Outpost24

Vulnerability Management made easy

MSSP OUTSCAN

System Requirements and Prerequisites

Version: 1.8
2019-03-15

Table of Contents

About This Document

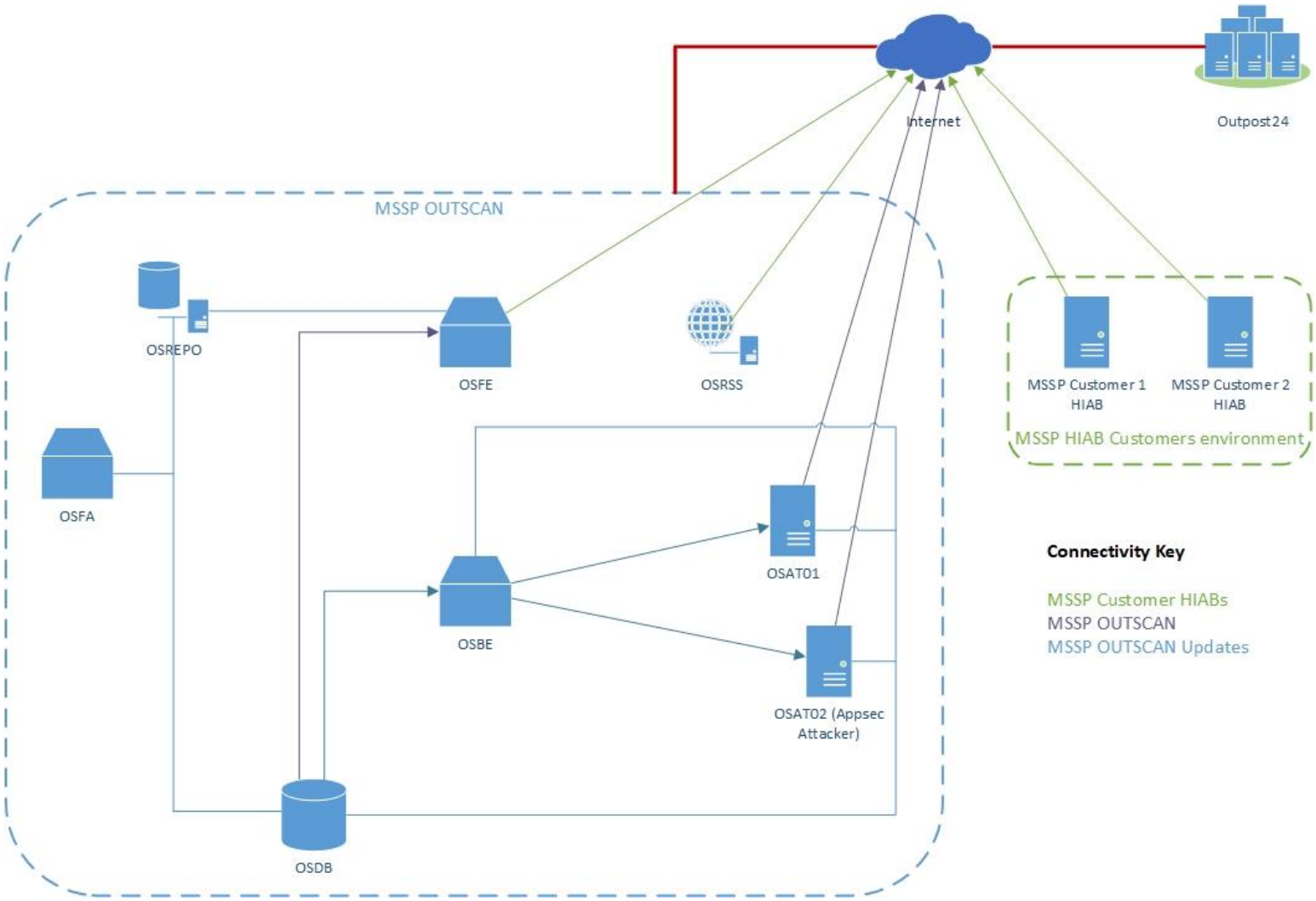
The purpose of this document is to provide an overview of the recommended MSSP setup and its prerequisites.

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

Copyright

Trademark

1 MSSP OUTSCAN Architecture Overview



2 Recommended Machine Specifications

Microsoft Setup	O24 Name	Number	Description
Virtual Machine 1	OSAT	2+	2 B2MS (2 vCPU(s), 8 GB RAM) x 730 Hours; Linux – CentOS; 1 managed OS disk– S30, 100,000 transaction units
Virtual Machine 2	OSFE	1	1 B2MS (2 vCPU(s), 8 GB RAM) x 730 Hours; Linux – CentOS; 1 managed OS disk – S30, 100,000 transaction units
Virtual Machine 3	OSREPO	1	1 B2MS (2 vCPU(s), 8 GB RAM) x 730 Hours; Linux – CentOS; 1 managed OS disk – S40, 100,000 transaction units
Virtual Machine 4	OSRSS	1	1 B2MS (2 vCPU(s), 8 GB RAM) x 730 Hours; Linux – CentOS; 1 managed OS disk – S30, 100,000 transaction units
Virtual Machine 5	OSFA	1	1 B2MS (2 vCPU(s), 8 GB RAM) x 730 Hours; Linux – CentOS; 1 managed OS disk – S30, 100,000 transaction units
Virtual Machine 6	OSBE	1	1 B2MS (2 vCPU(s), 8 GB RAM) x 730 Hours; Linux – CentOS; 1 managed OS disk – S30, 100,000 transaction units
Azure Database for PostgreSQL	OSDB		Basic, Gen 5, 2 vCores, 500GB storage, Backup Retention 14 days.

The disk requirements of the VM's of the Outpost24 devices – recommended is around 150-200GB of disc space on the devices if possible. They have a locked down OS running so that isn't using much of the disk in any way and most of the disk required is due to logging and/or temporary files (during updates).

The database should have a minimal requirement already in the documentation.

The devices can be resized (increased) afterwards so there are no wrong number, just less convenient. They can also be provisioned in a thin configuration if that isn't restricted by any company policy/deployment requirements on your side.

Full root access to the above machines is required for installation, maintenance and update purposes. This would only be used by Outpost24 personnel with the appropriate security clearance.

Functional Blocks: All machines must be configured with Static IP Addresses.

OSAT: OUTSCAN Attacker: Multiple instances used to perform scanning. It is not recommended to run these devices over stateful inspection firewalls, as they generate a large amount of traffic. It is preferable, in the case of servers having different network interfaces (such as for management only, and for exposing its services), to place the

interfaces exposing its services externally (there can be multiple instances of this, depending on network scalability).
***Note**: The Attacker should have outbound access but should not be accessible from the Internet.*

OSFE: OUTSCAN Frontend: The external facing device where the MSSP can access the service which is outscan.mssp.com.

OSREPO: OUTSCAN Repository: An update repository for deployed HIAB devices, provided by the MSSP OUTSCAN deployment. It contains the packages required for all updates.

OSRSS: Remote Support Server: This allows SOC members to access HIAB installations where administrators have enabled the feature and supplied the correct encryption key to the OUTSCAN personnel.
***Note**: Only available if the customer allows the traffic on port 22, enables the service in the HIAB, and provides the key. The access given is a remote shell to the HIAB installation where manual troubleshooting can be conducted.*

OSFA: OUTSCAN Frontend Administration: The optional external page where MSSP staff members will access the licensing, customer account, and other management features.

OSBE: OUTSCAN Backend: Background services required to run scan scheduling, execution, reporting and notifications.

OSDB: OUTSCAN database: Database instance for supporting the OUTSCAN installation.

3 Recommended Naming Convention

***Note**: The machines above must be configured with the following case sensitive naming convention:*

Server	Name
Repository Server	osrepo01
Frontend	osfe01
Backend	osbe01
Front Admin	osfa01
Attackers (normal)	osat01
Attackers (scale)	osat02
Remote Customer Support Server	osrs01
Database Servers (if not doing database as a service)	osdb01 (when using multiple servers, increment to 02, 03 etc.)

4 Operating System for Base Machines 1-6

Outpost24 will provide you with a virtual disk image for the implementation. The image is compatible with the environment and is requested by email to: msspsupport@outpost24.com

The image is then accessed through an SFTP server with credentials provided by Outpost24.

5 Certificates Required

Two certificates are required for the URL's to be used, one for the MSSP portal (outscan.mssp.com) and one for the admin portal (outscan-admin.mssp.com).

The certificate for the Frontend machine should be configured so that it is valid for the domain where it is being deployed.

6 Other Services and Configurations

Mail: Required to send email notifications. If allowed, these can be sent from the OSBE, or alternatively, an SMTP relay server must be provided and configured.

Please provide a reply email address that will be used for OUTSCAN notifications.

Example:
`noreply@example.com`

Backup: The OSDB instance is required to be backed up regularly.

VPN/Jump Host or other means: Any MSSP-approved access solution that can be used by Outpost24 to reach the infrastructure for Configuration and Maintenance (Root Access).

DNS: Required to look up Host Names added into the system against a Name Server. outscan_domain: The domain name for this instance of the MSSP OUTSCAN.

DNS entries for the following: (either using CNAME or A)

Name	Pointing To
outscan	osfe01
outscanattachment	osfe01
admin	osfa01
adminattachment	osfa01
consultancy	osfa01

***Note**: The above names are intended as an example, providing they are pointing to the recommendations above, the naming convention is up to the MSSP.*

NTP: Required for time synchronization for easier correlation and auditing of time in the Log Files. This is a requirement for the TOTP 2 factor authentication (a time-based one-time password).

7 Maintenance

- Rule updates are performed by Outpost24 periodically, as new rules are created by the Vulnerability Research team. Full root access to all machines for security-cleared O24 personnel is required for certain updates and maintenance.

8 Scalability

The average scan time may be assumed to be ~35 minutes per target which gives an indication of the capacity of the recommended deployment configuration. This value is based on successful, external OUTSCAN scans from 2018 with Normal scan policy, originating from attackers with the following parameters:

CPU: Intel(R) Xeon(R) CPU E3-1220 v5 @ 3.00GHz
Intel(R) Xeon(R) CPU E3-1240 v5 @ 3.50GHz
Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz
(or equivalent)

Memory: 8GB RAM

Disk: Standard SSD

Net/io: 20kpps

- Concurrent scans/worker: 50
- Factor: ~1,7
- Scans/hour: ~85
- Scans/day: ~2000
- Scans/week: ~14000

Some service degradation may arise if the concurrent scans/worker threshold value is significantly increased. Scalability is achieved in the first place by increasing the number of Attackers (OSAT).

***NOTE**: The scan time is affected by multiple factors associated with the specifications of the setup, parameters of the scanned target and the scan configuration itself:*

- *Network latency (higher latency = longer scan time)*
- *Network bandwidth (lower bandwidth = longer scan time)*
- *Overall performance of the worker machines the scans are originating from (lower performance = longer scan time)*
- *Overall performance of the target (lower performance = longer scan time)*
- *Number of open ports (more ports = longer scan time)*
- *Type of listening services (more HTTP services = longer scan time)*
- *Enabled vulnerability checks (more enabled checks = longer scan time)*
- *Configured target authentication (authenticated scans = longer scan time)*

Additionally, Outpost24 scanning solutions are highly adaptive to the scanned asset (including backoff mechanisms) and therefore the scan time of a single target might be significantly volatile between scan occurrences. The average scan time provided above might not be representative of the environment of the MSSP and should not be treated as such.

9 Nat Configurations Required

Below is a list of all configurations required:

- Base machine 1-6 and the database (OSDB) internally requires the firewall rules as described in the table below.
- The OUTSCAN Frontend machine (OSFE) must be accessible publicly via port 443.
- The OUTSCAN Frontend Administration machine (OSFA) must be accessible to administrators via port 443.
- The Attackers (OSAT) require access to the Public IP scanning range or IP but should not be accessible from the Internet.
- The Remote Support Server (OSRSS) must be accessible from port 2222,2022,22 for your support team.
- All base machines should be accessible on port 22 for Maintenance.
- The Repository (OSREPO) must be accessible via 443 by both HIABs and OUTSCAN nodes externally for HIABs to pull updates.
- The OSDB needs to be accessed via 5432 from OSBE, OSFA and OSFE

Host	Port
OSFE, OSFA, OSBE, OSREPO	443,22,5432
OSRSS	2222,2022,22
OSBE	22,8443
OSDB	5432

10 Configuration Information Required

Outpost24 requires the configuration information specified in Appendix 1 prior to installation of the OUTSCAN platform. Please complete the form and return as an encrypted file to: msspsupport@outpost24.com.