# CounterTack Sentinel

## Big Data Endpoint Threat Detection and Response

### Improve Incident Response Workflow and Unknown Threat Management

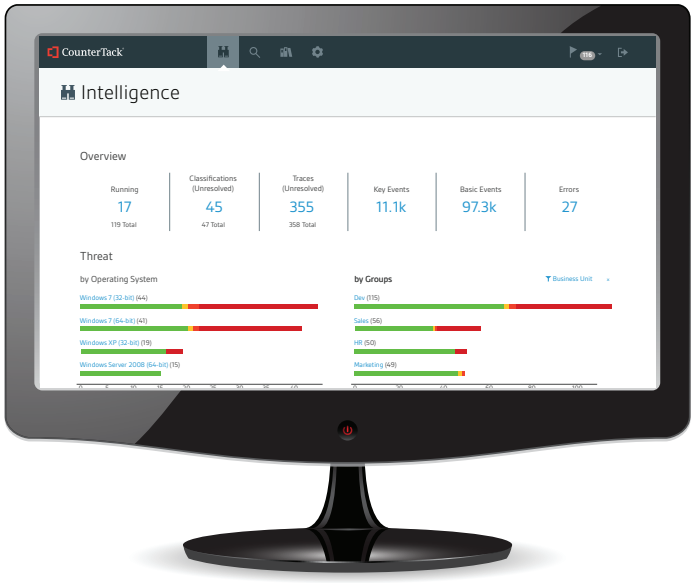
Built on Big Data architecture to counter endpoint attacks at-scale and leveraging tamper-resistant collection technology to capture malicious behavior on workstations and servers, Sentinel dramatically reduces the impact of advanced attacks in real-time, giving teams an opportunity to defend the enterprise before incidents escalate. CounterTack Sentinel is the only EDR (endpoint detection and response) platform that offers teams the flexibility, scale and integration necessary to take back control of security on a global scale, and effectively manage unknown threat detection.

### What Does CounterTack Sentinel Do?

CounterTack Sentinel is an enterprise-class, Big Data EDR platform. It delivers comprehensive attack intelligence to security teams so they can quickly identify and eliminate targeted threats on desktops and servers across sophisticated environments.

CounterTack's endpoint sensor provides low-level visibility into malicious behavior with no user presence and no impact on endpoint performance or stability. CounterTack Sentinel not only sees attacker behavior, it captures all events and processes that unfold as part of that attack. This unprecedented visibility provides real-time context as threats escalate that pose a broader risk to organizations, so teams can make better security decisions.

CounterTack Sentinel combines real-time OS-level surveillance with Big Data analytics, delivering an improved, automated workflow for incident response and threat detection across the enterprise. Sentinel also ships with an advanced set of indicator profiles that automate the prescriptive analysis and remediation of known and unknown threats. The built-in, and learned intelligence over time, characterizes attack techniques in real-time, like antivirus disabling, firewall modification and evasion, where signature-based tools, whitelisting and preventative solutions are blind.




### AT-A-GLANCE

- **Powerful Search Capability:** Identify an interaction on one endpoint, or search across your entire enterprise for specific behaviors
- **Customizable Collection:** Define any interaction and know exactly when and where it occurs in your infrastructure
- **Real-time analysis:** Identify and prioritize threats quickly and accurately for an optimal threat response
- **REST API:** Seamless integration with enterprise security ecosystems allows for import of external indicators into Sentinel
- **Remediation & Containment:** Ability to delete files and terminate processes on-demand, deny endpoints network access, and configure alert messages when a quarantine is activated
- **Visibility into behaviors:** Capture command line arguments for processes to understand immediately when a process is executed, how it was run and what options were enabled
- **Smart Groups:** Define custom groups to automatically correlate threats by business unit and manage endpoints in bulk

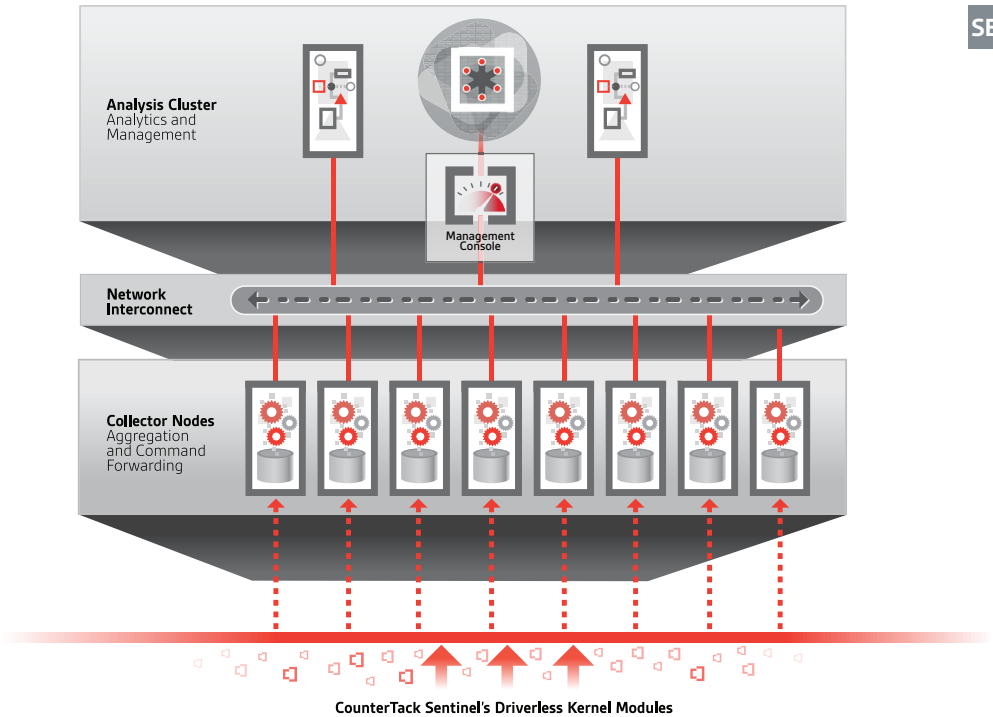
*The CounterTack Sentinel Management Console is built for unprecedented visibility for security teams and responders. Features include multiple dashboards and robust search to expand intelligence across active endpoints, classified threats, threat priority notifications and visualization of threat stages.*

# CounterTack Sentinel

**Big Data Endpoint Threat Detection and Response**

## CounterTack Sentinel Key Benefits

- CounterTack Sentinel is embedded into the OS — giving the complete access to system behavior and providing operators with full visibility — and is tamper-resistant.
- CounterTack Sentinel captures every component of an attack and produces a real-time classification that maps to the attack lifecycle, telling operators exactly what is happening.
- CounterTack Sentinel has full remediation capabilities allowing users to quarantine endpoints and threats, terminate processes or files on-demand, deny network access to an endpoint and configure whitelists so that security teams can still have access to the endpoint.
- CounterTack Sentinel detection capabilities include DLL injection processes, accessing remote file shares, removable media behaviors and processes across memory and registries.
- CounterTack Sentinel automatically hashes the backing file for any new process and new file created on the endpoint.
- CounterTack Sentinel cuts down the time from infection to remediation with full threat context and impact analysis that goes beyond what traditional malware detection tools are capable of.
- CounterTack Sentinel leverages Big Data analytics through its integration with Cloudera, allowing teams to monitor endpoints across the enterprise, and providing massive scale data correlation, for a prioritized threat response.
- CounterTack Sentinel's REST API helps extend attack intelligence across other security deployments, such as SIEM, and adds more value for SOC operators and security analysts by adding contextual, real-time data for seamless integration into the most robust and widely-deployed security platforms.




*CounterTack Sentinel's endpoint sensors install on workstation and server endpoints across the enterprise, giving teams widespread visibility of behaviors happening across the entire Operating System.*

## BIG DATA ANALYTICS AND INTEGRATION

- Real-time analysis engine follows attacks across the enterprise
- Knowledge Library identifies key events and classifies threat behavior
- Centralized management console
- Export to common SIEM and aggregation tools
- Built on Cloudera® Enterprise Core for scalability and reliability
- Cloudera® Manager functionality including management, monitoring, diagnostics and integration
- Real-time Delivery for HBase
- CybOX support for triggering remote file access

## SENTINEL DEPLOYMENT FEATURES

- Continuous monitoring on desktops, laptops and servers
- Support for physical and virtual environments (VMware®, Microsoft® Hyper-V and Xen®)
- Operating system support
  - Windows XP SP3 (32-bit)
  - Windows 7 SP1 (32- & 64-bit)
  - Windows Server 2008 R2
- Built-in integration for sandboxing technologies
- On-demand extraction of any file on any endpoint
- Compatible with AV tools from Symantec®, McAfee®, AhnLab®

## How Does CounterTack Sentinel Work?

The CounterTack Sentinel endpoint sensor embeds itself deep within the endpoint OS, capturing all host behavior, including process and memory interactions, file manipulations, registry modifications and network activity. This vantage allows Sentinel to see system-level behavior after encryption and other obfuscation approaches have been removed.

From a process standpoint, endpoint intelligence is collected, deduplicated, compressed and encrypted, then forwarded to the Endpoint Analysis Cluster, featuring collector nodes and data nodes, which help to characterize and correlate massive quantities of behavioral data in real-time.

Sentinel tracks each interaction with the target OS, as well as its impact on the system, and offers enterprise-wide correlation — exposing the anatomy and origin of attacks while they're still in progress. Operators can subscribe to real-time updates as threats escalate — providing the industry's only "complete attack capture" — tracking advanced threats throughout their entire lifecycle.

For incident response teams, the average organization receives over 16,000 malware alerts weekly. Its become difficult to validate, prioritize and respond to these alerts, often coming from net-work-based devices. Sentinel's endpoint sensor, gives operators a clear and continuous view of behavioral context as it impacts the endpoint after the network premier is compromised, informing CIRT teams of the following information:

- Which systems are infected and most at risk?
- How were these systems become infected, and what are the behaviors that indicate compromise?
- Identification of attack artifacts in real-time without the need for a post-breach forensics investigation
- A thorough understanding and context of detected suspicious activity, the short-term impact of that behavior and visibility into the potential impact on the broader system if a response is not implemented

Sentinel removes the manual work of incident investigation and lets teams prioritize a confident, educated response, while still providing critical details including root cause and data on how the infection developed – essential for resisting advanced, and unknown threats.

CounterTack is the only EDR platform that gives teams kernel level data collection, enterprise scale, on-premise data analysis and correlation, and the behavioral intelligence required to counter attacks that have penetrated your current defenses. CounterTack is 100% focused on the 30% of threats, which are unknown and previously unseen in your systems, so you can eliminate threats and stop chasing malware.

### Data Node Requirements

- CPU: Two processors (12 cores total); Intel Xeon E5 is recommended
- Memory: 128 GB RAM
- Storage: 8-12 disks (one per CPU core); 1 TB capacity (ea.) recommended but not required; 7200 RPM minimum spin speed
- Network: 2x1 Gigabit Ethernet NICs

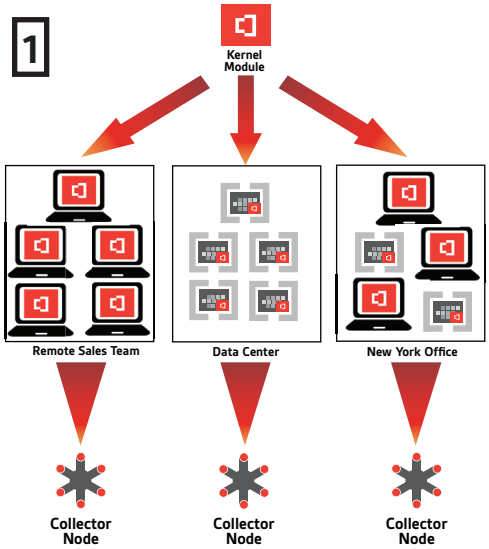
### Collector Node Requirements

- CPU: Minimum: 2.0 GHz Processor (4 cores); Intel Xeon E5 Processor (4 cores) is recommended
- Memory: Minimum: 64 GB RAM; At least 32GB RAM is recommended.
- Storage: Minimum: 250 GB; 500 GB and 7200 RPM minimum spin speed is recommended.
- Network: 2x1 Gigabit Ethernet NICs

# CounterTack Sentinel

**Big Data Endpoint Threat Detection and Response**

## The CounterTack Sentinel Incident Response Workflow




**PHASE I:**

-Sentinel endpoint sensors install on desktop and server endpoints.

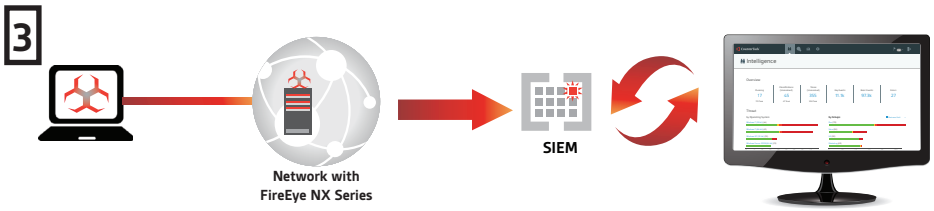
-Collector nodes start to collect data.

-An incident is reported by the network sensor (FireEye).

-The network sensor reports communication with a remote server that is on the reputation list.

**PHASE II:**

Leveraging Sentinel Search, operators can use the reported host IP to find all hosts across the enterprise, that have communicated with that IP address.


**PHASE III:**

Sentinel Search data gives operators information on the affected host, communication timestamp and process details (name, backing file and file location)

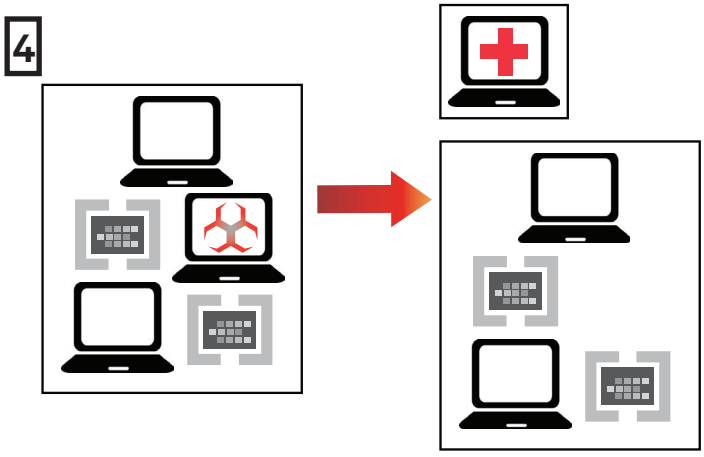
**PHASE IV:**

-Quarantine the affected machine for triage.

-Understand how the malicious program was dropped onto the host, and which process performed that.

-Identify if code has been injected into the process that communicated with the malicious remote server.

-Determine the true origin of the attack and preservation of evidence with a repeatable workflow.




CounterTack®

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com