CVAH – 2.1 Information

Endgame is a centrally managed endpoint detection and response platform that operates at the earliest and all stages of the attack life cycle. Through a single agent, Endgame instantly detects and stops privilege escalation, defense evasion, malicious persistence, credential access, and propagation.

Endgame automates the hunt for next generation attacks by automating data collection and analysis across all endpoints in seconds, instantly surfacing suspicious artifacts and malicious activity with tailored Tradecraft Analytics that highlight anomalous data. This enables analysts to act with precision to stop the adversary without business disruption.

Endgame provides the following capabilities:

- Accelerated endpoint detection and response
- In-band and out-of-band sensor deployment
- Advanced endpoint protection
- Automated hunting
- Multi-Client Management within an independent server

Endgame's advanced sensor technology allows the analyst choose to install a persistent sensor for long-term protection or a dissolvable sensor for minimal endpoint footprint.

CVAH – 1.2: Administrative Functions

Supported Platforms for Endgame

	Windows	Linux	MacOS	Solaris
Persistent Sensor	✓	✓	✓	✓
Dissolvable Sensor	✓	✓	✗	✓
Modifiable Signatures	✓	✗	✗	✗
In-Band Deployment	✓	✗	✗	✗
Out-of-Band Deployment	✓	✓	✓	✓
Enable Endpoint Protection	✓	✓	✓	✗
Add items to Exception List	✓	✓	✓	✗
Add items to Block List	✓	✗	✗	✗
Artemis Eventing	✓	✓	✓	✗
Create Investigations	✓	✓	✗	✓
Add a Trusted Application	✓	✗	✓	✗

Supported Platform Versions

Windows	Linux	MacOS	Solaris
Windows 7 x86 & x64	RHEL 6.5+ x64	High Sierra (10.13)	Solaris 10 (5.10) SPARC
Windows 8.1 x64	RHEL 7 x64	Mojave (10.14)	
Windows 10 x64 (1507, 1511, 1607)	RHEL 8 x64	Catalina (10.15)	
Windows 10 x64 - Build 1903	Amazon Linux 2	Big Sur (11.0)	
Windows 10 x64 - Build 1703	CentOS 6.5+ x64		
Windows 10 x64 - Build 1709	CentOS 7 x64		
Windows 10 x64 - Build 1803	CentOS 8 x64		
Windows 10 x64 - Build 1809	Ubuntu 14.04 x64		
Windows 10 x64 - Build 1909	Ubuntu 16.04 x64		
Windows 10 x64 - Build 2004	Ubuntu 18.04 x64		
Windows 10 x64 - Build 20H2	Ubuntu 20.04 x64		
Windows Server 2008 R2 x64			
Windows Server 2012 R2 x64			
Windows Server 2016			
Windows Server 2019			

To scan for new endpoints:

1. On the Left Navigation toolbar, click the ENDPOINTS button to display the Endpoint Dashboard.
2. On the Action toolbar, click Discover Endpoints.
3. Complete the requirements in the DISCOVER ENDPOINTS dialog window:
    a. ENTER IP ADDRESS/RANGE: In the text box, type the IP address or IP range to scan. To specify a range of IP addresses, enter a Classless Inter-Domain Routing (CIDR) prefix (e.g., 10.0.6.0/24) or use a hyphen between the first and last addresses (e.g., 192.68.1.4 - 192.68.1.56).
    b. CUSTOM PORT (Optional): By default, Endgame discovers Windows endpoints with port 5985 (WinRM). If you want to override the default port with a non-standard one, enter the location in the text box.
4. Click Start Scan. A "Scan successfully initialized" message appears to confirm the scan has begun.

CVAH – 1.3: Start an Investigation

Start an Investigation

NOTE: You can only create a single investigation for endpoints that run on the same operating system. For example, you cannot create an investigation that contains both Windows and Linux endpoints.

To start an investigation:

1. On the Left Navigation toolbar, click the ENDPOINTS button .
2. On the Action toolbar, select an operating system tab (i.e., Windows, Linux, or Solaris) to filter the Endpoints list.
3. Select the box to the left of each endpoint to include in the investigation.
4. On the Action toolbar, click Create Investigation.
5. Complete the requirements in the START INVESTIGATION dialog window:
    a. Step 1: Create an Investigation Profile or Apply an existing one
    b. Step 2: Launch Your Hunts

Remember: After you create an investigation, each hunt you selected appears as a separate event in the Activity Timeline

CVAH – 1.4 Artemis Queries

Event Type	Data Available	Supported OS
`Process`	A process name, hash, or PID	Windows, Linux MacOS
`Process Lineage`	A historical timeline of when and how a process was created	Windows, Linux MacOS
`Network`	IP, port, and the amount of data transmitted or received in a network connection	Windows, Linux MacOS
`File`	A specific filename	Windows, Linux MacOS
`DNS Information`	The domain name of the corresponding endpoint	Windows
`Security`	Dates and times of when a user logged on or off an endpoint	Windows

Unless specified, with the exception of process lineage search — which requires an IP address — Artemis searches all active endpoints by default. Keep this in mind if you need to search endpoints running on a specific operating system.

The following example is a valid query because it specifies the process name:

search for process calc.exe on all Windows endpoints

To search more than one value for a given entity — which is supported only for active endpoint searches— separate each value with a semi-colon:

search for processes calc.exe; lsass.exe

The following are sample queries NOTE this is not an exhaustive list; see the Endgame documentation for full reference:

A specific process by name or hash
"Show me process.exe on all Windows endpoints"
"Show me process.exe on all Linux endpoints"
"Search for process hash ABC1234567890 on IP 10.1.2.34"

The lineage of a specific process
"Give me the process lineage for badguy.exe on endpoint 10.1.2.34"

Endpoints that communicated to a specific IP
"Search for any endpoint that communicated to IP 10.1.2.34

Endpoints running a specific process sending more than a specific amount of data
"Search network data for process.exe sending more than 100MB"

All processes launched by a specific user
"Search processes created by user johndoe"