OVERVIEW

All too often, organizations find themselves stuck in the ultimate quagmire when it comes to responding to incidents in a timely and efficient manner. The sheer volume of incidents that must be dealt with on a daily basis is a function of inadequate detection combined with poor integration between the tools we use to detect and respond to threats, and the tools used to protect against them.

As threats become more ubiquitous and complex, it becomes increasingly important that we evolve our strategy. This strategy must include better means to detect both known and unknown threats, as well as tightly integrated prevention technologies that rely on intelligent automation, not human intervention, for response.

COMMON ISSUES RELATED TO INCIDENT RESPONSE

• The sheer volume of attacks that are successful in breaking through perimeter defenses and compromising endpoints remains extremely high. Static signature and IOC based detection mechanisms are often weeks if not months behind the constantly evolving threat landscape.

• Understaffed incident response teams face an overwhelming volume of alerts daily, often resulting in critical misses that would tip an organization off to a serious cyber attack - according to a recent survey cyber attacks on average operate for as long as 229 days within an organization before detection.

• Incident response remains manually intensive as traditional endpoint protection solutions lack sufficient integration with advanced detection and response technologies.

SentinelOne is the first and only next-generation Endpoint Protection Platform that is able to provide an incident response solution that leverages the intelligence and automation needed to keep up with security incidents in real-time. SentinelOne employs several key technical features that dramatically accelerate the detection, prevention and response to advanced threats, as well as facilitate better teamwork and communication processes to ensure any threats inside your environment are eradicated instantly.

SCALING INCIDENT RESPONSE WITH SENTINELONE

Gartner identifies 12 critical capabilities for complete protection in their “Adaptive Security Model”

**Fig 1.** Gartner identifies 12 critical capabilities for complete protection in their “Adaptive Security Model”
Until recently, security teams have focused the majority of their investments on the top half of this diagram with the hopes that they could prevent all cyber attacks. This effort, as many security organizations have realized, is futile, as no technology can guarantee 100% security efficacy. In order to fully guard against a large, debilitating breach, organizations must also invest in the lower half of the diagram - the ability to respond in real-time as new, high priority incidents are detected. The solutions that enable this capability must be well integrated into automated preventative mechanisms to ensure that incidents are immediately contained and removed before an attacker can achieve their first objective.

SentinelOne addresses the Gartner critical capabilities with a unified solution based on the following threat detection, prevention, and incident response features.

**GROUNDBREAKING INNOVATION**

SentinelOne constitutes a fundamentally new approach to endpoint security. The core components enabling all of SentinelOne’s capability are:

**Dynamic Behavior Tracking (DBT) Engine:**
SentinelOne’s patent-pending Dynamic Behavior Tracking Engine relies on behavioral logic and machine learning to inspect and detect new attack patterns at the OS kernel level. Unlike other methods, this engine can catch polymorphic and zero-day threats designed to evade detection by solutions such as antivirus software and network sandboxes. Kernel mode execution prevents tampering with or disabling the detection capability. The DBT Engine eliminates the tradeoff that leads to false positives by allowing controlled execution of suspicious software while observing all the related activity and pinpointing malicious patterns.

**Lightweight Agent:** SentinelOne employs a low footprint, extremely lightweight agent for its endpoint protection and incident response capability. This agent is designed as a highly capable, deep inspection engine that operates in the kernel-space which allows it to perform its full task with distinct performance advantages, and at the same time be highly tamper resistant to any attempts to evade or disable the agent.

**DETECT**

- **Dynamic Detection:** Legacy antivirus and anti-exploit products use static mechanisms like signatures to evaluate executables and processes. Even some of the newer technologies like sandboxing, micro-virtualization and browser defenses are ineffective against advanced malware designed to evade detection. SentinelOne uniquely allows limited execution to extract all relevant operations including system calls, network activity, disk and memory access, registry (on Windows) and more. This gives SentinelOne a true picture of the behavior of every process to determine whether it is truly malicious or not. Dynamic detection covers processes that create an on-disk image, as well as in-memory only malware that evade other detection products.

- **Cloud Intelligence:** SentinelOne leverages leading cloud threat intelligence sources to confirm and prioritize the existence of known threats on your endpoints. It uses and enhances the threat intel sources it relies on. As part of detection, the hashes of processes being monitored are checked against threat intel sources for known malware, and information about any new binaries exhibiting malicious behavior is fed back and shared across all endpoints within the organization in order to immediately immunize other endpoints from a new attack.

- **Quarantine:** With SentinelOne, users are able to automatically contain incidents as they are detected to prevent compromised assets and threats from wreaking havoc upon your organization. Malicious processes are immediately terminated upon detection, and associated files are quickly isolated within a quarantined environment on the endpoint, and/or the endpoint is removed from the network altogether. This prevents any potential for lateral movement of a threat across the organization, or the exfiltration of valuable IP.
RESPOND

• **360º View Of Attacks**: SentinelOne arms incident responders with an extremely detailed view of every attack so they can perform necessary investigation and response. The 360º View of Attacks include summary information (device/file/IP data, communications info, file reputation, packing methods used and more), detailed attack overview (malicious behavior employed, activities performed, dwell time and network calls made), attack story line (pattern of propagation, kinds of kernel/API calls, files/registry modifications) in addition to all the raw data available on the threat.

![Fig 2. Attack Story Line View Showing Attack Propagation](image)

![Fig 3. Detailed Attack Report with all malicious files and activity](image)

![Fig 4. Response and Mitigation actions are initiated automatically](image)

• **Retrospective Analysis**: According to a recent survey, malicious software goes undetected for over 229 days following an initial compromise. SentinelOne provides analysis capability that allows you to look for malicious behavior patterns and anomalies in historic data. This is particularly important in cases where the threat is able to evade direct detection/investigation after compromise, and the only way to identify that an endpoint was compromised in the past is to look for the patterns and indicators of compromise.

• **Automatic Response and Mitigation**: SentinelOne is the only solution that automates the response and mitigation necessary to prevent a massive data breach through simple policy-based Alert, Kill and Quarantine settings. Our ability to provide a single product that covers detection, prevention and response is unique. We have been certified by AV-TEST and are a true replacement for antivirus, and in addition uniquely satisfy the burning need for better detection and response capabilities.

• **Remediation**: SentinelOne provides automated rollback functionality that returns endpoints to their pre-attack state accelerating incident remediation. Threats make damaging changes to the endpoint as soon as they infect the device, often altering or deleting important system files. SentinelOne helps remediate this process with Rollback, and is the only solution that saves and protects the state of endpoints, making it uniquely capable of helping victims restore the endpoint to a trusted state effectively reversing the changes made by the malware infection.

**CONCLUSION**

SentinelOne is the only endpoint protection platform that natively integrates prediction, prevention, detection and response. By putting the right set of tools in many incident response teams, we have demonstrated orders of magnitude reduction in the average detection and response times saving security teams considerable time, energy and money while simultaneously improving the overall security posture of the organization. For more information on SentinelOne, visit [www.sentinelone.com](http://www.sentinelone.com).