



McAfee Endpoint Security 10.5

The Why's and How's of Upgrading

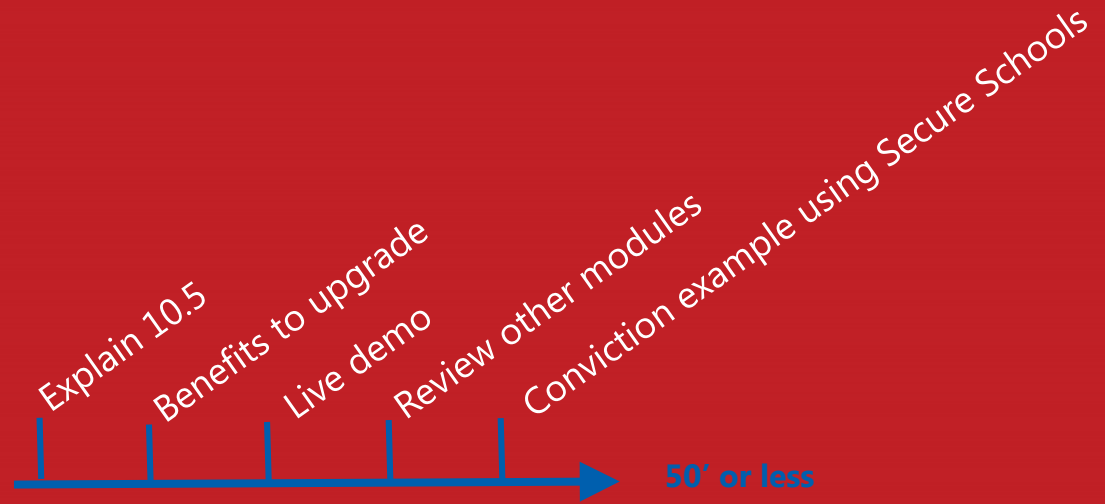
Sarah Taggart | MEEC Account Executive BELLTechlogix

Clayton Mathews | Sales Engineer

Frank Snyder | McAfee Account Executive



Housekeeping and Agenda



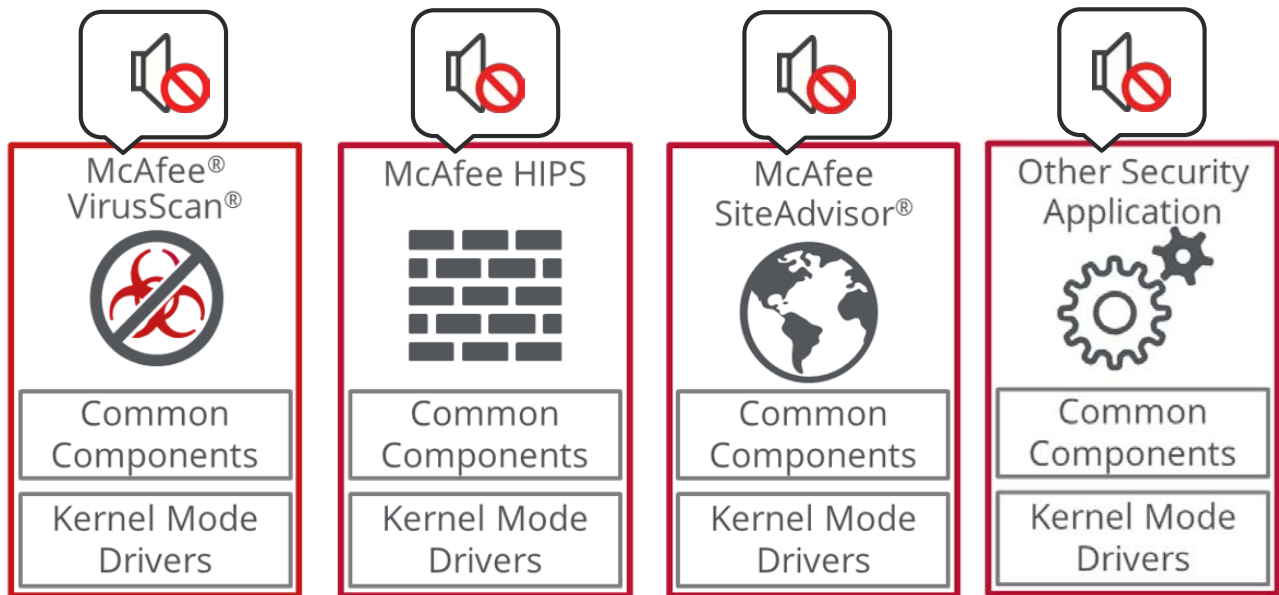
Q & A

Enter any questions in chat or Ask

Please enter your
School in Chat if you
would be so kind

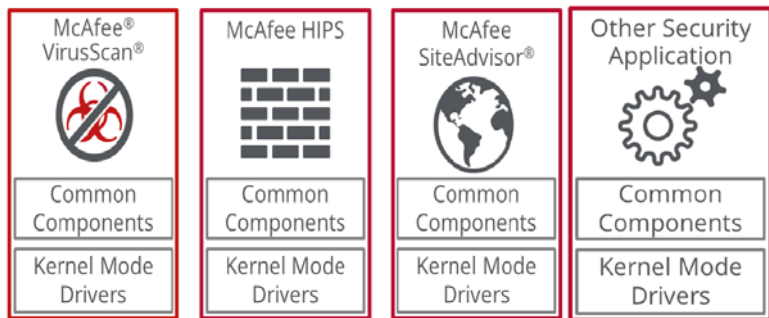
So, what is McAfee Endpoint Security
10.5?

What you have today on the legacy endpoint



ENS 10.5 is Completely Rearchitected

Modular in Nature

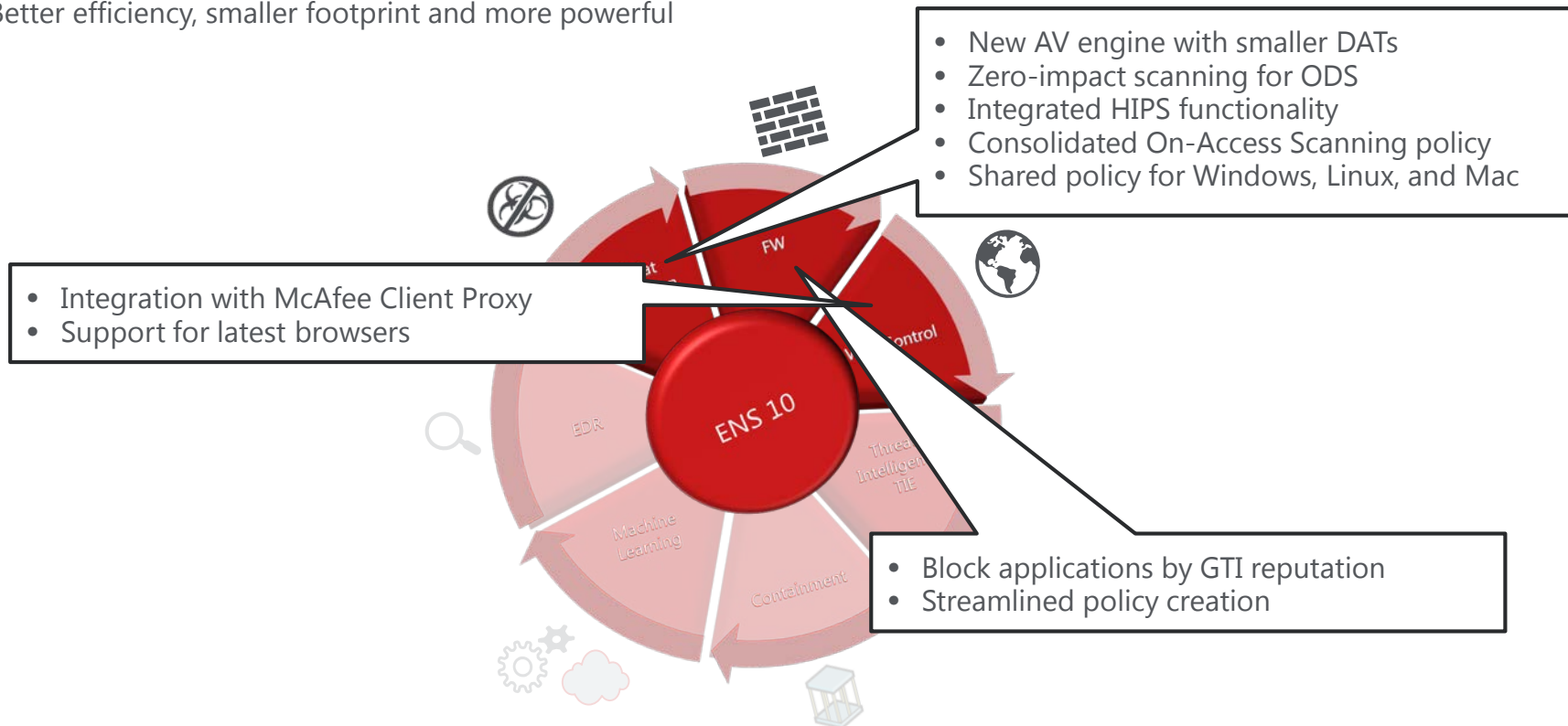


You own this!!!
it is the normal next version

Okay, that's great...
Why should I upgrade?

Why should I upgrade?

Better efficiency, smaller footprint and more powerful



Why Should I Upgrade?

New interface

The screenshot displays the McAfee Endpoint Security console. The top navigation bar includes the McAfee logo, a search bar, and buttons for 'Scan System' and 'Update Now'. The left sidebar contains navigation icons for 'Status', 'Event Log', and 'Quarantine'. The main content area shows a summary of 1030 events and a table of event logs. A specific event is highlighted, with its details expanded in a pop-up window.

Date	Feature	Action taken	Severity
11/9/2017 9:43 AM	Adaptive Threat Protection: Dynamic Application Containment	Released from containment	Warning
11/9/2017 9:36 AM	Adaptive Threat Protection: Dynamic Application Containment	Blocked	Critical

MFESE\afum1 ran MSDCSC.EXE, which tried to access HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM\DISABLEREGISTRYTOOLS, violating the rule "Disabling critical operating system executables", and was blocked. For information about how to respond to this event, see KB85494.

Analyzer / Detector

Analyzer content creation date	8/1/2016 6:11 AM
Analyzer content version	10.5.0000
Product name	McAfee Endpoint Security
Analyzer rule name	Disabling critical operating system executables
Product version	10.5.2.2108
Feature name	Dynamic Application Containment

Threat

Action taken	Block
Threat category	'Registry' class or access
Threat event ID	37279
Threat handled	Yes

- Unified interface for multiple technologies
- Unified event log for easier troubleshooting
- Event log entries "translated into English"

Let's do this!

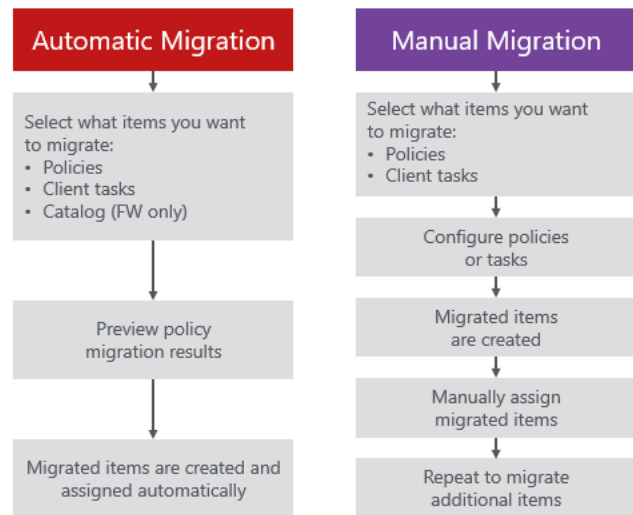
How do I get upgraded?

How do I upgrade?

Tools to upgrade to Endpoint Security 10.5

Endpoint Migration Assistant

Migrates legacy product policies to new Endpoint Security policies. There are two methods of migration; **Manual** and **Automatic**.

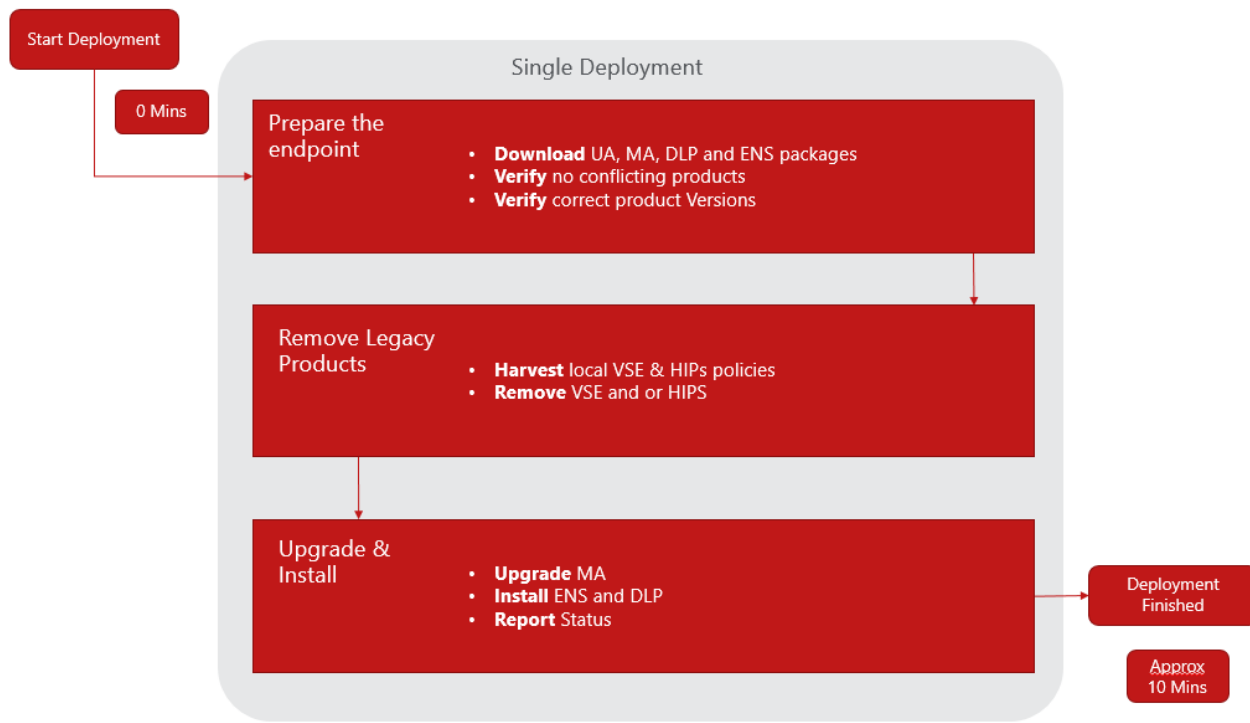


Endpoint Upgrade Assistant

- Analyzes environment to identify systems that meet the requirements to upgrade
- Identifies incompatible products and versions and prescribes required steps to prepare those systems for upgrade
- Tags machine in ePO based on their upgrade readiness
- Automatically upgrades endpoints to Endpoint Security including other solutions (e.g. DLP, Drive Encryption, DXL, etc)
- Tracks progress of endpoint upgrades
- Package builder available for 3rd-party deployment

How do I upgrade?

Endpoint Upgrade Assistant

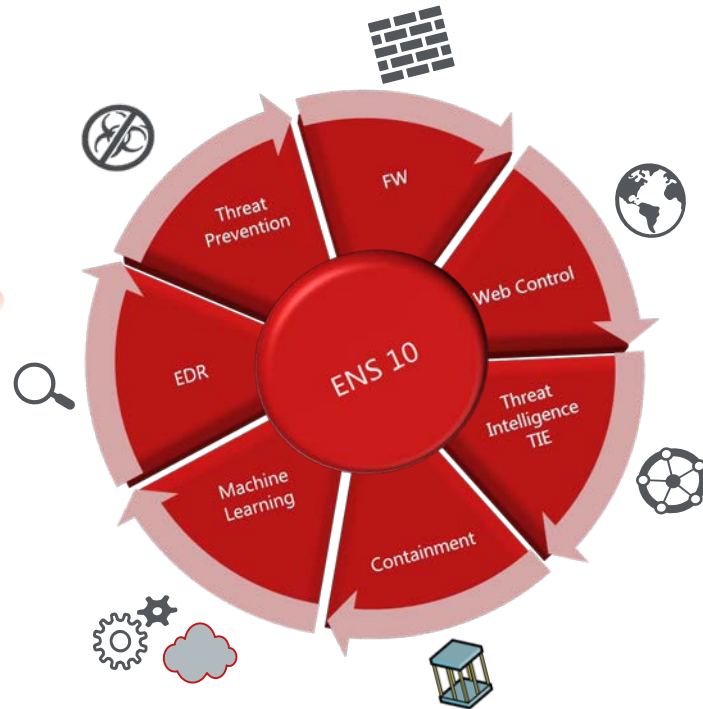


Live Demo

Endpoint Migration Assistant (EMA) and
Endpoint Upgrade Assistant (EUA)

.....you can turn on the "Secure Schools" features Just ask BellTech Logix.....

Secure Schools



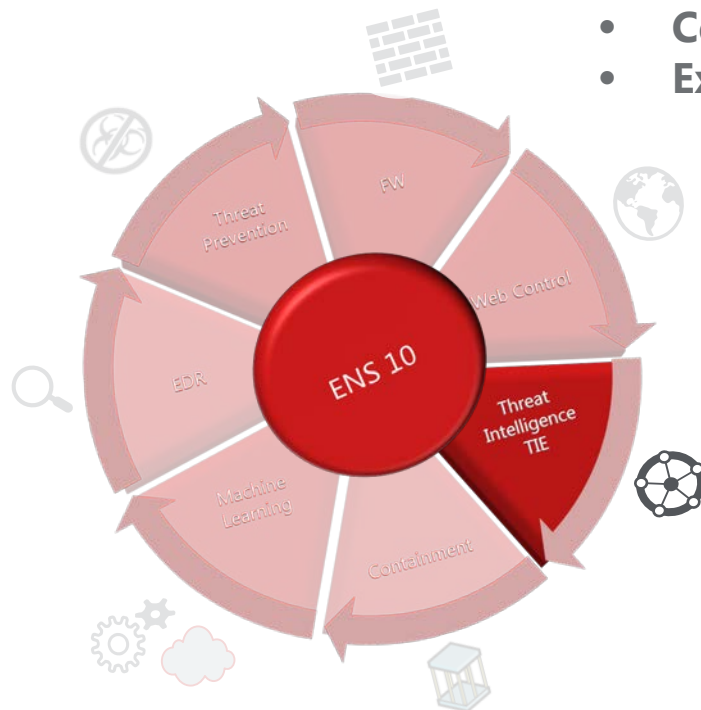
BELL Techlogix

Q & A

Enter any questions in chat

Threat Intelligence Exchange (TIE)

- Local and Global File Reputation
- Local prevalence and age
- Certificate reputation
- External reputation sources

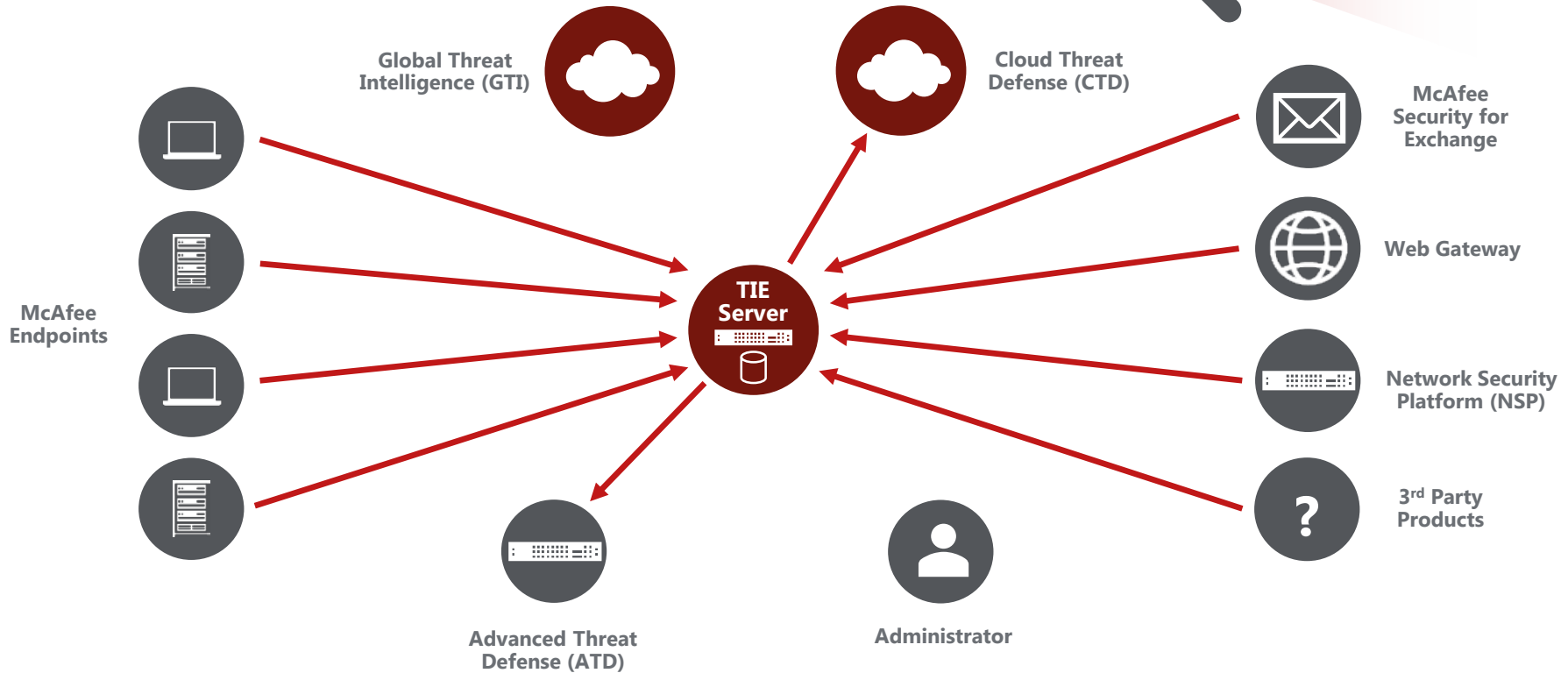


Threat Intelligence Exchange



Enhanced visibility

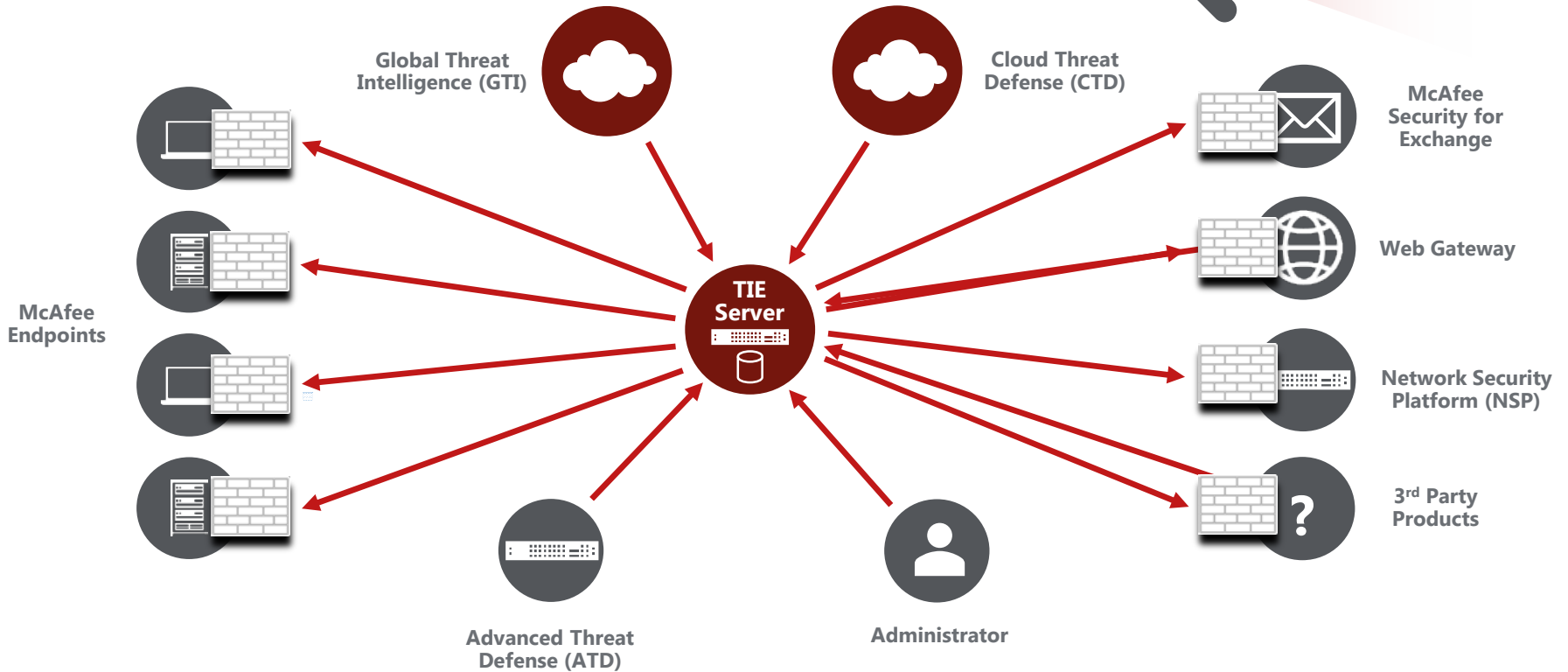
- Provide information on
- Provide analysis



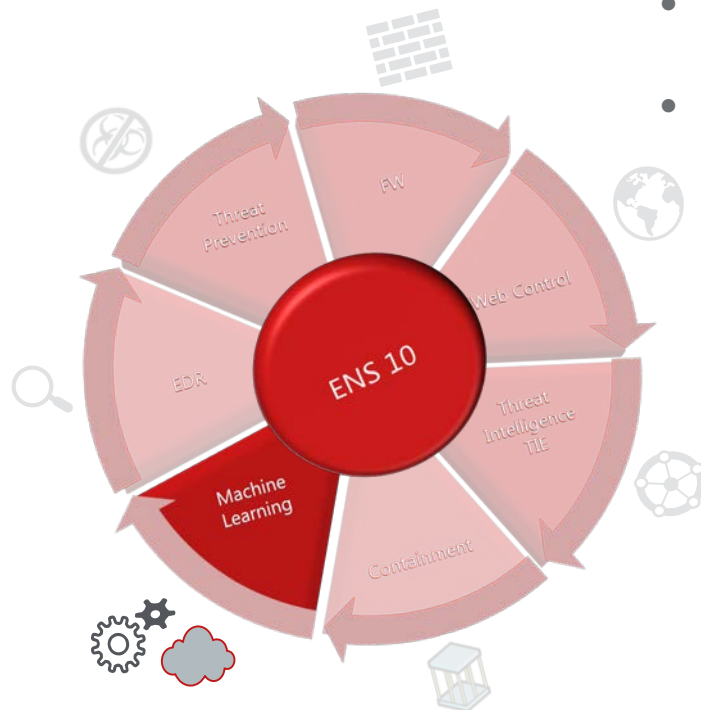
Threat Intelligence Exchange



Alerts and Data



Real Protect – Machine Learning Cloud Behavioral Analysis



- Pre-execution scan using machine learned algorithms
- Post-execution cloud behavioral monitoring
- Cleans up after convicted malware

Features and Feature Vectors in Real Protect

Behavioral Trace

```
        ;  
CreateProcess("c:\user\roaming\fsdfs.exe")  
CreateRegistryKey("HKLM","Software\KeyKill")  
  
SetRegistryValue("InstallDate","213355533")  
        ;  
        ;
```

Features Hash

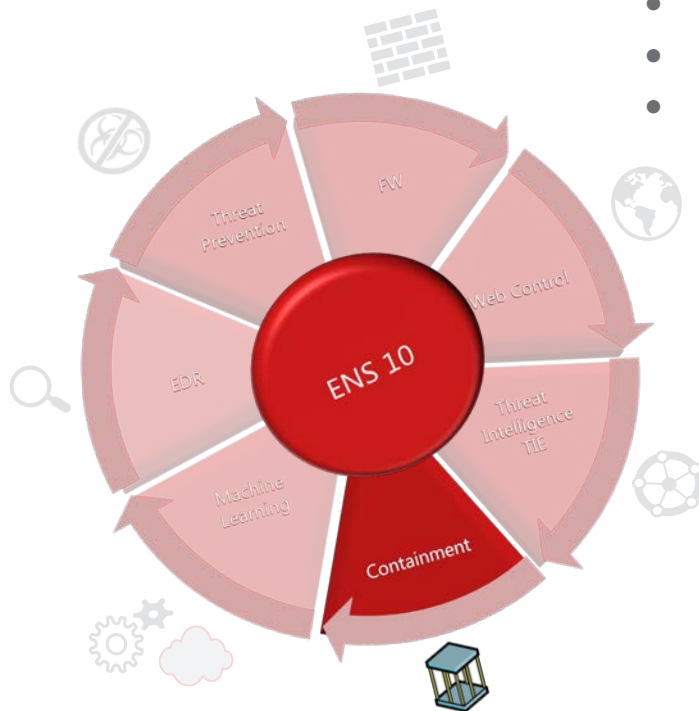
```
➔ AF12ACE76D  
➔ F2A212AC6E  
➔ 22F1CAFFA8  
;  
;
```

Feature Vector

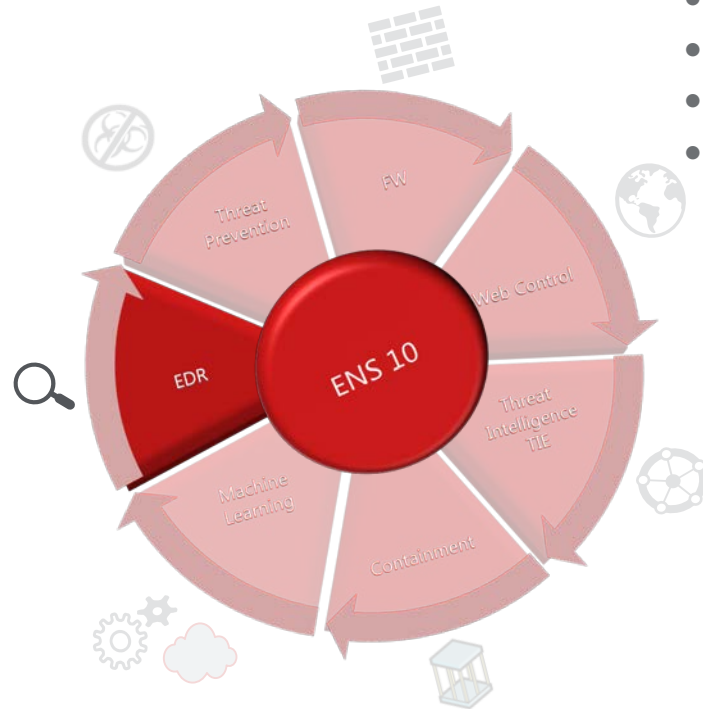
AF12ACE76D	F2A212AC6E	22F1CAFFA8	;	;
------------	------------	------------	---	---

Dynamic Application Containment (DAC)

- Allows unknown files to run
- Constrains unknown processes
- Saves patient zero
- Protection without detection



Endpoint Detect and Response (MAR) Active Response



- Threat Hunter
- Deep forensics
- Continuous monitoring
- Automated capture
- Trace Analysis
- Find dormant threats

What is McAfee Endpoint Security 10?

An example threat scenario



Risk Rating

Known Good

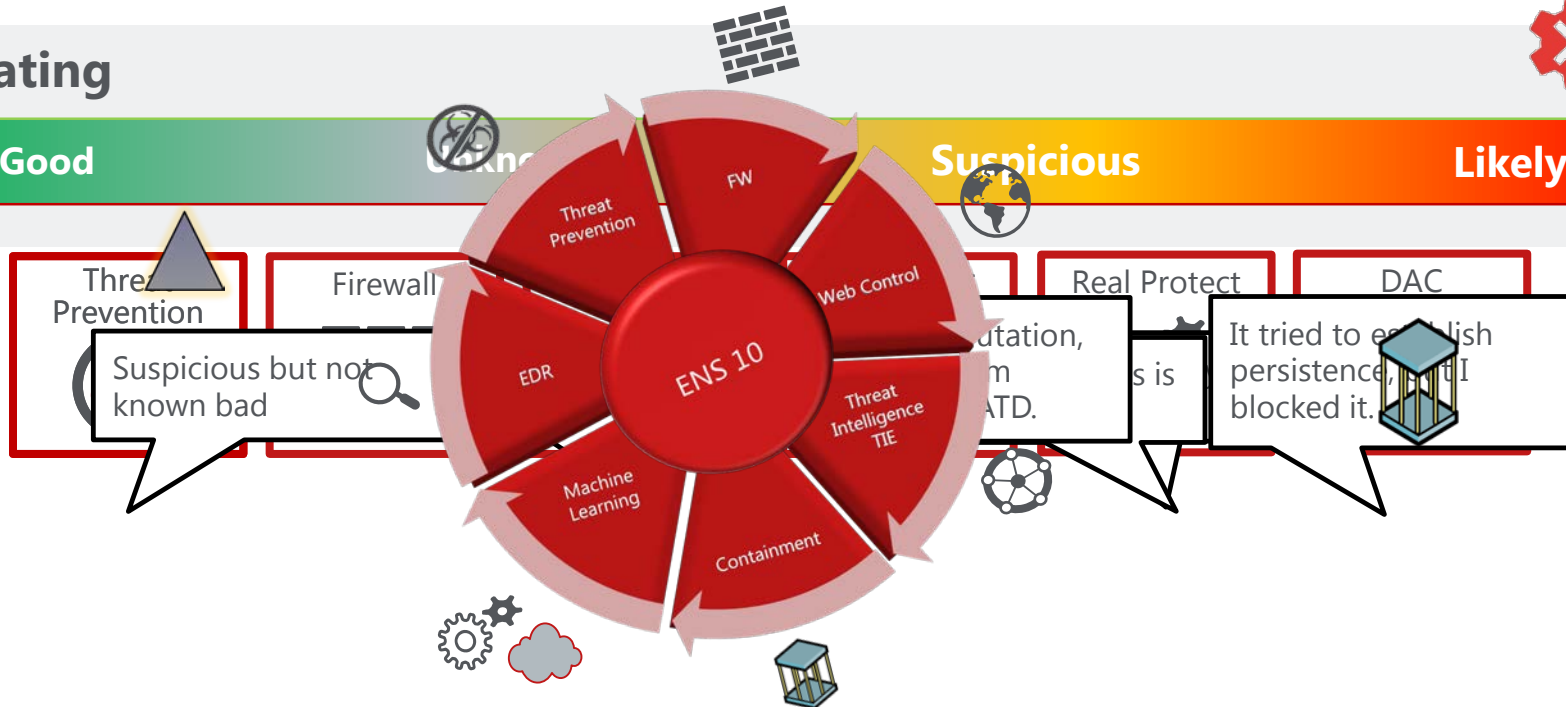


Unknown

Suspicious



Likely Bad



Additional Resources

- McAfee Expert Center (<https://community.mcafee.com/community/business/expertcenter>)
- Sales Engineer “Tech Check” Program
- Endpoint Migration Guide (<https://kc.mcafee.com/corporate/index?page=content&id=pd26801>)
- Endpoint Upgrade Assistant Product Guide (https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27281/en_US/eua_150_pg_0-00_en-us.pdf)



McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee LLC.