FireEye Endpoint Security Tech Preview - Process Guard User Guide

AUGUST 2019

FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) info@fireeye.com | www.FireEye.com

TABLE OF CONTENTS

WELCOME!

Thank you for taking the time to evaluate our latest feature update. FireEye Endpoint Security spent considerable effort on architecting a new approach to rapid feature delivery based upon our investigative findings from our front-line consultants.

TECHNICAL PREVIEW

Technical Previews are an easy way to evaluate Beta-quality features with a meaningful experience, so we can tune the next feature update with your suggestions in mind. Technical Preview is a direct line to our engineering team on what works well, needs to be improved, or enhancements on what would work best for your environment with regards to the feature you are evaluating. Technical Preview gives our engineering team direct to help triage an issue or offer advice on feature enhancements. This enables feedback for our engineering team to immediately work on making the experience better, before it's Generally Available.

Technical Preview features are not a Generally Available solution; therefore, Customer Support can help collect data as needed, but may not be able to dive deeper as these features are still new for them. It is expected that you work with the account team and our FireEye engineering team as you see issues or need to an answer a technical question. Your FireEye account team can provide an introduction to an Endpoint Engineering team lead to better enhance your overall experience.

INTRODUCING MODULES

Modules are part of our Innovation Architecture, as known as the Rapid Delivery experience. Modules can be loaded into the Endpoint Security Console and those features can be delivered directly to an assigned host set of your choice. New policies will be added and any features with detection capabilities will have their results populate into the existing alert workflow.

Modules give flexibility to the FireEye Endpoint Security product line, so our Consultants, family of products, and potential partners can add new capabilities to deliver to their audience. It also offers a tailored experience on how you want to define the agent and its security posture within your technical environment. Modules are not tied to each release, rather they are designed to be used on any release of Endpoint Security Consoles v4.8 or higher. There may be cases where a minimum Endpoint Security Console version is required to support a specific module. Minimum version support will be noted in the Modules release note.

IDEAL EXPERIENCE

To better your experience on Technical Previews, our recommendation is to download a virtual console or use a test console, if you have one, and set up Endpoint Security Server v4.8 in your lab. Deploy agents to your test environments and load the Modules to understand the workflow. Discuss with your team on how a Module should be deployed to your production environment.

You can download a virtual console at no additional cost. Deployed agents do count against your allotment of active nodes. Virtual consoles can run on your local ESX and HyperV infrastructure. Please refer to the FireEye Endpoint datasheet for virtual console requirements.

https://docs.fireeye.com/docs/docs_en/HX/sw/4.8/DG_V/HX_DG_V_4.8_en.pdf

ADMIN MODULE OVERVIEW

The administration module is the management interface for adding new modules. It is expected in future builds that this module will be standard on all deployments. However, for this technical preview, please load the admin module first, so it enables all the subsequent modules to load thereafter. The admin module is used to enable additional modules. It does not offer any additional features. Instructions for installing this module can be found in a later section of this document.

Note: Please install the Admin Module first, or the additional Modules will not work.

PROCESS GUARD OVERVIEW

Process Guard's goal is to prevent attackers from obtaining access to credential data or key material stored within this process to protect endpoints against common credential theft attacks.

Supported OS: Windows 7/2012+

Support Architecture: 64-bit only

Note: Process Guard requires outbound internet access in order to provide telemetry data the FireEye team. Please allow outbound to https://prod.dss3.cis.apps.fireeye.com:443 when using Process Guard so that your HX controller can communicate properly.

If a process requests access to processes with credential data, Process Guard will take action to prevent the request. This action is inclusive of all processes by default. A whitelisting capability is available if this action is incompatible with specific software.

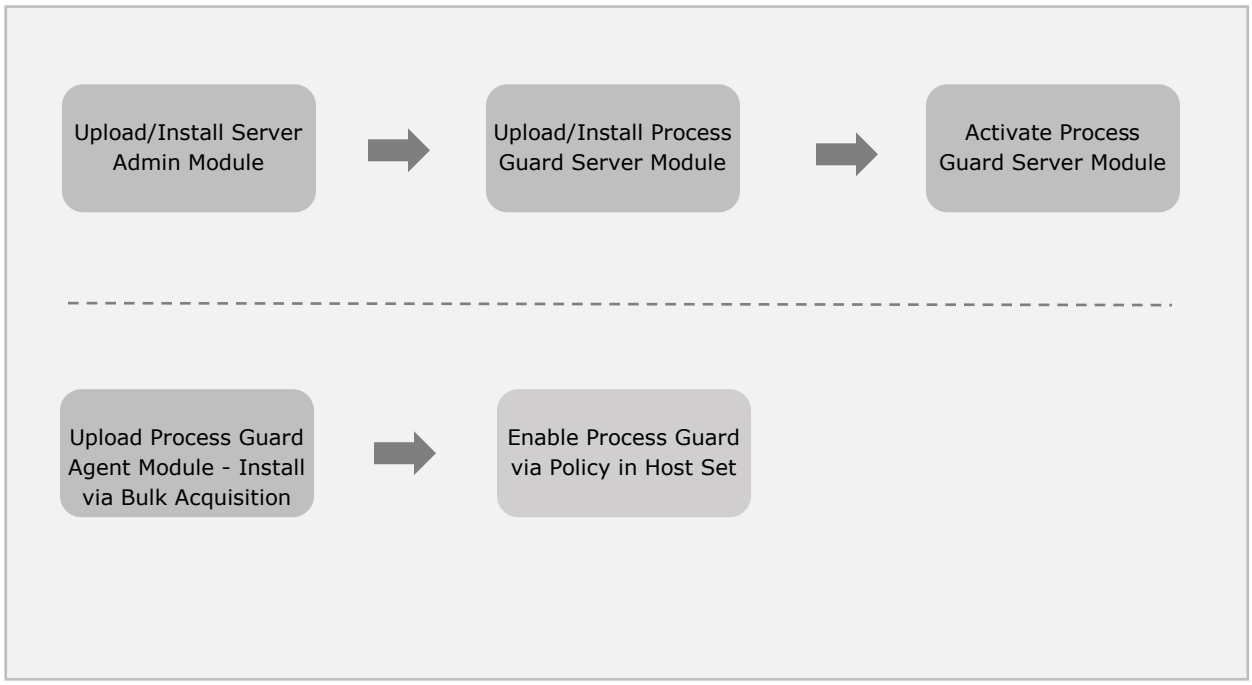
When a process requests access to this data, an event is generated and viewable in the Process Guard Module user interface on your HX controller. Again, by default Process Guard will block all processes from accessing credential data. Events are available in the Process Guard Events page. This page will allow users to troubleshoot any potential compatibility issues.

Process Guard provides a whitelisting feature that allows users to bypass the preventative actions of Process Guard by specifying a full process path. This alleviates any issues with incompatible software that requires full system access.

Note: As with any new software introduction, it is recommended to enable a few hosts at first, so you can monitor the runtime of the endpoint environment and overall compatibility issues, then deploy to a larger host set

MODULE INSTALLATION

PROCESS GUARD INSTALLATION OVERVIEW



HOW TO INSTALL THE ADMIN MODULE

Modules require API access at this time. Verify you have API access with the following commands:

Get a Token:

```
$ curl --insecure 'https://localhost:3000/hx/api/v3/token' -X 'GET' -H
'Accept: application/json' -H 'Authorization: Basic
Y2dhcGk6cEBaaaaaaaa=' -I



HTTP/1.1 204 No Content
Date: Fri, 12 Jul 2019 19:45:18 GMT
Server: Apache/2
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
```

```
Expires: 0
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-FeApi-Token: IM13kYfZg1oznzxGYgGpTsCD7vEAAAAA/53E0evPMmAAAAA=
X-Frame-Options: SameOrigin
```

If a proper username and password is not used, you will receive the following error:

```
HTTP/1.1 401 Unauthorized
```

Use the Token from above:

```
$ curl --insecure 'https://localhost:3000/hx/api/v3/version' -X 'GET'
-H 'Accept: application/json' -H 'X-FeApi-Token:
IM13kYfZg1oznzxGYgGpTsCD7vEAAAAA/53E0evPMmAAAAA='


{"details":[],"route":"/hx/api/v3/version","data":{"version":"2.15.16"
,"msoVersion":"4.8.0","applianceId":"869AD5A457AA","isUpgraded":true,"
intelVersion":"321.101","intelLastUpdateTime":"2019-07-
12T19:27:14Z"},"message":"OK"}
```

Load Your Module:

Load your <module>.cms file into your Endpoint Security Console

NOTE: On the target HX, consider running CLI "show log continuous" to observe module success.

NOTE: If you run WINSCP, then it will default to SFTP. Please remember to verify that you are able to SCP to the Endpoint Security Console.

Run an SCP command to the console with the following path:

```
$ scp module-admin.cms admin@<ip address>:/var/home/root
```

On the Endpoint Security Console, check to see if the module is loaded

```
Jul 12 20:11:58 user1 sshd[79193]: User user1 logged in via ssh2 from
192.168.91.2

Jul 12 20:11:58 user1 scp[79219]: AUDIT: xferlog: user user1: writing
file: '/var/home/root/module-admin.cms' --> success

Jul 12 20:11:58 user1 sshd[79193]: ssh secure channel: Received
disconnect from 192.168.91.2: 11: disconnected by user

Jul 12 20:11:59 user1 pm[4876]: [pm.NOTICE]: Output from
plugin_installer (Plugin Installer) (pid 7329): Verification
successful
```

You can also check by querying the API:

https://<ip_address>:3000/hx/api/services/plugin

Example below

```
User1@A1-G5262BZQ-1BA /cygdrive/c/Users/user1/Documents/Resources/Pre-
Sales/Product/HX/Plugins
```

```
$ curl --insecure 'https://localhost:3000/hx/api/v3/token' -X 'GET' -H
'Accept: application/json' -H 'Authorization: Basic
Y2dhcGk6cEBzc3aaaaa=' -I



HTTP/1.1 204 No Content
Date: Fri, 12 Jul 2019 20:15:25 GMT
Server: Apache/2
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-FeApi-Token: IATQ1lTlqP/0KSuZJHkW+ueWpGcmTR+5tIoY9qFzoeAAAAA=
X-Frame-Options: SameOrigin
```

```
User1@A1-G5262BZQ-1BA /cygdrive/c/Users/user1/Documents/Resources/Pre-
Sales/Product/HX/Plugins
```

```
$ curl --insecure 'https://localhost:3000/hx/api/services/plugin' -X
'GET' -H 'Accept: application/json' -H 'X-FeApi-Token:
IATQ1lTlqP/0KSuZJHkW+ueWpGcmTR+5tIoY9qFzoeAAAAA='

{"data": [{"config_prefix": "/config/module-admin/1.0.0",
"build_date": "2019-06-10T17:24:56", "install_dir":
"/data/hx/plugin_manager/data/pluginDoncg", "display_name": "HX Module
Administration", "uid": "module-admin_5lNpa", "web_component_uris":
{"prod": {"home": {"uri": "/hx/ui/plugins/module-admin_5lNpa/module-
admin/1.0.0/prod/pi-management-plugin-bundle.html", "web_component":
"pi-management-plugin-home"}, "config": {"uri":
"/hx/ui/plugins/module-admin_5lNpa/module-admin/1.0.0/prod/pi-
management-plugin-bundle.html", "web_component": "pi-management-
plugin-config"}}, "dev": {"home": {"uri": "/hx/ui/plugins/module-
admin_5lNpa/module-admin/1.0.0/dev/pi-management-plugin-home.html",
"web_component": "pi-management-plugin-home"}, "config": {"uri":
"/hx/ui/plugins/module-admin_5lNpa/module-admin/1.0.0/dev/pi-
management-plugin-config.html", "web_component": "pi-management-
plugin-config"}}}, "contact": "support@fireeye.com", "enabled": false,
"components_uri": "/plugin/1/component", "supported_platform":
">=4.1", "name": "module-admin", "disable_uri": "/plugin/1/disable",
"source": "git@github1.eng.fireeye.com:HX-Plugins/module-admin.git",
"version": "1.0.0", "enable_uri": "/plugin/1/enable", "plugin_uri":
"/plugin/1", "versions_uri": "/plugin/version?plugin_name=module-
admin", "installed_on": "2019-07-12T20:12:07", "id": 1, "description":
"Module Admin is the Admin UI allowing HX Administrators to Install,
Unistall, Enable and Disable Modules on an HX instance"}]}
```

Note the id from the response

To enable the Module, conduct an HTTP POST on this endpoint. It may also be enabled via the Module-Admin UI as well.

```
/hx/api/services/plugin/{id}/enable
```

Note: These APIs can only be accessed with a header token that can be obtained from hx/api/v3/token

Sample:

```
User1@A1-G5262BZQ-1BA /cygdrive/c/Users/user1/Documents/Resources/Pre-Sales/Product/HX/Plugins

$ curl --insecure 'https://localhost:3000/hx/api/services/plugin/1/enable' -X 'POST' -H 'Accept: application/json' -H 'X-FeApi-Token: IATQ1lTlqP/0KSuZJHkW+ueWpGcmTR+5tIoY9qFzoeAAAAA='
```

Verify by browsing to:

https://localhost:3000/hx/#/plugin/module-admin

Once the CMS file is copied, the Module will auto-install and your console user interface will have a new menu item listed as **PLUGINS.**

HOW TO INSTALL THE PROCESS GUARD SERVER MODULE

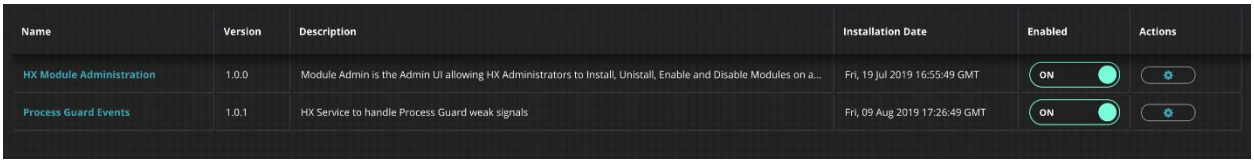
Follow the same steps as in the Admin Module but using the Process Guard file.

```
$ scp process-guard-watcher_X.X.X.cms admin@<ip_address>:/var/home/root
```

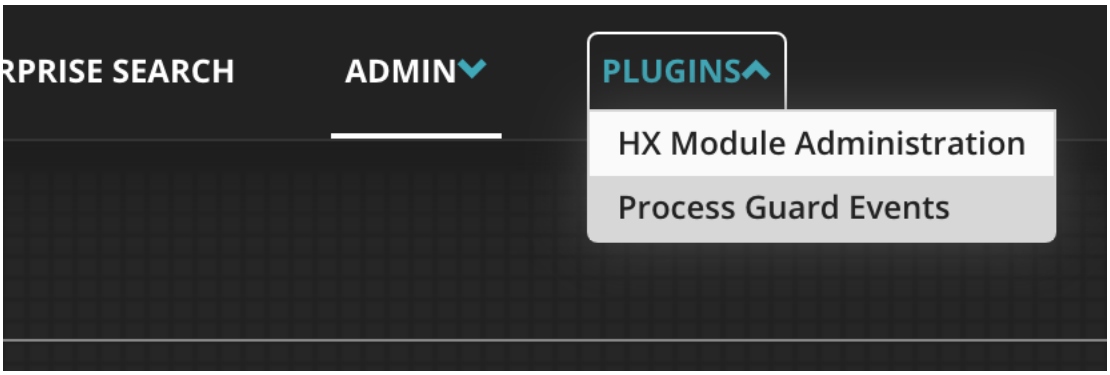
Sample Log:

```
Jul 12 20:21:47 user1 pm[4876]: [pm.NOTICE]: Output from plugin_installer (Plugin Installer) (pid 7329): Verification successful
```

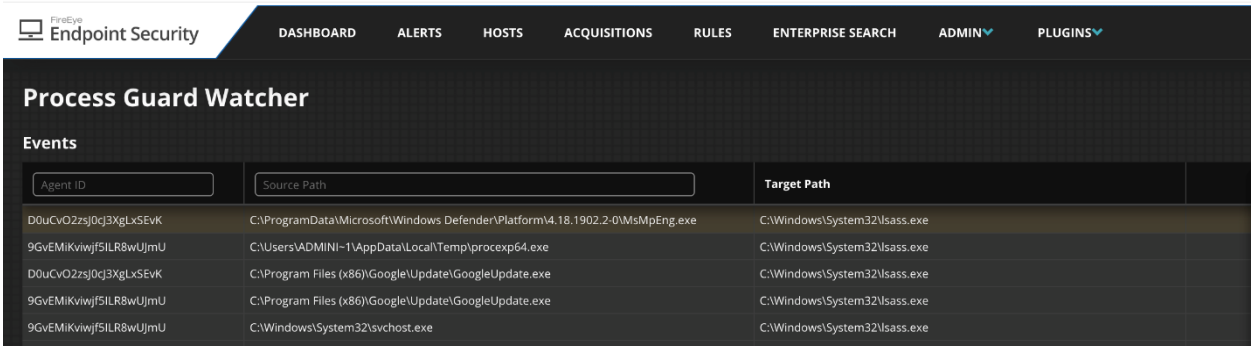
Once the CMS file is copied, the Module will auto-install. Process Guard can be activated through the "PLUGINS" menu drop down. Process Guard will also appear as a policy to assign your host set. The plugin toggle should be moved to enabled and any whitelisted process paths should be added as necessary.



After activating the plugin via the Module Administration page, there should now be a drop down for the "Process Guard Events" as seen below.



From there, simply click the drop down to be taken to the "Process Guard Watcher" page.



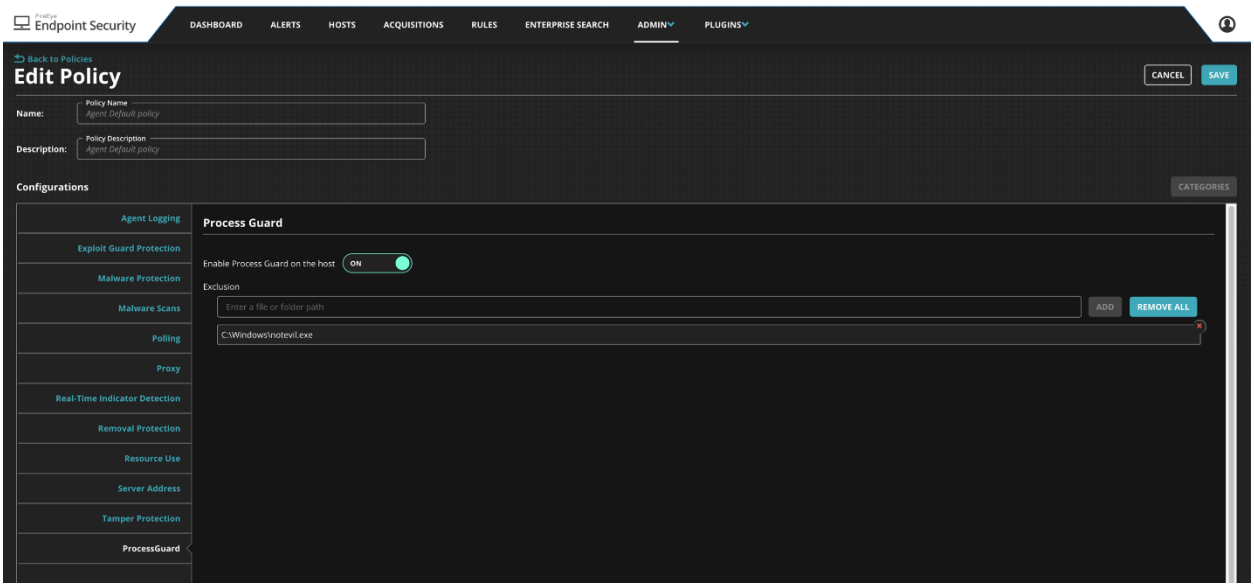
This page will display events observed by the endpoint Process Guard plugin. One thing to keep in mind, these events are not necessarily an indicator of blocking, they are simply to inform of processes that requested access to a process that contains credential data.

If a user wishes to exclude one of these processes from being blocked, simply head over to the Policy config for Process Guard and add the file path to the exclusion list.

HOW TO INSTALL THE PROCESS GUARD AGENT MODULE

Modules are still undergoing additional improvements and will simplify agent feature deployments in the upcoming Endpoint Security v4.8 release. At this time, you must manually install the Process Guard module by using HXTool (recommended) and bulk acquisitions. Please see HXTool's technical documentation for more information on this process. If a reinstall is required, it is recommended to first perform an uninstall (see below) followed by an install.

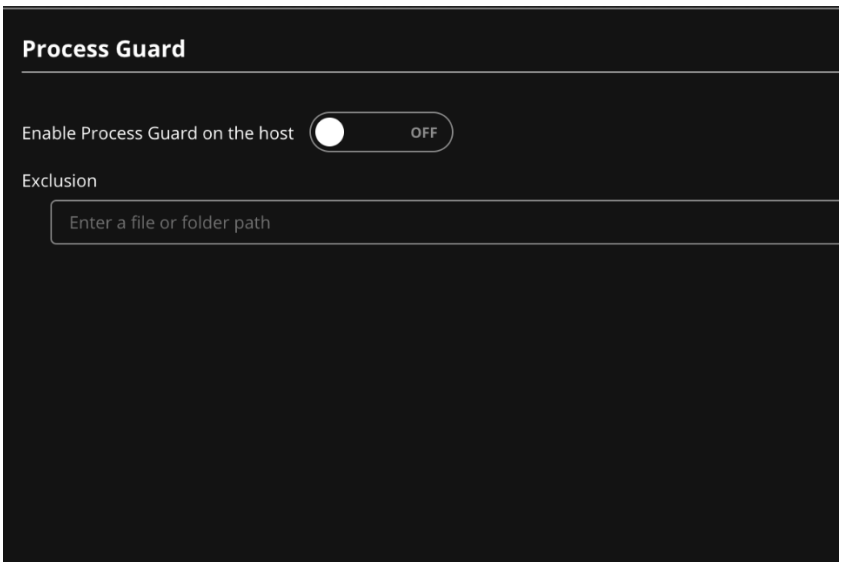
After issuing the bulk acquisition job to install the Process Guard Agent module (process_guard_agent_install.xml), the capability should now be ready to enable on the endpoints via the Policy Configuration settings as seen below.



Setting the "Enable Process Guard on the host" toggle will enable or disable the plugin on the installed endpoints. A process exclusion or "whitelist" feature is also available if a piece of software is found to be incompatible with Process Guard. To whitelist a process, enter the full path to the affected executable and click "Add". This will allow the entered process path to not have any preventative actions taken to it's access requests.

HOW TO UNINSTALL THE PROCESS GUARD AGENT MODULE

The Process Guard agent module can be disabled or uninstalled. To disable the plugin, simply go to the Policy page and toggle the slider to "Off". This will disable Process Guard from running on any endpoint systems. It will not uninstall the module from the endpoint but prevent it from running.

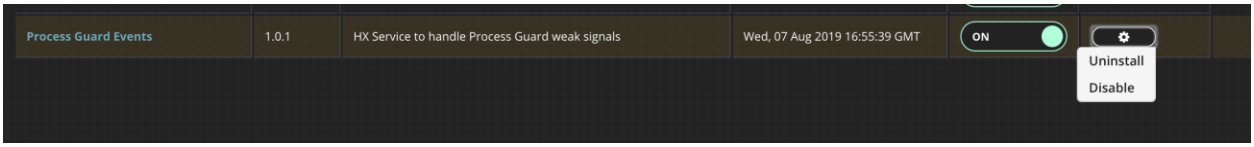


Note: Disabled Process Guard does not remove the files or unload the driver from endpoint systems but will completely disable its functionality. To completely stop and remove all components, please uninstall the plugin from agents via a bulk acquisition using the uninstall script.

If you wish to completely remove Process Guard from hosts, another bulk acquisition job should be run with the supplied process_guard_agent_uninstall.xml script. This will completely remove the module from endpoints. A redeploy will be needed to enable the plugin again.

HOW TO UNINSTALL THE PROCESS GUARD SERVER MODULE

Uninstalling the Process Guard server module can be done via the Module Admin interface. Simply, right click the Process Guard settings and click uninstall. It is recommended that you uninstall the Process Guard agent module first.



RISKS

Process Guard takes preventative actions on all processes by default and this could cause poorly written software to not function properly causing a negative impact on the system.

During internal testing, FireEye identified an issue with a commonly used credential dumping tool. It performed no error checking, and then injected code into the Windows process. Since the tool ignored the fact it encountered an error, it crashed the Windows process and the machine gracefully rebooted itself.

These risks can be mitigated by adding malfunctioning process paths to the exclusion list described above.

SUPPORT

IMPORTANT: FEEDBACK NEEDED

Technical Previews are your chance to shape this feature moving forward. FireEye Endpoint Security expects the Market Place experience to be better over time, so you do not need to install through SCP. However, all workflows suggestions and feature enhancements are welcomed. Please list out the good and the bad, so we can continue to better the overall approach before it becomes Generally Available.

The direct line to our engineering team can be contacted below:

EndpointTechPreview@fireeye.com

NOTE: Please CC your sales account team as well.

SUPPORTABILITY

Customer Support has been notified to pass any comments or issues to the FireEye Endpoint Security Engineering team. They can assist in collecting data as needed, but they are not expected to provide a deeper level of support. Your support path on Process Guard will be on the Endpoint Technical Preview email and account team above.

UPGRADES

Upgrades are not supported for this first iteration of Process Guard. An uninstall and reinstall is needed. The existing data should remain in-tact. FireEye Endpoint Engineering will work with you on expectations and how to better the upgrade experience.

Thank you again for evaluating our latest feature developments.