SentinelOne®

Unlock the Synergistic Power of Singularity™ Endpoint Data in Your Singularity™ AI SIEM

White Paper

Table of Contents

Introduction

The Evolving Threat Landscape and the Need for Integrated Security

Today's adversaries employ multifaceted tactics, moving laterally across networks, evading traditional security controls, and leveraging sophisticated techniques that leave subtle footprints across various systems. Detecting and mitigating these intricate attacks requires a holistic view of the security environment, a perspective often obscured by fragmented data and disjointed security tools that leads to overwhelming alert volumes and hinders effective threat detection.

A powerful solution to these challenges lies in breaking down data silos and enriching security intelligence by leveraging Endpoint Detection and Response (EDR) data within a Security Information and Event Management (SIEM) platform. EDR solutions provide granular visibility into endpoint activity capturing critical information about processes, file modifications, network connections, and user behavior. By integrating this rich endpoint telemetry into the centralized analysis capabilities of a SIEM, organizations can gain a unified view of their security posture, enabling more effective threat detection, faster incident response, and ultimately, a more resilient security program.

This strategic imperative is further underscored by recent industry trends. A LinkedIn poll revealed that approximately 85% of respondents are already sending all or a subset of their EDR data to their SIEM. This widespread adoption highlights the recognized value of this integration. For organizations not fully leveraging their EDR data within their SIEM, particularly if they are paying for its ingestion, they are either incurring unnecessary costs for SIEM ingest or potentially limiting their security visibility by only sending a subset of crucial endpoint telemetry, possibly due to cost considerations.

For SentinelOne customers, integrating their Singularity Endpoint data with Singularity AI SIEM offers a significant advantage. Singularity AI SIEM provides free ingestion of 100% of their Singularity Endpoint data plus 10GB of free data ingestion allowing customers to begin leveraging the powerful correlation and analysis capabilities of their AI SIEM with their rich endpoint data right away. This unique value proposition immediately translates into significant cost savings by eliminating the often substantial expenses associated with ingesting high-volume endpoint logs into a separate SIEM.

Foundational Advantages: Why EDR Data Belongs in Your SIEM

Integrating EDR data into your SIEM transcends simple data aggregation. It unlocks a suite of foundational advantages that enhance security posture, optimize operational efficiency, and ultimately deliver a more robust defense against modern threats.

Reducing Costs Associated with Log Ingestion of Other Data Sources

Organizations ingest a diverse array of log sources into their SIEM for various critical reasons. Primarily, these include meeting compliance and regulatory requirements, ensuring adherence to industry standards and legal mandates for data retention and security monitoring. Secondly, log ingestion is vital for enabling and improving the Security Operations Center's (SOC) work in defending the organization, providing the raw material for threat detection, investigation, and incident response. Finally, SIEMs can also assist with other IT and operational use cases, such as performance monitoring, troubleshooting, and capacity planning, which necessitate the ingestion of relevant system logs.

By having comprehensive EDR data within the SIEM, organizations can strategically reduce their reliance on ingesting certain redundant log sources, leading to significant cost savings in data ingestion and storage. Consider the guidance provided by the Cybersecurity and Infrastructure Security Agency (CISA) in their M-21-31 directive for Federal Government Agencies. This document outlines recommended log sources for enhanced cybersecurity visibility, including a substantial number of logs originating from Operating Systems (OS).

✔ **Comprehensive Overlap by SentinelOne EDR Agent:** These logs are extensively collected and analyzed by the SentinelOne EDR agent.

✓ **Endpoint-Derived Data Complementing Network Logs:** The SentinelOne EDR agent extensively collects and analyzes OS-level data, including a strong overlap with these CISA-recommended event types.

⊖ **Beyond EDR Agent Scope:** These categories (e.g., Cloud, SaaS) are not directly collected by the EDR agent but can be covered by other SentinelOne platform products (e.g., Identity, Cloud Native Security).

CISA Recommended Types of Events	SentinelOne EDR Agent Coverage
Identity, Credential, and Access Management (ICAM); Privileged ICAM (PICAM)	⊖ Manage/track changes in attributes and credentials ⊖ Track usage of credentials
Operating Systems (Windows/Linux/Mac where applicable)	✔ Process creation ✔ Remote terminal or equivalent access and log off (success/failure) ✔ System access and logoff (success/failure) ✔ Scheduled task changes ✔ Service status changes (start, stop, fail, restart, etc.) ✔ Active network communication with other hosts ✔ Command-line interface (CLI) ✔ PowerShell execution commands ✓ Windows Management Instrumentation (WMI) Events ✔ Installation or removal of storage volumes or removeable media
Network device infrustructure	✓ Domain Name System (DNS) query/response logs ✓ Dynamic Host Configuration Protocol (DHCP) lease information including media access control (MAC) address, IP address ✓ Firewall logs
Cloud environments (general logging)	⊖ Any activity on breakglass account(s) (which should never have to be used)
Amazon Web Service (AWS)	⊖ AWS CloudTrail
Cloud Azure	⊖ Azure Active Directory Logs ⊖ Azure Activity
Microsoft 365	⊖ Unified audit log (with advanced audit features)
Google Cloud Platform (GCP)	⊖ Admin audit

As evident, a SentinelOne customer already possesses a wealth of information within their EDR tenant that directly corresponds to a large portion of the OS logs recommended by CISA. By leveraging AI SIEM, these organizations can potentially avoid ingesting 100% of those recommended OS logs (and the associated ingestion costs), as the equivalent rich data is already available and accessible within the SIEM through their EDR deployment.

Furthermore, on the front of reducing costs associated with enabling the SOC, many security teams rely on frameworks like MITRE ATT&CK to understand their visibility into potential attacker behaviors. The SentinelOne console provides a clear view of its EDR's coverage across the MITRE ATT&CK matrix. With finite security budgets, knowing that 100% of logs related to SentinelOne's detection of these MITRE ATT&CK techniques are already within the SIEM allows security teams to strategically focus their log ingestion budget on filling visibility gaps in other critical areas, ultimately achieving greater security coverage for their investment.

To view MITRE ATT&CK coverage, navigate to the Singularity Operations Center and select MITRE ATT&CK from the Help dropdown menu on the top of the console. You can also read the blog post: SentinelOne Continues to Set the Standard in MITRE ATT&CK® Evaluations | 100% Detection, Zero Delays and 88% Less Noise.

Enabling Net New Detections of Security Issues

As previously highlighted with the MITRE ATT&CK coverage, the richness of EDR data empowers the creation of net new detections directly within the SIEM. When novel attack techniques or Indicators of Compromise (IOCs) related to areas covered by SentinelOne Endpoint are discovered, organizations without integrated EDR and SIEM often need to first identify and then ingest the relevant OS system logs before they can even begin querying for these new threats.

> With Singularity Endpoint data already residing in AI SIEM, security teams can immediately apply these new threat intelligence insights and craft detection rules against this existing dataset. This eliminates the delay and complexity of onboarding new log sources, enabling proactive detection of emerging threats at no additional ingestion cost.

Moreover, certain types of detections are inherently more effective when performed within a SIEM's analytical environment rather than directly within a point security product. These broadly include:

- **Detecting Behaviors Over Time:** Analyzing trends and deviations in endpoint behavior over extended periods (e.g., unusual network traffic volumes compared to historical baselines) often falls outside the scope of real-time or point-in-time focused security tools.
- **Retroactive Detection:** When new threat intelligence emerges, SIEMs excel at efficiently querying historical data to determine if the malicious behavior occurred in the past – a capability often limited in real-time prevention tools.
- **Cross-Correlation Detections:** Identifying sophisticated attacks often requires correlating events and behaviors across multiple security layers. Having rich EDR data within the SIEM facilitates the creation of these complex correlation rules, providing a more holistic view of potential threats.

For cross-correlation, a compelling example involves leveraging network traffic data. It is common for edge firewalls, such as a Palo Alto Firewall, to generate threat logs concerning internal IP addresses attempting communication with potentially malicious external IPs or URLs. While this detection capability is valuable for blocking connections, the sheer volume of such alerts can lead to significant time spent chasing false positives. A more effective approach involves correlating these firewall alerts with detailed information about the behavior of the endpoint associated with that internal IP address at the time of the alert.

Specifically, we can examine the endpoint’s internal network connectivity patterns. This can be achieved by leveraging a query that joins Singularity Endpoint data with Palo Alto Firewall threat logs:

```
| join
a = (
dataSource.name=‘SentinelOne’ event.type = ‘IP Connect’
| filter net_private(dst.ip.address)
| filter dst.port.number in (22 , 445, 3389)
| group Count=count() by src_endpoint.ip=src.ip.address
),

b=
(dataSource.name contains ‘Palo’ event.type=‘THREAT’
| group Palo_Threat_Log_Count=count() by src_endpoint.ip
)

on src_endpoint.ip
```

This search performs the following actions:

- Grabs all network connections originating from or destined for all endpoints with a SentinelOne agent installed.
- Filters down to only traffic involving private IP addresses, focusing on potential lateral movement within the internal network.
- Further filters the traffic to include only attempts to connect to common remote access ports (22 - SSH, 445 - SMB, 3389 - RDP).
- Groups a count of these internal connections by the source IP address.
- Retrieves all threat logs generated by the Palo Alto Firewall.
- Groups these Palo Alto threat logs based on the source IP address.
- Returns only the IP addresses that appear in both datasets.

The result is a significantly refined list of internal IP addresses. These are endpoints that the Palo Alto Networks firewall has flagged for potentially communicating with a command-and-control (C2) server or similar malicious entity, and which have also exhibited internal activity indicative of lateral movement attempts. In a lab environment, this correlation effectively reduced the number of IPs requiring investigation from approximately 40 flagged by Palo Alto down to just 2.

src_endpoint.ip	Count	Palo_Threat_Log_Count
10.0.0.1	42	1,438
192.168.0.1	46	2,876

Enhancing Detections from Other Log Sources to Speed Up Detection and Investigation

The true power of integrating EDR data with a SIEM lies in its ability to enrich alerts from other security tools, providing crucial context that accelerates detection, reduces false positives, and streamlines investigations.

Consider an alert originating from an edge firewall, such as a Palo Alto Firewall, indicating potential communication between an internal IP address and a known malicious external IP or URL. While the firewall's detection is valuable, investigating each such alert can be time-consuming and often yields false positives.

The ability to correlate this network-based alert with detailed endpoint behavior at the originating IP address provides invaluable context. For instance, the following query demonstrates how to join network traffic data from Singularity Endpoint with threat logs from a Palo Alto Firewall:

```
| join
a = (
dataSource.name = ‘SentinelOne’ event.type = ‘IP Connect’
| columns src.process.displayName, src.ip.address, dst.ip.address, src.port.
number, dst.port.number, endpoint.name, event.network.direction, src.port.number,
dst.port.number, site.name, src.process.image.path, src.process.image.md5, src.
process.cmdline, src.process.user, src.process.publisher
| let src_endpoint.ip=src.ip.address, dst_endpoint.ip=dst.ip.address, src_
endpoint.port=src.port.number, dst_endpoint.port=dst.port.number
),

b=
(dataSource.name contains ‘Palo’ event.type=‘THREAT’
| columns threat.name, src_endpoint.ip, dst_endpoint.ip, src_endpoint.port, dst_
endpoint.port
)

on src_endpoint.ip, dst_endpoint.ip, src_endpoint.port, dst_endpoint.port
```

When investigating a high-confidence alert from another source, such as a firewall identifying a connection matching a known threat signature, enriching this alert with EDR data can significantly speed up response. Instead of just an IP address, a simple join query can provide details about the specific endpoint associated with that IP at the time of the event, including the hostname, the process initiating the connection, its hash, and its publisher. This immediate endpoint context allows security teams to quickly pivot to the affected machine within the SentinelOne console for containment, remediation, and further analysis.

Reducing False Positives Derived from Detections from Other Log Sources

A common challenge in security operations is the high volume of false positive alerts generated by certain detection rules. A prime example is the “Impossible Traveler” detection, which flags user logins originating from geographically disparate locations within a short timeframe. While the underlying logic aims to identify compromised accounts, legitimate user behavior such as VPN usage, proxy connections, and rapid travel can trigger numerous false positives, leading to wasted analyst time.

Singularity Endpoint can significantly reduce these false positives by providing valuable endpoint context. The EDR agent records the public IP address an endpoint connects from during its registration process. This information can be accessed with a query similar to:

```
dataSource.name =‘asset’ activity_name=‘Collect’
| columns device.agent.last_ip_to_mgmt, device.agent.last_logged_in_user_name,
device.name, device.hw_info.serial_number, device.ip_external
```

By leveraging this EDR-collected public IP information, organizations can enhance their “Impossible Traveler” detection logic, which might look something like the below:

```
Username = * ClientPublicIP = *
| group first_ip = oldest(ClientPublicIP), last_ip = newest(ClientPublicIP) by
Username
| let first_location = geo_ip_location(first_ip), last_location = geo_ip_
location(last_ip)
| filter first_location != last_location
| let kilometers = geo_distance(first_location, last_location)
| let hours=(queryend() - querystart())/1000000000/60/60
| let kmh=kilometers/hours
| sort -kmh
| filter kmh > 250
```

The proposed solution involves:

1. Creating a lookup table of all public IPs that legitimate endpoints report in from. This can be achieved by appending `| savelookup` to the agent registration log query and running it on a scheduled basis.
2. Modifying the “Impossible Traveler” detection query to check if both the initial and subsequent login IPs are present in this trusted public IP lookup table.

By adding a lookup command at the end of the "Impossible Traveler" query, the system can effectively dismiss alerts where the seemingly impossible travel is explained by legitimate changes in the user's external IP address due to VPN or proxy usage. This is possible because comparing the pattern of IP addresses for SSO login to the pattern of IP addresses the user's endpoint is connecting from, we can see that they match. This suggests that the user is likely using a VPN or proxy, giving the appearance of their user (and machine) moving from IP to IP, rather than a threat actor attempting to log in with stolen credentials from multiple IPs. This significantly reduces the noise of false positive alerts, allowing analysts to focus on genuine indicators of compromise.

Establishing these foundational advantages, the integration of EDR data into a SIEM transforms security operations from a reactive, data-constrained endeavor to a proactive, context-rich defense. The ability to reduce costs, enable new detections, enhance existing ones, and minimize false positives underscores the strategic imperative of leveraging the wealth of information residing at the endpoint within the centralized analytical power of the SIEM.

Deep Dive Into Cross-Correlation Use Cases

Cross-correlation stands as a cornerstone of modern threat detection, moving beyond isolated security alerts to identify sophisticated attacks that weave together seemingly disparate events across various layers of the IT environment. By analyzing relationships and patterns between different data sources, cross-correlation unveils subtle indicators of compromise that individual security tools might miss, proving particularly powerful in detecting advanced persistent threats (APTs) and insider threats. Integrating rich EDR data into the SIEM significantly amplifies the effectiveness of cross-correlation, providing crucial endpoint context to network, identity, and other security events.

To illustrate the power of this approach, we can categorize several key use cases where combining EDR data with other log sources yields superior detection capabilities and enhanced investigative insights:

Use Case	Security Challenge	Correlation Logic	Benefits
Network Focused: Identifying Potential Command and Control (C2) via DNS Anomalies and Suspicious Endpoint Behavior	Detecting covert communication channels established by malware or threat actors using DNS. While network-based DNS security tools can flag suspicious DNS requests, understanding the originating endpoint process and its concurrent behavior provides critical context.	This use case involves joining DNS query logs (e.g., from a DNS firewall or server) with EDR process and network connection events. The logic looks for endpoints making suspicious DNS requests (e.g., to newly observed domains, domains with unusual character patterns, or domains associated with known threats) and then examines the originating process for anomalous behavior such as unusual network connections, the spawning of child processes, or suspicious command-line arguments.	**Improved Accuracy:** Reduces false positives from legitimate applications making unusual DNS requests. **Faster Investigation:** Provides immediate insight into the affected endpoint and the potentially compromised process. **Broader Visibility:** Connects network-level indicators with endpoint activity, revealing the full attack chain.
Network Focused: Detecting Potential Data Exfiltration Correlating Unusual Network Connections with File Activity	Identifying instances where sensitive data might be leaving the organization through unauthorized network channels. Network DLP solutions can flag potential exfiltration attempts, but understanding the endpoint context of the data access and transfer is crucial.	This use case combines network connection logs (especially connections to external or untrusted destinations) with EDR file access and modification events. The logic looks for endpoints exhibiting unusual spikes in outbound network traffic to suspicious locations immediately following the access or modification of sensitive files. VPN connection logs can also be incorporated to identify potentially unauthorized exfiltration occurring outside of expected secure channels.	**Improved Accuracy:** Distinguishes legitimate file transfers from potentially malicious exfiltration. **Faster Investigation:** Provides a clear timeline of file access and network activity on the involved endpoint. **Broader Visibility:** Extends DLP visibility down to the endpoint level, capturing activity that might bypass network controls.
Identity Focused: Detecting Lateral Movement by Correlating Anomalous Logins with Suspicious Endpoint Activity	Identifying threat actors moving laterally within the network after an initial compromise. While unusual login patterns (e.g., logins to multiple hosts from a single compromised account) can be detected in identity logs, confirming malicious activity requires examining the actions taken on the newly accessed endpoints.	This use case involves joining authentication logs (e.g., Windows Security Logs, SSO logs) with EDR process creation, network connection, and privilege escalation events on the destination endpoints of the anomalous logins. The logic looks for instances where a suspicious login is followed by the execution of unusual processes, attempts to access sensitive files, or lateral network connections originating from the newly accessed host.	**Improved Accuracy:** Reduces false positives from legitimate administrative access. **Faster Investigation:** Immediately highlights the actions taken by the potentially compromised account on the target systems. **Broader Visibility:** Connects suspicious login behavior with on-endpoint activity, confirming successful lateral movement.

Practical Implementation and the SentinelOne Advantage

The theoretical benefits of integrating EDR data with a SIEM are compelling, but the practical implementation is equally critical. For SentinelOne customers, the journey to realizing these advantages is significantly streamlined through the tight integration with AI SIEM.

SentinelOne's approach to data ingestion in AI SIEM:

- **Ingestion of SentinelOne's Core Data: SentinelOne provides free ingestion for the data it generates to power its own security products.** This includes the rich EDR data collected by SentinelOne agents, which is fundamental to the platform's detection and response capabilities. This data is seamlessly ingested into the Singularity Data Lake, providing customers with immediate access for analysis and correlation within the AI SIEM. While customers can pay to extend the retention period for this data, the initial ingestion itself incurs no cost. This represents a substantial cost saving, especially for organizations with high EDR data volumes; some SentinelOne customers generate up to 500TB of EDR logs daily, and ingesting this into a traditional SIEM would be prohibitively expensive.
- **Ingestion of Other Data and Logs:** In addition to the free ingestion of SentinelOne's core data, AI SIEM also supports the ingestion of data and logs from other sources. This includes data from various third-party security tools, IT infrastructure, and applications. For this "other" data, SentinelOne provides a permanent free tier of 10GB per day. Organizations that exceed this 10GB daily limit will need to purchase licensing for the overage.

This clear separation of data ingestion costs provides SentinelOne customers with flexibility and cost-effectiveness. They can leverage the full power of their EDR data within Singularity AI SIEM without incurring ingestion fees, while also having the ability to ingest other relevant data sources as needed, with a reasonable free tier and transparent pricing for higher volumes.

Beyond data ingestion, building sophisticated correlation rules and intuitive dashboards within AI SIEM is designed for ease of use. The platform offers a user-friendly interface with intuitive query languages and visual tools that empower security analysts of all skill levels to create custom detection logic tailored to their specific threat landscape and organizational needs. Leveraging the normalized and enriched EDR data alongside other security logs, analysts can quickly construct correlation rules that identify complex attack patterns, as illustrated in the cross-correlation use cases discussed previously. The platform's dashboarding capabilities further enhance operational efficiency by providing real-time visibility into key security metrics, trends, and the output of custom correlation rules, enabling proactive monitoring and faster incident triage.

AI SIEM offers significant performance and scalability benefits when handling the high volume and rich context of security data. Traditional SIEM architectures can often struggle with the ingestion, storage, and analysis of such detailed telemetry. AI SIEM's cloud-native architecture is designed to efficiently process massive datasets in real-time, ensuring that security teams can query and analyze their data without performance bottlenecks. The inherent scalability of the cloud allows the platform to adapt to growing data volumes as an organization's digital footprint expands, providing a future-proof solution for managing and analyzing critical security data.

Conclusion

Future-Proofing Your Security Posture with Integrated EDR and SIEM

The strategic integration of EDR data within a SIEM represents a paradigm shift in modern security operations. By breaking down data silos, organizations can significantly reduce operational costs associated with redundant log ingestion while simultaneously enhancing their threat detection capabilities. The rich endpoint context provided by EDR enriches alerts from other security tools, leading to faster investigations and a dramatic reduction in false positives. For SentinelOne customers, the inherent advantage of free Singularity Endpoint data ingestion into Singularity AI SIEM further amplifies these benefits, offering a cost-effective and powerful pathway to unified security visibility and proactive threat defense.

Looking ahead, the evolving threat landscape will continue to demand increasingly sophisticated and integrated security solutions. The synergy between endpoint intelligence and advanced analytics, powered by AI, will be crucial in staying ahead of determined adversaries. Organizations that embrace this integrated approach, leveraging the granular visibility of EDR within the analytical power of an AI SIEM, will be better positioned to not only detect and respond to today's threats but also to proactively anticipate and mitigate tomorrow's emerging risks, ultimately building a more resilient and future-proof security posture.

Appendix: Sample EDR Queries

DNS resolutions:

```
event.type in (‘DNS Resolved’, ‘DNS Unresolved’)
| columns endpoint.name, event.dns.request, event.dns.response, osSrc.process.
cmdline, osSrc.process.image.path, osSrc.process.image.sha1, osSrc.process.image.
md5, osSrc.process.image.sha256, osSrc.process.name, osSrc.process.signedStatus,
osSrc.process.user, site.name, src.process.cmdline, src.process.user, src.process.
name, timestamp
```

URL events:

```
dataSource.name = ‘SentinelOne’ url.address = *
| group count() by url.address, event.type, endpoint.name, os.name, site.name,
src.process.cmdline, src.process.displayName, src.process.image.sha256, src.
process.name, src.process.parent.publisher, src.process.signedStatus, src.process.
user
| columns url.address, event.type, endpoint.name, os.name, site.name, src.process.
cmdline, src.process.displayName, src.process.image.sha256, src.process.name, src.
process.parent.publisher, src.process.signedStatus, src.process.user
| limit 100
```

IP network connections:

```
dataSource.name = ‘SentinelOne’ event.type = ‘IP Connect’
| columns src.process.displayName, src.ip.address, dst.ip.address, src.port.
number, dst.port.number, endpoint.name, event.network.direction, src.port.number,
dst.port.number, site.name, src.process.image.path, src.process.image.md5, src.
process.cmdline, src.process.user, src.process.publisher
```

Login events:

```
dataSource.name =‘SentinelOne’ event.type in (‘Login’ , ‘Logout’ , ‘Logon’,
‘UserLoginFailed’ )
| columns endpoint.name, meta.event.name, os.name, event.login.failureReason,
event.login.loginIsSuccessful, event.login.userName, site.name, src.endpoint.
ip.address
```

File events:

```
dataSource.name= ‘SentinelOne’ event.type in (‘File Creation’,‘File Rename’,‘File
Deletion’,‘File Modification’)
| columns endpoint.name, event.type, site.name, src.process.cmdline,src.process.
displayName,src.process.image.md5,src.process.image.path,src.process.image.
sha1,src.process.image.sha256,src.process.name,src.process.parent.name,src.
process.user,src.process.publisher,src.process.signedStatus,tgt.file.path,tgt.
file.sha1,tgt.file.sha256
```

Process events:

```
dataSource.name= ‘SentinelOne’ event.type in (‘Module Load’,‘Process
Creation’,‘Named Pipe Creation’,‘Command Script’,‘Driver Load’ )
| columns endpoint.name, event.type, site.name, src.process.cmdline, src.process.
displayName, src.process.image.md5, src.process.image.path, src.process.image.
sha1, src.process.image.sha256, src.process.parent.cmdline, src.process.parent.
image.path, src.process.publisher, src.process.signedStatus, src.process.user,
tgt.process.cmdline
```

Generally extracting info about endpoints:

```
endpoint.os contains “windows”
| columns endpoint.name, endpoint.type, os.name, site.name, src.process.name, src.
process.cmdline
```

Endpoint registrations:

```
dataSource.name =‘asset’ activity_name=‘Collect’
| columns device.agent.last_ip_to_mgmt, device.agent.last_logged_in_user_name,
device.name, device.hw_info.serial_number, device.ip_external
```

SentinelOne®

Contact Us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.