FIREEYE ENDPOINT SECURITY (FES)

Provides comprehensive endpoint defense, protecting from threats, detecting attacks, and empowering response.

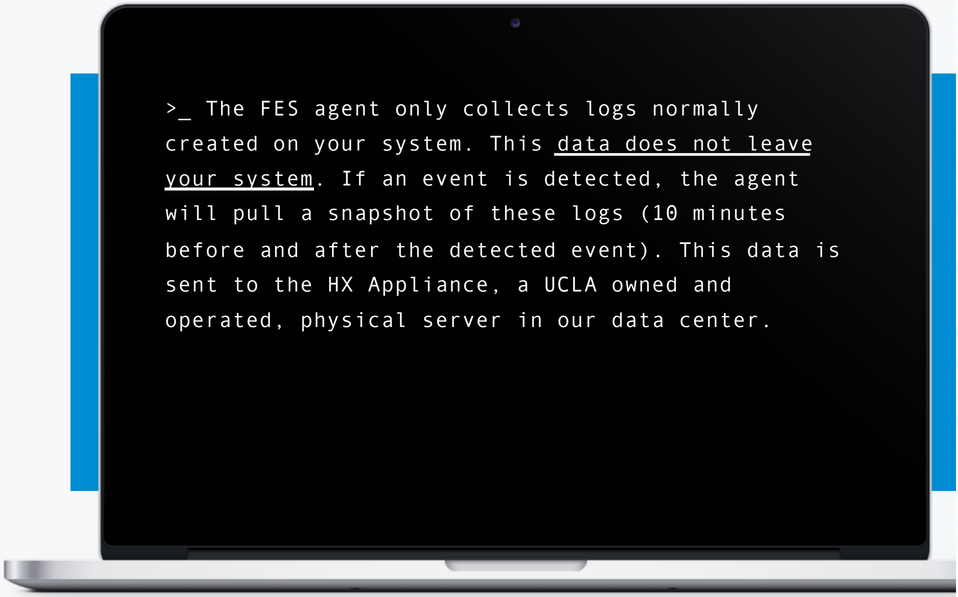
Small piece of software that monitors your system for potential security events

- Protection against known threats with signature protection
- Protection against advanced threats with MalwareGuard
- Protection against exploits with ExploitGuard
- Detection of anomalous behavior with real-time IOC engine

UCLA

DATA COLLECTION: MONITORING

SYSTEM LOGS ARE CREATED DURING NORMAL OPERATION FES MONITORS THESE LOGS FOR SIGNS OF TROUBLE



>_ The FES agent only collects logs normally created on your system. This data does not leave your system. If an event is detected, the agent will pull a snapshot of these logs (10 minutes before and after the detected event). This data is sent to the HX Appliance, a UCLA owned and operated, physical server in our data center.

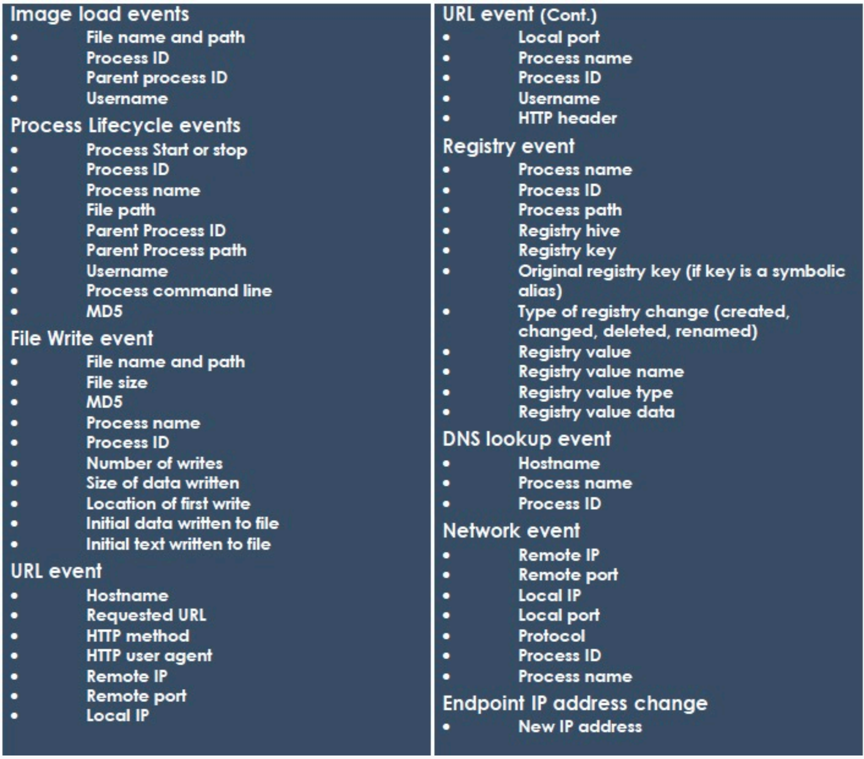


Image load events
- File name and path
- Process ID
- Parent process ID
- Username

Process Lifecycle events
- Process Start or stop
- Process ID
- Process name
- File path
- Parent Process ID
- Parent Process path
- Username
- Process command line
- MD5

File Write event
- File name and path
- File size
- MD5
- Process name
- Process ID
- Number of writes
- Size of data written
- Location of first write
- Initial data written to file
- Initial text written to file

URL event
- Hostname
- Requested URL
- HTTP method
- HTTP user agent
- Remote IP
- Remote port
- Local IP

URL event (Cont.)
- Local port
- Process name
- Process ID
- Username
- HTTP header

Registry event
- Process name
- Process ID
- Process path
- Registry hive
- Registry key
- Original registry key (if key is a symbolic alias)
- Type of registry change (created, changed, deleted, renamed)
- Registry value
- Registry value name
- Registry value type
- Registry value data

DNS lookup event
- Hostname
- Process name
- Process ID

Network event
- Remote IP
- Remote port
- Local IP
- Local port
- Protocol
- Process ID
- Process name

Endpoint IP address change
- New IP address

System logs used to match indicators of compromise

UCLA

WHO HAS ACCESS TO MY DATA

The principle of “least invasive degree of inspection” and “least perusal of content” guides access to security data

USER ENDPOINT

UCLA Staff

The FireEye Agent (FES) collects data that is already being generated on your system and holds it for 1 to 6 days (depending upon space). If a security event is detected, a portion of the data is sent to a UCLA HX Appliance.

UCLA HX APPLIANCE

UCLA Security Staff/FireEye Analysts

Alert data is sent to HX Appliances at UCLA when a security event is triggered (malicious activity is discovered). The data includes details about what was happening on the system at the time of detection, including a window of 10 minutes before and 10 minutes after the event. Data are retained for 1 year.

FIREEYE SECURITY OPERATIONS

FireEye Security Analysts

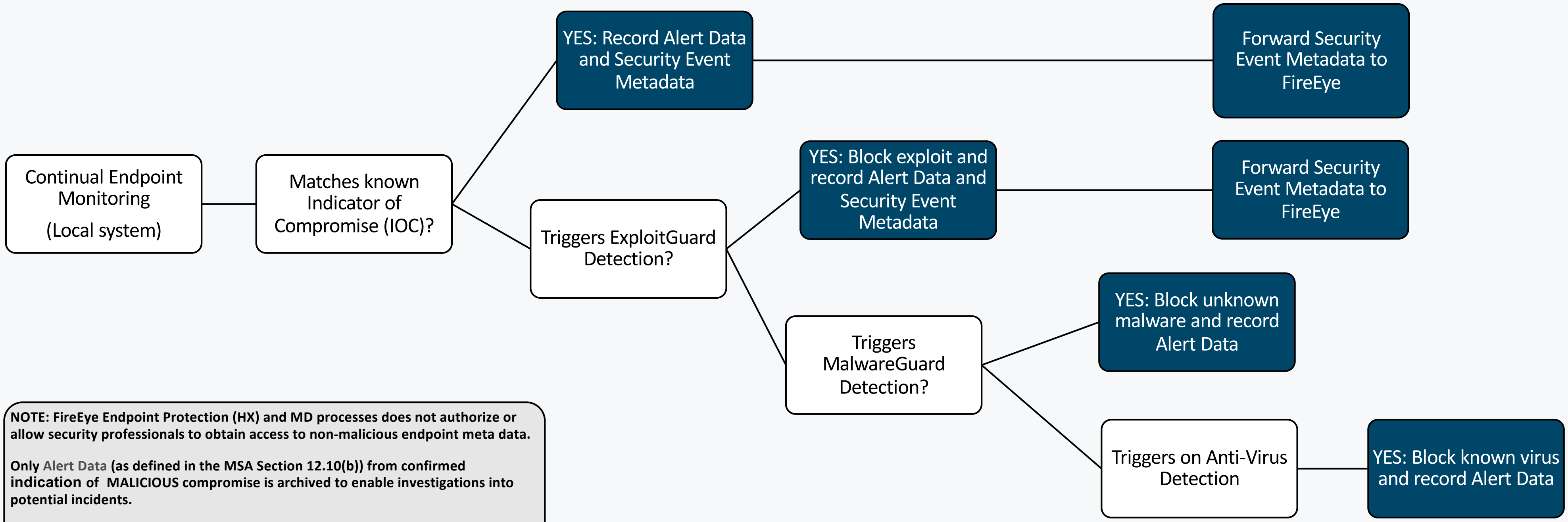
Security Event Metadata (a log of the suspicious activity) is sent to FireEye’s Security Operations Center for analysts to review. Data are retained for 1 year. (*US Datacenters)

Both FireEye Analyst and UCLA Information Security staff must limit data access to the least invasive inspection necessary to resolve the event.

UCLA

WORKFLOW IN THE CONTEXT OF ENDPOINT PROTECTION

The workflow below describes how the FES product works in the context of a security event being detected



Continual Endpoint Monitoring

(Local system)

Matches known Indicator of Compromise (IOC)?

YES: Record Alert Data and Security Event Metadata

Forward Security Event Metadata to FireEye

Triggers ExploitGuard Detection?

YES: Block exploit and record Alert Data and Security Event Metadata

Forward Security Event Metadata to FireEye

Triggers MalwareGuard Detection?

YES: Block unknown malware and record Alert Data

Triggers on Anti-Virus Detection

YES: Block known virus and record Alert Data

NOTE: FireEye Endpoint Protection (HX) and MD processes does not authorize or allow security professionals to obtain access to non-malicious endpoint meta data.

Only Alert Data **(as defined in the MSA Section 12.10(b)) from confirmed indication of MALICIOUS compromise is archived to enable investigations into potential incidents.**

Security Event Metadata **is forwarded to FireEye. This data is used by other FireEye tools in the FireEye TDI solution to identify computers that may have been compromised by the malware identified in the malicious endpoint event.**

UCLA

PRIVACY PROVISIONS AND PROTECTION

Security and privacy are not opposite ends of the spectrum…they can coexist

UCLA MASTER SERVICES AGREEMENT

The MSA has specific privacy provisions to ensure that the Electronic Communications Policy is followed.

LIMITED RETENTION

Data are retained for a limited period of time on all systems.

AUDITABLE LOGS

All actions taken by UCLA Information Security staff and the FireEye team are logged and auditable to ensure privacy is protected consistent with the ECP.

OGC REVIEWED

The UC Office of General Counsel reviewed the agreement with FireEye and confirmed that it is compliant with the Electronic Communications Policy.

QUESTIONS?

If you have questions about the FireEye Endpoint Security (FES) implementation or the FES agent please contact security@ucla.edu.

Also check out our Frequently Asked Questions page at https://www.ociso.ucla.edu/services/fireeye-endpoint-security-antivirus/faqs