MORPHISEC
Moving Target Defense

Morphisec Unified Threat Prevention Installation Requirements Version 4.5

Morphisec Unified Threat Prevention 4.5, Rev. 1

Published: July 2020

Copyright © 2020 Morphisec Information Security 2014 Ltd. All rights reserved.

This document contains confidential and proprietary information of Morphisec Information Security 2014 Ltd. None of the information contained in this document may be used for any other purpose or disclosed to any third party without the prior written consent of Morphisec Information Security 2014 Ltd.

ABOUT MORPHISEC UNIFIED THREAT PREVENTION

Morphisec provides the only prevention solution based on Moving Target Defense, which prevents the execution of advanced, in-memory attacks. Morphisec shifts the security paradigm to proactive early prevention, and uses the hackers' tactics to beat them at their own game.

Moving Target Defense technology morphs the runtime environment, so authorized code runs safely, while malicious code is blocked and trapped. By preventing attacks before a breach can occur, Morphisec changes security economics, cutting costs while minimizing disruption and damage to organizations.

UTP is extremely lightweight, with no runtime performance penalty or footprint, and does not require updates. It does not generate false positives, nor negatively impact the end user environment.

The Morphisec UTP solution provides its own dashboards for managing Endpoint Protectors, and for viewing alert and attack information. Alerts can also be forwarded to the organizational SIEM.

ABOUT THIS DOCUMENT

This document describes the Morphisec Unified Threat Prevention solution architecture, and outlines the hardware and software requirements for deploying Morphisec UTP.

RELATED DOCUMENTATION

For information on installing the Morphisec Server, see the *Morphisec UTP Server Installation and Administration Guide*.

TABLE OF CONTENTS

ARCHITECTURE

Morphisec Unified Threat Prevention is a multi-tiered, on-premise or SaaS-delivered solution. It comprises the following components:

ENDPOINT PROTECTOR TIER

On each endpoint (physical or virtual Windows machines protected by Morphisec UTP), the following modules run as Windows Local System Services:

MORPHISEC PROTECTOR

Activated at application load time, it protects applications in real-time.

MORPHISEC AGENT

Responsible for communication and alerts. It acts as the Client to the Server tier application.

MORPHISEC NOTIFIER

Responsible for endpoint user notifications.

MORPHISEC WD SERVICE

Retrieves and manages Microsoft Windows Defender AV events. This service is installed only if the WD_INTEGRATION flag is turned on, when installing the protector.

SERVER TIER

The Morphisec Server runs the following modules:

MORPHISEC WEB SERVICES

These services are responsible for:

- Endpoint management:
  - Retrieving Protector information.
  - Managing Protectors.
  - Storing information in the repository for persistence.
- Dashboard services - generating and populating user dashboards.

PostgreSQL

Lightweight database, used to store system user and certificate data.

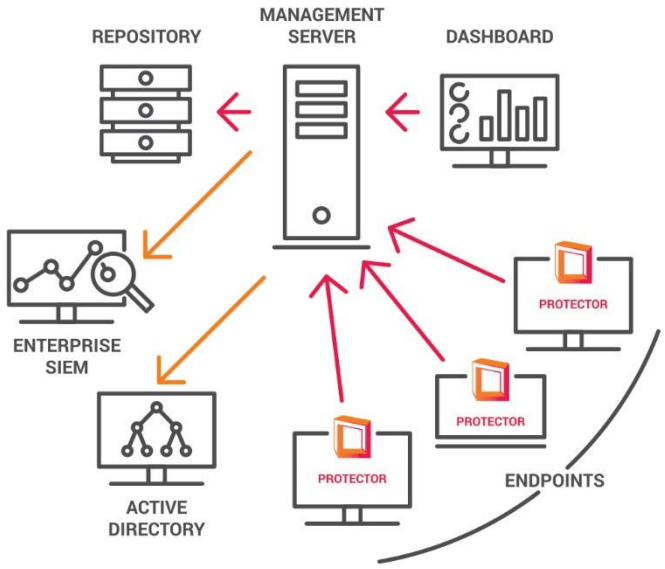
Apache Solr

Search platform for:

- Agent properties and management.
- Attacks - high level, and deep-dive data.

Inter-Tier Communications

Communication between tiers is performed over an SSL connection.



Morphisec System Architecture

SOFTWARE & HARDWARE REQUIREMENTS

ENDPOINT MACHINE

HARDWARE REQUIREMENTS

Hardware as recommended by Microsoft, required to run the software detailed under Software Requirements, below.

SOFTWARE REQUIREMENTS

The Protector must be installed on a physical or virtual image, running one of the following operating systems:

- Microsoft Windows 7 Service Pack 1, 32-bit or 64-bit, with a Windows update that supports SHA-2. *See kb3033929 for additional information*.
- Microsoft Windows 7 Embedded Standard, Embedded Standard SP1
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012/2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

In addition:

- The image must include Microsoft .NET 4.0 or later.
- WMI control must be enabled during installation.

Server Machine

Hardware Requirements

Processors

- Pre-production deployment - use one of the following:
  - 2 Core-2 processors.
  - Quad-core processor with hyper-threading.
- Production deployment - use one of the following:
  - 2 Quad-core processors.
  - 8-core processor with hyper-threading.

Memory and storage

# of Endpoints and Deployment Type	Memory	Disk Size
Pre-Production Deployment		
Up to 100 endpoints	8 GB RAM	10 GB
Production Deployment		
Up to 20000 endpoints	16 GB RAM	250 GB
20001-43000 endpoints	16 GB RAM	500 GB
Over 43000 endpoints	Requires scaling	

Disk

- 7200 RPM
- For high availability
  - Minimum disk array: RAID 1
  - Recommended disk array: RAID 5

SOFTWARE REQUIREMENTS

- The server must be installed with a physical or virtual image, running Microsoft Windows Server 2012 R2 or later.
- WMI control must be enabled during installation.

DEPLOYMENT AND SETUP

PRE-INSTALLATION REQUIREMENTS

The following must be installed on the Morphisec Server machine, prior to installing the Morphisec software. You can pre-install them on your machine/image either prior, or during the installation process, , with the assistance of Morphisec Field Engineering.

- Java SE 8/Amazon Corretto JRE 8
- PostgreSQL version Winx86-64 versions 9.5 and above, where version 11 is recommended

NOTE: A PostgreSQL Admin user account is required to complete the installation process.

NETWORKING REQUIREMENTS

- During installation, you must configure the inbound firewall rules to use an available port.
- If the server machine does not have a fully qualified domain name, it must have a static IP address.
- For an on-premise deployment, if you wish to manage the Protectors using Active Directory, you must have valid credentials for the organizational Active Directory. If your AD is encrypted, you will also need a valid certificate.
- If you want to configure your organization's SSL certificate, do so during the installation process.