



## McAfee Host Intrusion Prevention for Desktops with ePO ("HIPS")

HIPS-8.x

### Quickstart Scope Definition Guidelines

McAfee® Host Intrusion Prevention ("HIPS") is a host-based intrusion detection and prevention system that protects system resources and applications from external and internal attacks. HIPS protects against unauthorized viewing, copying, modifying, and deleting of information and the compromising of system and network resources and applications that store and deliver information. It accomplishes this through an innovative combination of HIPS signatures, network intrusion prevention system signatures, behavioral rules, and firewall rules.

#### New Installation: 2 X MD-QS-SMB-4HR\*

A McAfee Subject Matter Expert ("SME") will remotely configure and deploy HIPS based on McAfee's Best Practices.

- Review server and software requirements
- Install and Configure HIPS from the ePO Server:
  - Install the HIPS Extension
  - Install License
  - Add the HIPS deployment package to the ePO Repository
  - Deploy and enable the HIPS Agent to endpoints (up to 5)\*
  - Create HIPS policies based on your environment (up to 5)\*
- Test the HIPS policies to verify they are working properly.

#### Upgrading: 1 X MD-QS-SMB-4HR\*

McAfee's SME will perform the following tasks:

- Review server and software requirements
- Upgrade and Configure HIPS from the ePO Server:
  - Export current HIPS policies
  - Install the latest HIPS extension
  - Update the HIPS license
  - Add the latest HIPS deployment package to the ePO Repository
  - Install and enable the new HIPS Agent on endpoints (up to 5)\*
  - Import and Modify HIPS policies (up to 5)\*
- Test the HIPS policies to verify proper operation.

#### Optimization: 1 X MD-QS-SMB-4HR\*

McAfee's SME will perform the following tasks:

- Verify the HIPS software functions as expected.
  - HIPS Features:
    - Intrusion prevention
    - Firewall
    - Application blocking

- HIPS Framework:
  - Signature Based IPS
  - Spot and block new vulnerabilities
- HIPS Categories:
  - Known threat
  - Signature threat
  - Unsolicited outbound traffic
- Review current HIPS policies for compliance with McAfee Best Practices (up to 5)\*
- Validate HIPS Policy Assignment functionality.
- Confirm availability of HIPS queries and dashboards.

#### Knowledge Transfer: 1 X MD-QS-SMB-4HR\*

McAfee's SME will perform the following tasks:

- Explain the HIPS features:
  - Intrusion prevention
  - Firewall
  - Application blocking
- Explain the two principal mechanisms that enable HIPS:
  - Signature Based IPS
  - Spot and block new vulnerabilities
- Explain HIPS Categories:
  - Known threat
  - Signature threat
  - Unsolicited outbound traffic
- Explain policy creation and assignment based on the previous uses mentioned (up to 5)\*.
- Review the available HIPS queries and dashboards (up to 5)\*.

### Session Requirements - before getting started: Client's responsibility...

- Functional ePO environment based on McAfee's recommended requirements
- McAfee Agent installed on the servers to be managed by HIPS
- Identify the names of the targeted clients
- List applications to be whitelisted (allow)
- Validate that all endpoints, databases and servers meet McAfee's hardware and software requirements (See Product Guide)
- Validate that all applicable McAfee software licenses have been installed via Client's valid grant number
- Perform necessary backups
- Indicate if there are any outstanding Service Requests/Trouble Tickets opened with McAfee Technical Support

\* Configurations and deployments exceeding these numbers will require additional sessions. Each remote session lasts up to 4.0 hours