plans, or other intellectual property?

Integrity is the assurance that data is authentic and complete. It is the prevention of unauthorized data modification. What happens when a virus wipes out records in your payroll database?

Availability refers to data or services being accessible when needed. How will a denial-of-service hack of your web server affect your ability to market your products or services? What happens if a network attack takes down your phones? Will it cripple your sales team?

Other risks have direct business or legal implications:

- What danger does an attack pose to your organization's reputation?
- Will a breach drive away customers?
- Is there a possibility of getting sued or fined?

Knowing in what way your organization is at risk can help you set priorities for deploying scan engines and scheduling scans.

.

4 Determining How Much You Need

The scope of your HIAB investment includes the license cost and the number of appliances that you need to purchase. When you are considering how much you need, it's important to keep your security goals in mind.

Make sure your organization has a reliable, dynamic asset inventory system in place to ensure that your license provides adequate coverage. It may not be unusual for the total number of your organization's assets to fluctuate on a regular basis. As staff numbers grow and reduce, so does the number of workstations. Servers go online and out of commission, employees who are traveling or working from home plug into the network at various times using VPNs.

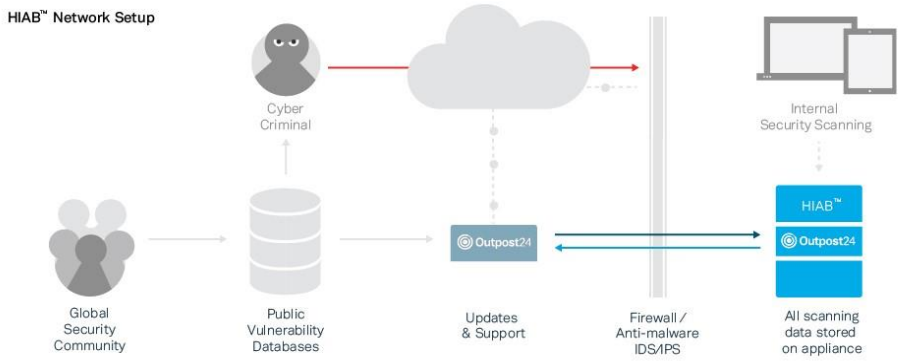
This fluidity underscores the importance of having a dynamic asset database. Relying on a manually maintained spreadsheet is risky. There will always be assets on the network that are not on the list and, if they're not on the list, they are not being managed which results in added risk.

The best way to keep your asset database up to date is to perform discovery scans on a regular basis. The HIAB has functionality to perform this type of discovery on a scheduled basis.

Look at your network inside out: hosted vs. distributed engines.

There are two types of HIABs that you can use when you build your scanning solution, a scheduler and scanner (the scheduler can also be connected to the external solution). You can choose to only use one option, or you can use them both in a complementary way. It is important to understand their roles in your network to deploy them efficiently. The external solution will scan your external perimeter and the scheduler can be used as a single scanner that later can be extended with additional scanners if you require to up scale the solution.

With the use of the external solution, you will be able to see your network as an external attacker does. The external solution will scan everything on the periphery of your network, outside of your firewall. These are normally assets that are required to be present in order to provide public access, like web sites and e-mail servers.



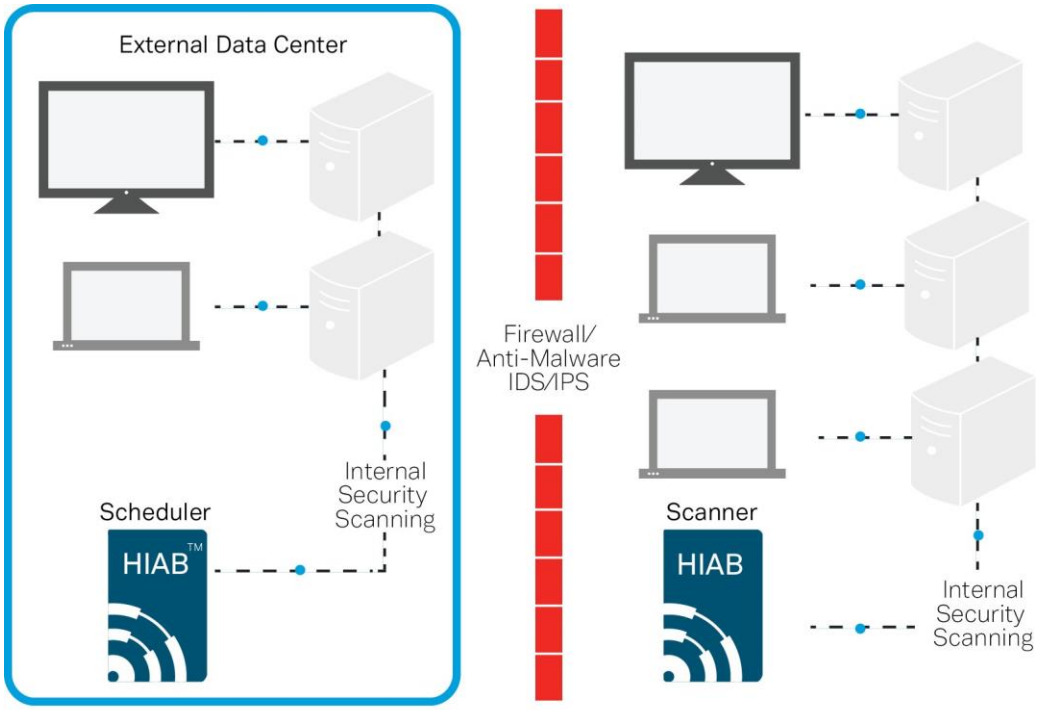
Outpost24 maintains the external scanners, you do not need to install nor manage them. The scanners reside in a continuously monitored data center that ensure high standards for availability and security.

***Important Note**: If your organization uses outbound port filtering, you need to modify your firewall rules to allow the HIAB to connect to Outpost24 (to retrieve updates and schedule external scans).*

With these advantages, it might be tempting to use only external scanners. But they have limitations that in certain aspects would make an internal appliance more suitable, for example access rights.

***Important Note**: The HIAB scanner and the external service will not store the report data on the appliance.*

The HIAB scheduler and scanner allows you to inspect your network from the inside, ideal for core servers and workstations. You can deploy scanners anywhere in your network to obtain multiple views. This flexibility is especially valuable when it comes to scanning a network with multiple sub networks, firewalls, and other forms of segmentation.



4.1 Distribute scanners strategically

When determining where to put your scanners, it is helpful to look at your network topology. What are the areas of separation, and where are the connecting points? Once you have the answers to those questions you have a good base for where to deploy the scanners.

***Note**: It is possible to run scans from the HIAB scheduler if needed. This may not be appropriate for a larger production environment with multiple scanners since the scanning will consume memory which may be better used when managing the scanners and any user requests.*

Situations that could call for the placement of a scanner are:

- Firewalls, IDS, IPS, and NAT Devices
- VPNs
- Sub Networks
- Perimeter Networks (DMZ)
- ACL
- WANs and Remote Asset Locations

Firewalls, IDS, IPS, and NAT Devices

If you have a firewall separating two or more sub networks and deploy a HIAB on one side, you will not be able to scan the other sub network without opening the firewall (which may violate your corporate security policy).

An application layer firewall may have to inspect every packet before it will route it. The firewall should track the state for each connection. A typical scan can generate thousands of connection attempts in a short period, which can overload the firewall state table or state tracking mechanism.

Scanning through an Intrusion Detection System (IDS) or Intrusion Prevention System(IPS) can overload the device or generate a massive number of alerts. Any IDS should be set to logging only when performing a scan through it. The IPS should be disabled, since it may try to protect the asset by interfering with the scan, which will lead to inaccurate scanning results. It may be desirable to disable an IDS or IPS for network traffic generated by a scanner.

Having the scanner send packets through a Network Address Translation (NAT) device may cause the scan to slow down, since the device may only be able to handle a limited number of packets per second.

In each of these cases, a viable solution would be to place a scanner on either side of the intervening device to maximize bandwidth and minimize latency.

VPNs

Scanning across VPNs can also slow things down, regardless of bandwidth. The problem is the workload associated with connection attempts, which turns VPNs into bottlenecks. As a scanner transmits packets within a local VPN endpoint, this VPN must intercept and encrypt each packet, and the remote VPN endpoint must decrypt each packet. Placing a scanner on either side of the VPN tunnel eliminates this type of bottlenecks, especially for VPNs with many assets.

Sub Networks

The division of a network into sub networks is often a matter of security. Communication between sub networks may be severely restricted, resulting in slower scans. Scanning across sub networks can be frustrating because they are often separated by firewalls or have Access Control Lists (ACLs) that limit which entities can contact internal assets. For both security and performance reasons, assigning a scan engine to each sub network is a best practice.

Perimeter Networks (DMZ)

Perimeter networks, which typically include web servers, e-mail servers, and proxy servers, are "out in the open" which makes them especially attractive to hackers. Because there are so many possible points of attack, it is a good idea to scan this network both from the inside and outside. The OUTSCAN service can provide a view from the outside looking in and an internal scanner can provide an interior view of the DMZ.

ACL

ACL can create divisions within a network by restricting the availability of certain network assets. Within a certain address space, such as 10.0.0.1/254, the HIAB may only be able to communicate with 10 assets because the other assets are restricted by an ACL. If modifying the ACL is not an option, it may be a good idea to assign a scanner to ACL protected assets.

WANs and Remote Asset Locations

Sometimes an asset inventory is distributed over a great distance. Attempting to scan geographically distant assets across a Wide Area Network (WAN) can tax limited bandwidth. A scanner deployed near remote assets can collect scan data and transfer that data to a more centrally located database. It is less taxing on network resources to perform scans locally.

Other factors that might warrant a scanner include routers, portals, third-party-hosted assets, outsourced e-mail, and virtual local-area networks.

4.2 Understanding Scanners

Another way to project how many scan engines you need is by counting the total number of assets that you intend to scan and how quickly you need to scan them. The following calculation will give you a general idea. Keep in mind that average numbers for simultaneous scans and total scan hours will vary depending on the types of assets you are scanning and the scan template you are using.

In this example, you may wish to scan a range of 600 IP addresses within 6 hours. A scan engine can run approximately 50 simultaneous scans. Each scan of a live asset can take up to two hours or more, depending on conditions mentioned in the preceding paragraph. If you multiply 600 assets by 2 hours of scanning for each asset, the result is 1200 total scan engine hours.

If you then divide 1200 with 50 you will get 24 scan hours. Divide this with your preferred scanning time and you will get the number of scanners that may be required to have to perform the scanning within that time frame. In this case, it will be 4 scanners just to scan those 600 IPs within 6 hours. But please keep in mind that this is based on an average time of 2 hours to scan a target. If this is not the case, you need to recalculate how many scanners are required to meet your goal. The HIAB solution can always be extended afterwards if you notice that the scanning can't be achieved within the required time.

Having more scanners potentially means faster scanning. However, certain constraints may affect how quickly you can expect to complete a scan job. Bandwidth often is the biggest issue, as faster scanning requires more bandwidth. If you have limited bandwidth, you will have to allow for wider scan windows.

5 Setting Up HIAB and Getting Started

5.1 Understanding Deployment Options

The HIAB can either be a scheduler or a scanner. The scanner acts as a terminal that only perform scanning based upon requests from the scheduler. The scheduler can act as both by default and can also be set up to have the OUTSCAN service as a scanner. This allows you to perform external scanning without the use of an additional scanner that must be placed outside of your network perimeter.

The different ways to install the HIAB solution address different business scenarios and production environments. You may find one of these to be similar to yours.

5.1.1 Small Business

The owner of a single, small retail store has a network of 30 to 40 workstations and need to ensure that they are PCI compliant. The assets include file servers, data servers, registers, and administrative computers. They are all located in the same building. A single HIAB is sufficient in this scenario.

5.1.2 Mid-size Company with Some Remote Locations

A company has a central office and two remote locations. The main office and the other location have a limited number of assets between them. The other remote location has 100 assets. Network bandwidth is adequate. In this scenario, it makes sense to deploy a scanner within the 100-asset location. The rest of the environment can be scanned from the scheduler.

5.1.3 Global Enterprise with Multiple, Large Remote Locations

A company have its headquarter in one country and locations on several places in the world. Each location has a large number of assets and one or more dedicated scanners. In this situation, it is advisable not to use the scheduler as a scanner since the scheduler will have to manage many scanners and a large amount of data.

5.1.4 Where to Place the HIAB Scheduler

The scheduler can be placed where it is most convenient with regards to network segmentation and administration. The scheduler and scanners communication can be defined as either push or pull, depending on requirements of how the traffic are allowed to flow between the different locations or network segments. It all boils down to how the network rules in the firewall is set up.

If the firewall rules say that a scheduler can only send information to the scanner, but the scanner cannot send anything back, the scheduler need to be set to push. If the scheduler is set to push, you need to manually interact with the scanner through the scheduler. Tasks, such as start a scan or update now from the distribution settings, is then sent to the scanner. It is possible to set up an automatic process for the scan jobs to run without interactions.

If the firewall allows the scanner to send traffic back to the scheduler, the scanner can be set to pull the information. The scanner then frequently asks the scheduler if it has something to do, such as: Updates, scan jobs and so on. It is highly recommended to have the scanners up to date at all time.

***Note**: During the deployment, the scanner needs to be paired with the scheduler before it can be used. This requires that the person who deploys the scanner on-site need to pair with the scheduler using the main account details. The password can be changed afterwards without affecting the pairing.*

5.2 An Example Deployment Plan

Let's return to the example environment table for My Company:

Network Segment	Address Space	# of Assets	Location	Asset Functions
London Sales	10.0.1.0/24	254	Building A Ground level	Workstations
London IT/Administration	10.0.2.0/23	50	Building A Floor 1	Workstations Servers
London Printers	10.0.3.0/24	16	Building A	Printers
London DMZ	172.18.0.0/25	30	Data center	Web server Mail server
Japan Sales	10.1.1.0/24	67	Building 1	Workstations
Japan Development	10.1.2.0/23	34	Building 1 Floor 2	Workstations Servers
Japan Printers	10.1.3.0/25	14	Building 1 Floor 1-2	Printers
Japan DMZ	172.18.1.0/25	21	Building 1 Basement	File server Mail server

The best practice deployment plan looks like this:

The eight groups contain a total of 486 assets. Depending on if you would like to scan them weekly or daily, you need to calculate how many tests you would like to have a license for. In this case, we will go for daily scanning on all targets and that would give us 486 x 365, which is 177,390 scans. If your company does not require daily scanning for certain asset types, then you need to agree on a frequency that will fulfill the company security goals. It is best practice to perform regular discovery scanning to detect any new assets that might have been added to the network without following the proper protocol.

My company should deploy the scheduler and scanner throughout its physical location:

- Building A (London)
- Building 1 (Japan)

Considering the number of targets, if the number of assets in the main (London) office were higher, it might be wise to deploy an additional scanner there to decrease the workload of the scheduler.

The IT or security team should evaluate each of the LAN/WAN connections between these locations for quality and bandwidth availability. The team should also audit these pipes for devices that may prevent successful scanning, such as firewalls, ACLs, IPS, or

IDS. Finally, the team must address any logical separations, like firewalls and ACLs, which may prevent access.

The following table reflects the plan:

Asset	Location
HIAB Scheduler	London – Building A
HIAB Scanner	Japan – Building 1

6 Deployment Checklist

When you are ready to install, configure and run scans, it is a good idea to follow a general sequence. Certain tasks are dependent on others being completed. You will find yourself repeating some of these steps:

1. Deploy HIAB scheduler and scanners
2. Configure the HIAB scheduler
3. Log on to the HIAB scanners
4. Configure the scanners and pair them with the scheduler
5. Log on to the scheduler
6. Create user accounts and assign roles and permissions
7. Create targets and assign them to a scanner
8. Create asset groups
9. Schedule scans based on asset groups
10. Run scans
11. Examine reports
12. Assign remediation tickets to users
13. Re-run scans to verify remediation

7 Required Appliances

To determine how many HIAB appliances are required for your organization, check the following tables:

Number of Targets	Daily Scanning	Weekly Scanning	Monthly Scanning
5000	2	1	1
10000	4	1	1
50000	15	5	1

Number of Separate Networks	Number of Appliances
10	1
50	5

***Note**: The information given above might not reflect the actual number needed for your organization, other factors may have to be taken into consideration when designing your solution.*

8 Recovery Plan

To fully restore the HIAB appliance, you need to regularly back up the stored data. The backup solution can back up a secure copy of the installed data on a remote device with the use of FTP, FTPS, SFTP, CIFS, or NFS.

A standby HIAB appliance may be warranted for your organization’s recovery plan for critical servers. If the recovery plan goes into effect, a standby server can be used to import the latest information and perform limited scans of critical servers.

9 Communication Overview

List of required network connections for: HIAB distributed communication, updating and enrollment, SMTP, WEB UI access, OUTSCAN integration, and SSH admin.

Service	Destination	Port	Protocol	Direction	Description
Remote Support	91.216.32.136	22	TCP	Outbound	Remote assistance channel
Update	91.216.32.142	443, 5000	TCP	Outbound	HIAB Updates for the appliance
	2001:67c:1084:2::142				
	repo.outpost24.com				
Enrollment Rule updates	91.216.32.141	443	TCP	Outbound	Registering HIAB
	2001:67c:1084:2::141				
	outscan.outpost24.com				
External	91.216.32.141	443	TCP	Outbound	External scanning from HIAB
	2001:67c:1084:2::141				
	outscan.outpost24.com				
WEB	<HIAB IP>	443	TCP	Inbound	WEB GUI
Scanner	<HIAB IP>	443	TCP	Inbound Outbound	Communication to scanner depends on Polling enabled or not.
SMTP	<SMTP server>	25	TCP	Outbound	For the HIAB to send emails
DNS	<DNS server>	53	UDP / TCP	Outbound	To resolve host names
SSH	<HIAB IP>	22	TCP	Inbound	To allow remote access to console
Proxy	<PROXY IP>	<proxy port>	TCP	Outbound	To communicate using a proxy server
FTP	<FTP IP>	<ftp port>	TCP	Outbound	

Service	Destination	Port	Protocol	Direction	Description
SCP	<SCP IP>	<scp port>	TCP	Outbound	To perform backup and import
CIFS	<CIFS IP>	<cifs port>	TCP	Outbound	
NFS	<NFS IP>	<nfs port>	TCP	Outbound	

10 Frequently Asked Questions

How does the scheduler know which scanner to use?

When adding targets manually in *Target Management*, you can set the scanner for each target. When running discovery scans, you can choose which scanner to use for the discovery, and the targets added from the discovery use that scanner. This can later be changed manually in *Target Management*.

If a scanner is not performing, is this reflected in the way the scheduler distributes the next set of targets?

No. Since which scanner to use is an attribute of the target, they can not be distributed to different scanners.