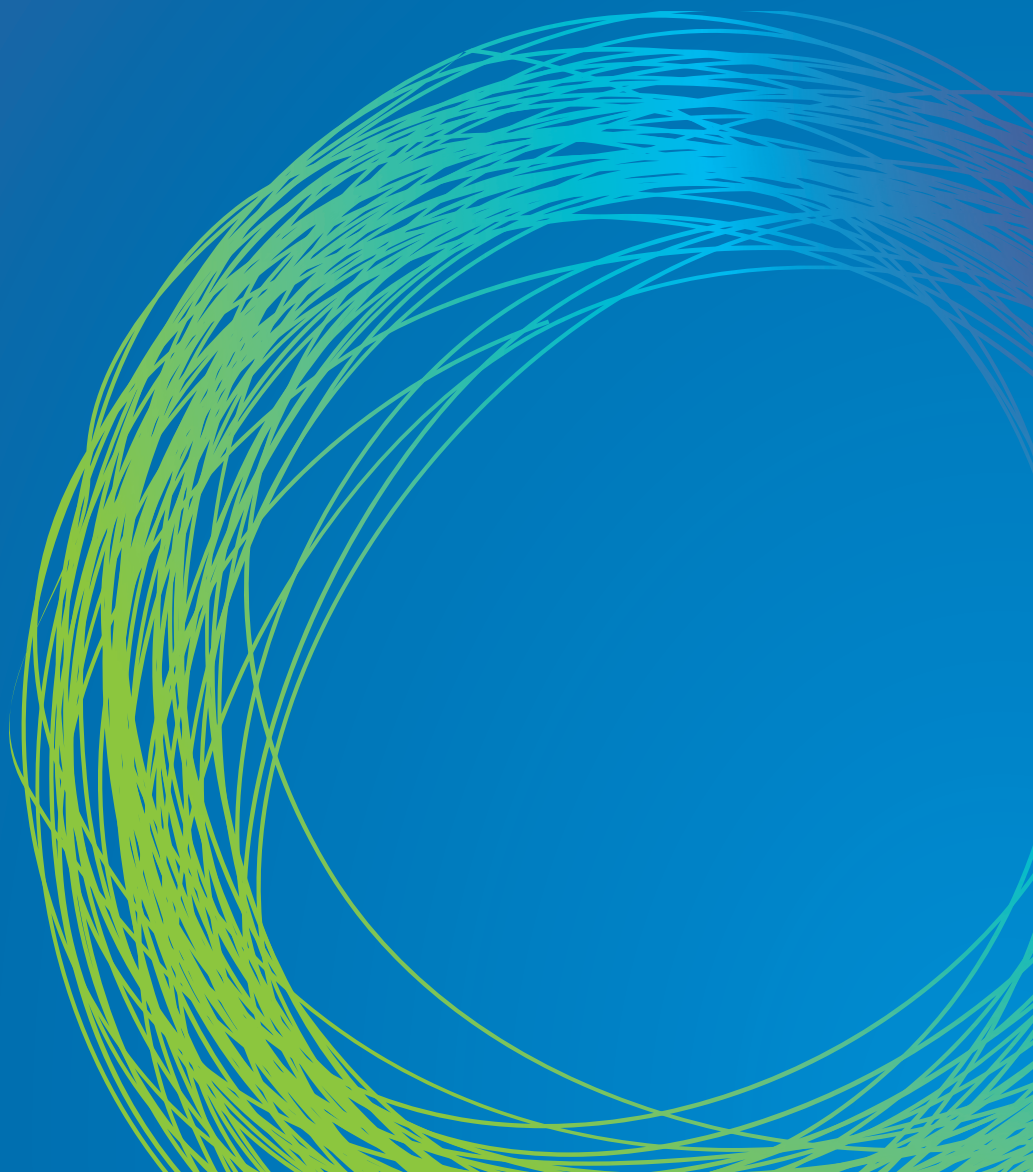
SentinelOne

Next-Generation Endpoint Protection



What is Next-Generation Endpoint Protection?

By now, you have probably heard the term “Next-Generation Endpoint Protection” as there are a slew of companies, startups and incumbents alike, which are using the term to describe some of their offerings. But what does it actually mean? What are the capabilities you should look for in a Next-Generation Endpoint Protection Platform? What makes it “Next-Generation”?

OVERVIEW

This whitepaper will lay out and define the critical components of a next-generation endpoint protection (NGEP) platform, the role of each capability, and the challenge it addresses. In addition, it will offer a series of solution attributes that are important to consider when planning to deploy NGEP solutions across a modern enterprise environment.

SUMMARY

Endpoint protection is one of the most critical security programs organizations of every size and focus must build. Today's threat landscape is comprised of an increasingly diverse set of highly sophisticated threats, and no endpoint device or platform is left untargeted. The static methods (antivirus solutions) that have long been the sole preventative measures are no longer effective against today's advanced attacks. A new approach to endpoint protection requires capabilities that address the entire threat execution lifecycle: from pre-execution to post-execution. Furthermore, the underlying technology must drive the ability to not only identify a threat by what it is, but by how it *behaves*, and enable intelligent threat response at machine speed. The 7 critical NGEP capabilities this paper will highlight are:

PRE-EXECUTION

- Prevention of known threats
- Application whitelisting and blacklisting

ON EXECUTION

- Dynamic exploit detection
- Dynamic malware detection

POST-EXECUTION

- Mitigation
- Remediation
- Real-time forensics

BACKGROUND

Back in the day when viruses ruled the cyber threat landscape, it was the Windows-based computer that was most vulnerable. These PCs and laptops comprised the predominant endpoint platform most organizations deployed. Protecting each computer against viruses and file-based malware involved a simple installation of antivirus software on the local machine, requiring periodic downloads of new signatures to protect against the latest viruses.

Today, organizations now manage more endpoint platforms than just Windows; Macs have grown to comprise a significant percentage of enterprise endpoint devices, and Linux-based servers are being deployed in abundance (physically, virtually, and in the cloud) to support a wide variety of business-critical applications. The definition of an endpoint has expanded considerably, and now includes mobile devices, embedded devices, SCADA systems and many other types of devices with internet connectivity. The resulting endpoint attack surface is much broader, and thus much more difficult for organizations to reduce and defend against today's threats, which have evolved far beyond run-of-the-mill computer viruses and basic exploits.

Enterprise organizations collectively face *billions* of highly sophisticated attacks across multiple vectors—not just file-based malware. In fact, even the malware that AV would normally catch is often altered and packaged in ways that make it appear new or benign, allowing it to completely evade detection. Common techniques include using polymorphic malware, packers and wrappers. Threat prevention by static methods alone provides little protection.

Given the heightening sophistication of malware, IT security professionals needed new ways to determine whether an unknown file was malicious or benign. Security vendors then developed network-based sandboxes (also known as breach detection systems (BDS) or Advanced threat detection systems) that emulate the execution of suspicious files inside a virtual machine residing on the network, and then monitor the file's behavior throughout its execution. Attackers quickly realized that although their current packing techniques and malware variations could not evade these sandboxes as easily as they could bypass static signature-based solutions, they could employ other techniques to render sandbox-based detection ineffective. For example, the malware could be designed to determine whether or not it is being run inside a sandbox, as opposed to an actual target endpoint device. Sandbox solutions limit emulation time, and there is an obvious lack of user interaction. These characteristics can be exploited such that the malware will not run in the emulated environment, and will be flagged as 'benign'. In those cases, the malware simply lays dormant until it can continue its route to a target endpoint.

Though cyber threats can be easily disguised in a variety of ways, it is far more difficult for their behavior to be altered. Therefore, the ability to see what is actually running on the endpoint device itself, and see how every application or process is behaving, is key to combatting the detection problem. This is the key technological underpinning of next-generation endpoint protection.

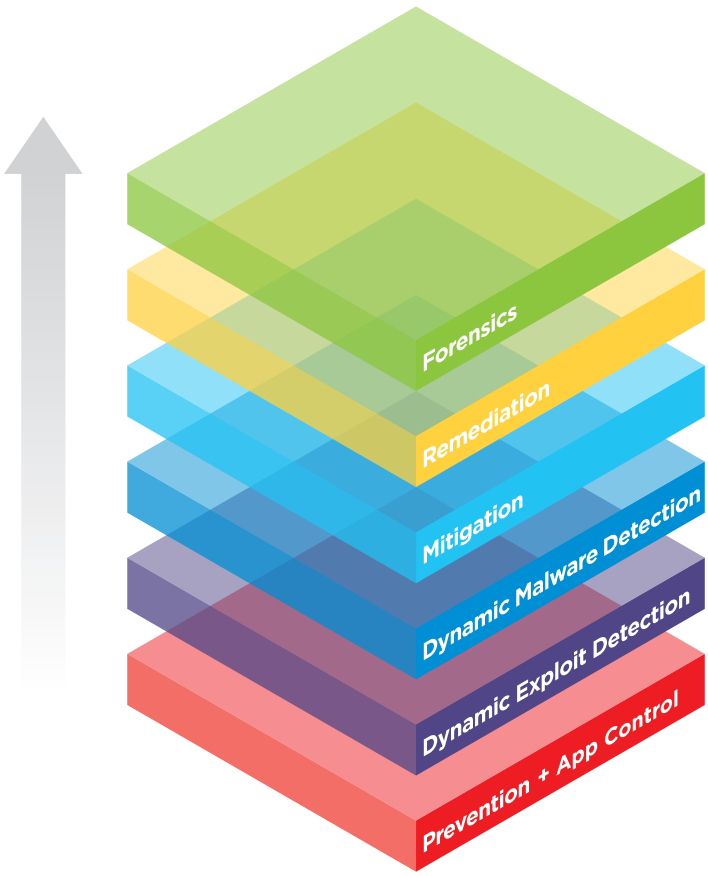


Fig 1. *Next Generation Endpoint Protection Platform - Critical Pillars*

©2016 SentinelOne. All Rights Reserved.

Next Generation Endpoint Protection

At a high level, a next-generation endpoint protection solution needs to operate on the endpoint device itself, and be effective against all major attack vectors across the entire threat execution lifecycle (pre-execution, on execution, and post-execution). This requires real-time behavior analysis and forensics, along with the ability to mitigate and remediate threats at machine speed.

This section describes the critical capabilities and features of next-generation endpoint protection as they apply across the three phases of the threat execution lifecycle.

PRE-EXECUTION: STATIC PREVENTION, WHITELISTING AND BLACKLISTING

While next-generation endpoint protection needs a fundamentally new approach to stop advanced malware and zero-day threats, there is still good reason to leverage proven techniques to block known threats, as there are many still out in the wild. File-based malware can be prevented from executing on a target endpoint device, provided the malicious file's signature or hash matches that profiled in a reputation service's signature database.

Today, organizations can leverage over 40 leading vendors' reputation services by tapping into cloud intelligence services and taking advantage of wider coverage.

Also, organizations have begun supplementing the shortcomings of their antivirus software by deploying whitelisting and blacklisting technology as an additional layer of protection. These techniques combine to form a brute force method of gating which applications are allowed to run on a particular endpoint device. This form of prevention is an effective means of significantly shrinking the organization's overall attack surface, and makes hackers and cybercriminals work harder (and spend more money) to penetrate the organization's IT infrastructure via the endpoint.

By today's standards, pre-execution protection should be considered table stakes for any next-generation approach to securing the endpoint.

> ***Recommendation:*** Choose an NGEP solution that not only leverages multiple vendors' reputation services to proactively block threats, but one that also uses a lightweight method to index files (passive scanning, or selective scanning) instead of ones that routinely execute resource-intensive system scans. The solution should provide application control functionality as well.

ON EXECUTION: DYNAMIC BEHAVIOR-BASED DETECTION OF ADVANCED THREATS

Unknown threats (often carefully wrapped or altered variants of known threats) escape static prevention measures and begin to execute on the endpoint device. It is at this point where behavior-based analysis techniques—the basis of NGEP-- come into play.

The identification of advanced threats through behavioral analysis requires continuous monitoring of all system-level activity on the endpoint device: system calls, network calls, I/O transactions, memory transactions, etc. This degree of monitoring is necessary in order to build a context of normal system and application behavior, against which an advanced threat can be rapidly identified. Furthermore, deep endpoint activity monitoring is essential for rendering meaningful, detailed forensics-- a key ingredient of successful post-execution processes.

As with file-based malware, the application of sophisticated algorithms that map suspicious processes into malicious patterns enables highly-effective detection of memory-based malware, advanced exploits and insider/script-based attacks.

Overall, behavior-based detection has been proven to be far more effective than static detection. It is also more effective than other self-proclaimed next-generation solutions which use mathematical modeling to find

similarities between a suspicious binary's structure among different variations and families of malware. These methods are still limited to file-based malware, and fall into the same cat & mouse game of attackers and security vendors trying to outsmart each other.

Recommendation: Dynamic behavior analysis and an approach that does not rely solely on prior knowledge of a specific indicator to detect an attack will prove to be superior when dealing with true zero day attacks. Zero-day attacks rarely display any static indicator of compromise, even though the attack's behavior will be largely familiar. Ensure the NGEP solution can dynamically detect zero-day threats and advanced malware without the need for static measures. Furthermore, the NGEP solutions should be able to detect attacks that exploit vulnerabilities in web browsers and documents, along with memory-based attacks (for example, heap spraying, stack pivots, ROP attacks, and memory permission modifications) and script-based attacks that are typically perpetrated by insiders.

POST-EXECUTION: MITIGATION, REMEDIATION AND REAL-TIME FORENSICS

Once an attack successfully executes on one or more endpoints, the organization remains vulnerable until security personnel can fully mitigate it, stopping its lateral spread and eliminating it from affected devices. Cyber attacks often create, modify, or delete system files and registry settings, as well as make changes to configuration settings. These changes or remnants can cause system malfunction or instability, and require substantial effort to clean up without the proper capabilities.

Many technologies today are focused on identifying and alerting to the existence of a threat. This sends incident response personnel into a scramble, armed with a combination of mitigation and forensics point tools and manual procedures through which attempts at finding and quarantining infected systems are made. Sometimes, expert security consultants are called in (at a considerable expense) when internal teams need assistance with mitigation, remediating affected files, or generating and interpreting forensic data.

Ultimately, the most effective response is one where attack mitigation and remediation are automatically executed at the initial point of detection, and are driven by detailed, real-time forensic data.

The most complete next-generation endpoint protection solutions take the holistic approach of integrating response capabilities with threat detection and prevention. This eliminates any potential interoperability issues between security tools, and ensures the fastest possible response time.

MITIGATION

Recommendation: the NGEP platform should support automated policy-based mitigation that is flexible enough to cover a wide range of use cases. For example: quarantining infected files, killing malicious processes, disconnecting infected machined from the network, or even shutting compromised devices down completely. Mitigation should be performed in a timely manner (for example, if the tool needs to phone home to a central server to receive a mitigation command the attack may still have time to spread laterally). Rapid mitigation during inception stages of the threat lifecycle will minimize damage and minimize the amount of remediation effort required.

REMEDIATION

Recommendation: the NGEP solution should be capable of easily remediating affected files by rolling them back to their last known trusted states.

FORENSICS

Recommendation: An NGEP solution should provide complete and granular visibility of what happened on an endpoint during an attack-- from source to target-- in real-time, and provide the capability to search for indicators of compromise across endpoints. Forensic data should be presented both in intuitive graphical format and in several file formats compatible with other security tools such as a SIEM.

©2016 SentinelOne. All Rights Reserved.

Beyond the Critical Capabilities: Important Solution Attributes

ALWAYS-ON PROTECTION

With the cloud changing the possibilities around where assets are located and how users can access them, the definition of an organization's perimeter has changed significantly. This further underscores the need for an autonomous endpoint agent that monitors and protects against cyber attacks, even when a user goes outside the workplace and connects to a much less secure environment.

> ***What to look for:*** The NGEP solution's ability to prevent and detect threats on the endpoint is independent of the endpoint device's network connectivity.

CROSS-PLATFORM SUPPORT

Organizations today support many different types of endpoint devices and platforms. An NGEP solution needs to offer the same level of protection across different types of laptops, desktops and servers.

> ***What to look for:*** Solutions that support devices running Windows, OS X, and different versions of Linux. All protected endpoints should be visible and manageable from a single console.

PERFORMANCE

When it comes to endpoint protection, performance continues to be a high-priority issue for endpoint users and data center administrators alike. Legacy AV solutions are notorious for degrading device performance as a result of periodic signature updates and scans. NGEP solutions must remain unobtrusive and cannot interfere with end-user productivity or precious server performance.

> ***What to look for:*** The best NGEP solution agents are extremely lightweight, and consume less than 2% of endpoint CPU cycles. For servers especially, it is critical that monitoring be performed out-of-band (as opposed to in-line) which can delay execution of applications.

FALSE POSITIVES

An NGEP solution should be intelligent enough to minimize false positives while maintaining high detection rates.

> ***What to look for:*** Solutions that can baseline an environment and learn what applications can and cannot be run.

SCALE

To be considered enterprise-ready, a NGEP solution needs to scale to hundreds of thousands of endpoints across both centralized and distributed environments. This requires that the agent be lightweight and easily deployable. Furthermore, the agent-to-server transport should be kept to a minimum, and the server itself should scale to support endpoint growth.

> ***What to look for:*** Avoid 'big data' type solutions that need massive storage and compute power on the server side in order to process large amounts of data. These solutions will typically not scale easily, and will introduce a lot of latency.

TAMPER PROOF

An NGEP platform must have strong measures in place to protect itself from malware or bad actors from disabling or interfering with that protection. As an NGEP solution becomes more effective and harder to evade, attackers will look for ways to compromise protection to increase the probability of a successful attack.

> ***What to look for:*** Agents that are active in both user space and kernel space are less likely to be circumvented, and solutions that have visibility into system events can, in most cases, detect tampering attacks, unlike solutions which don't monitor process execution.

INTEGRATION WITH OTHER ENTERPRISE SECURITY PLATFORMS

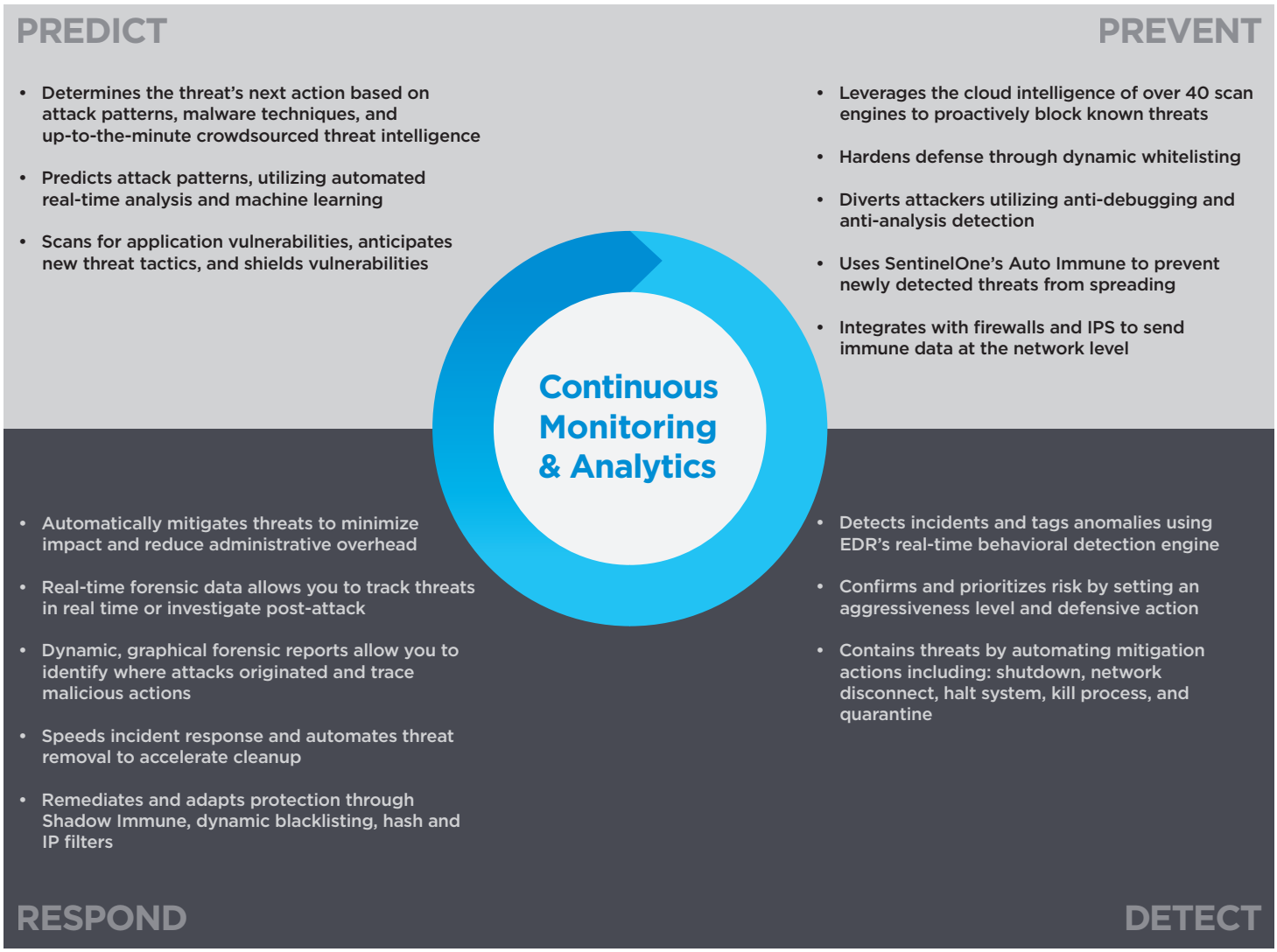
Enterprises use various solutions to collect threat information and indicators of compromise to monitor the health status of their environments and perform timely mitigation. While protecting endpoints is critical, an NGEP solution also needs to fit in well with the organization's overall security strategy by easily integrating with other infrastructure.

What to look for: Solutions that can offload indicators to SIEMs or other tools using industry standard formats (CEF, STIX, openIOC), and can integrate with leading network security solutions.

GARTNER ADAPTIVE SECURITY ARCHITECTURE

The adaptive security architecture as defined by Gartner includes four stages (Preventive, Detective, Predictive, and Retrospective) along with the assertion that continuous monitoring and analytics must serve as the core of the architecture. An NGEP solution should align with this architecture and its four stages in order "to deliver comprehensive, adaptive protection from attacks."

What to look for: Compare the NGEP solution to the Gartner Adaptive Security Architecture to ensure that its capabilities map to the four stages.



©2016 SentinelOne. All Rights Reserved.

CONCLUSION

Considering the growing diversity of devices and endpoint platforms coupled with a rapidly-evolving threat landscape, endpoint protection is more relevant and critical than ever before. Though there are several distinct approaches and solutions that fall under the umbrella of 'next-generation endpoint protection', there is a well-defined set of critical capabilities and attributes a NGEP solution requires in order to best serve today's enterprise organizations.

The solution must operate in a lightweight fashion on the endpoint itself, protect multiple platforms, and be effective against all major vectors of attack across the entire threat execution lifecycle. It must prevent known threats, use dynamic behavior-based threat detection, intelligently mitigate and remediate threats at machine speed, and generate detailed, real-time forensics.

ABOUT SENTINELONE

SentinelOne is a next-generation endpoint security company founded in 2013 by a group of Israeli cybersecurity experts who developed a fundamentally new, groundbreaking approach to endpoint protection. SentinelOne unifies endpoint threat prevention, detection and response in a single platform driven by sophisticated machine learning and intelligent automation.

With SentinelOne, organizations can predict malicious behavior across multiple vectors, rapidly eliminate threats with fully-automated, integrated response capabilities, and adapt their defenses against the most advanced cyber attacks. SentinelOne was the first company to coin the term "next-generation endpoint protection", and use it to describe its product offering, and vision.

www.sentinelone.com