SentinelOne

Web Copy – Home Page, 3 Category Pages, Product Page & Solutions

View Web Archive - Note: 4 top banners and some graphics do not appear
http://web.archive.org/web/20140826174137/http://www.sentinelone.com/

HOME PAGE

<PAGE TITLE and/or Browser tag for SEO>
SentinelOne – Endpoint Security: Advanced Threat Detection and Response

<**4 Rotating Banners** – not visible in web archive>
1

SentinelOne Endpoint Protection

Detects, predicts, and blocks advanced threats, giving you fully automated, real-time protection before, during, and after attacks.

Always on. Always secure.

Set up a demo >
How it works > link to EDR product page

2

SentinelOne Endpoint Protection

Only SentinelOne supports all major platforms—so you can unify protection, management, and visibility across Windows, Mac, Android, and soon, Linux.

Close the Security Gaps

Set up a demo >
See the advantage > link to platform category page

3

SentinelOne Endpoint Protection

Monitor and track threats as they unfold. The real-time defense system blocks and removes threats automatically.

Next-Generation Security

Set up a demo >
How it's better > link to solution page

4

SentinelOne Lab Report

What happens when cybercriminals get their hands on government-grade advanced threats? SentinelOne analyzes new tactics we can expect to see more.
Read our threat blog >

3 COLUMNS below top banner:
FEATURES

Predictive Execution Inspection

Powered by the industry's first and only predictive execution inspection engine, SentinelOne rapidly adapts and responds to threat activity.

Stop more threats >

Automated Response and Mitigation

Cut down your incident response time from hours to milliseconds. With real-time forensics, you can track and investigate attacks as they attempt to execute.

Keep business humming >

Universal Platform Protection

SentinelOne supports all major platforms—Windows, OS X, Android, and soon iOS and Linux—more than any other vendor. With one solution and lightweight agents, stop advanced threats from slipping between the cracks.

Close the gaps >

<Section 2>

Next-Generation Endpoint Protection

<Insert UI image>

By rethinking the sequence of malware detection, we've built a new paradigm that puts security ahead of threats, even zero-day and targeted attacks.

At the first sign of suspicious activity, SentinelOne Endpoint Protection predicts threat behavior and blocks the attacker's next move.

Fully automated cross-platform security

- Monitors activity at all times—without slowing performance
- Detects, predicts, blocks, and removes threats in real time
- Lowers costs with a faster, fully automated threat response
- Correlates and shares threat data to improve security
- Supports all major platforms to ensure universal protection

See how it works >

RIGHT COLUMN PROMO

Fight Back with Intelligence

SentinelOne Endpoint Protection detects threat behavior, predicts the next move, and blocks the attack.

The future of security is here >

<QUOTES>

< Netfilx, Yahoo, and Box logos go here>

IT experts say…

"SentinelOne's unique lightweight agent-based [security]…is the solution that we've been waiting for.**"**

- Netflix, VP of IT Operations Mike Kail

<Full quote for roll-over balloon>

"Signature-based endpoint security solutions were never a great solution, and the convergence of cloud, consumerization and always-mobile means that endpoint protection is more important than ever. SentinelOne's unique lightweight agent-based solution, combined with the management console and global threat feed, is the solution that we've been waiting for."

- Netflix, VP of IT Operations Mike Kail

"I believe SentinelOne represents the future of [advanced persistent threat] detection.**"**

- Yahoo, CISO Alex Stamos

<Full quote for roll-over balloon>

"I believe SentinelOne represents the future of APT detection. Targets of APTs that have deployed the leading centralized solutions are starting to deal with their serious downsides. SentinelOne solves these problems by running on the targeted host and detecting successful compromise."

- Yahoo, CISO Alex Stamos

"Sentinel is providing a critical solution…that will benefit the entire industry."

- Box, Chief Trust Officer Justin Somaini (former Symantec CISO and SentinelOne advisor)

<Full quote for roll-over balloon>

"With the onslaught of malicious actors deploying advanced malware and the limitations of existing antivirus software, SentinelOne is providing a critical solution to this problem. A solution that will benefit the entire industry.**"**

- Box, Chief Trust Officer Justin Somaini (former Symantec CISO and SentinelOne advisor)

<SECTION 3>

View Endpoint Activity in Real Time

<Insert Image: Management Portal UI>

This is a small sample of the data you can view in real time. Our management portal allows you to see what's happening at all times, across all endpoints, local and remote. With one solution using lightweight agents, you can secure all major platforms and track threats as they unfold.

END HOME PAGE

SentinelOne - **3 Category Web Pages**

Archived Web Page – Category 1
http://web.archive.org/web/20150102192805/http://www.sentinelone.com/adaptive-threat-protection/

1 of 3 TOPICS: Category 1 - Protection

Adaptive Threat Protection

Next Generation Endpoint Security

Unlike static antivirus filters, predictive behavioral patterning is truly dynamic. SentinelOne Endpoint Security responds to what is happening on your endpoints in real time.

3 Layers of Protection

1. Prevents Threats at Inception

Our first line of defense stops the majority of malware, even one-of-a-kind advanced threats, by detecting and predicting threat behavior the instant it starts.

- Monitors all endpoint activity at all times, tracking each newly-created process to detect memory modifications, heap spray attempts, and exploitation techniques
- Predicts what the threat will do next based on attack patterns, evasion techniques, and up-to-the-minute crowdsourced threat intelligence
- Moves ahead of the attack to block its next move in real time

<Middle column>

<Insert graphic illustrating 3 layers>

2. Stops Attacks as They Unfold

Application monitoring runs non-stop to catch the small percentage of threats that progress to the next stage.

- Analyzes threat behavior based on low-level instrumentation of all OS activities and operations, including memory, disk, registry, network, and more
- Detects and tags anomalies using behavioral logic derived from advanced clustering techniques and machine learning
- Predicts the attack sequence, using dynamic behavioral patterning to accurately sort, optimize, and match the type of attack
- Stops the threat from fully executing to prevent damage and data loss
- Creates and shares behavioral patterns to prevent the spread of infection to other endpoints

<Right column>

3. Detects and Removes Active Threats

As a last line of defense, our advanced threat sensors detect, block, and remove advanced threats that are already entrenched.

- Finds hidden threats by detecting kernel tampering, exfiltration attempts, and aberrant behavior, including “low and slow” stealth activity that’s invisible to other defenses
- Shuts down the attack, removes malware, cleans up any damage, rolls back changes, and alerts administrators to a security breach—a fully automated incident response
- Minimizes damage and data theft by reducing threat dwell time
- Shares new threat intelligence to prevent reinfection and protect all endpoints in the crowdsourced community, creating a full circle defense system

See a Demo >

View Product Page >

END CATEGORY 1 PAGE

CATEGORY 2 PAGE – AUTOMATED RESPONSE

View Web Archive: http://web.archive.org/web/20140828081950/http://www.sentinelone.com/automated-response-and-mitigation/

Automated Response and Mitigation

The Need for Speed

Targeted attacks are designed to gain high privileges and evade detection while they quietly collect and exfiltrate your confidential data over the course of months, even years. SentinelOne tackles this problem with a fully automated real-time threat defense system that prevents or minimizes dwell times and costly damage.

<3 column format>

Automates Response & Removal

Every step is fully automated, from behavioral detection to threat prevention and remediation. SentinelOne monitors, predicts, blocks, and removes threats at every stage of attack.

- Delivers faster protection with a built-in response chain, so there are no delays, no security gaps
- Removes threats for you—unlike other EDR solutions that offer suggestions on how you might be able to remove the threat yourself, a difficult and tedious task
- Eliminates or minimizes the need for incident response and policy management
- Reduces the time and cost to manage security across all endpoints, local and remote

<Middle column>

<Insert image from Management UI>

Maximizes Visibility & Control

Real-time forensic tools and graphical reports give you full visibility through a single management console, accessible from any device, anywhere.

- Empowers you with real-time forensics to monitor endpoint activity and track threats as they attempt to execute
- Reflects the current status of your security posture across all endpoints in real time
- Identifies security events, attack patterns, and threat vectors so you can reduce risk
- Provides the information you need to prove compliance with industry regulations and speed security audits

<Right column>

Eliminates Performance Drag

High-volume antivirus scans slow endpoint performance and employee productivity to a crawl. With a lightweight security client, SentinelOne speeds throughput to provide a truly agile, efficient solution ideal for today's mobile workforce.

- Monitors, predicts, and blocks attack behavior based on dynamic, up-to-the-minute threat intelligence—so there are no static signatures, whitelists, and static IOCs to slow you down
- Observes processes by trailing them, adding less than a microsecond per monitored process with an average CPU usage of 0.4 percent

- Speeds throughput as a fully distributed system that uses a local client to secure every endpoint, a key advantage over network-based security

- Minimizes or eliminates helpdesk calls related to performance drag or system crashes, saving you time and costs

See a Demo >

View Product Page >

END CATEGORY 2

Category 3 – Platforms

View web page archive:
http://web.archive.org/web/20140828002523/http://www.sentinelone.com/universal-platform-protection/

Universal Platform Protection

Expand Protection as You Need It

Why limit your options? SentinelOne provides the broadest platform support of any endpoint security solution on the market today. Plus you can choose the deployment method that meets your IT and cost requirements.

<3 column format >
<Left column>

Close the Security Gap

As the only vendor to secure all major platforms, SentinelOne offers many advantages:

- Unifies protection across Windows, Mac, Android, and soon Linux—all with a single solution

- Frees you from the headache of managing multiple disparate endpoint security products

- Bridges the IT silos that separate platforms to prevent threats from slipping between the cracks

- Improves security with a single pane of glass for visibility and control across all endpoints

- Integrates with your existing SIEM or logging solutions and can be configured to communicate with your firewall or intrusion prevention systems (IPS) to block attacks at the gateway

Supports the most platforms:

- Windows
- OS X
- iOS (coming soon)
- Android
- Linux (coming soon)

<Middle column>

A single solution secures:

- Smartphones and tablets
- Laptops and desktops
- Virtual desktop infrastructure (VDI)
- Servers, physical and virtual
- Embedded systems, like PoS
- Critical infrastructure, like SCADA

Deployment Options

SentinelOne endpoint security runs on a client/server model. The server can be deployed in a private cloud or as a virtual appliance. Our IT experts can help you decide what's best and will do the installation for you. Each deployment mode offers its own advantages:

1. Secure Cloud

   Using a private cloud server is arguably the most secure, maintenance-free, cost-effective, and elastic deployment for a variety of reasons:

   - Provides a secure path for communication with encrypted tunnels
   - Connects the server with your endpoint clients everywhere they go, whether on or off network, giving you better visibility of endpoint activity at all times
   - Lowers costs relative to deploying a local server, which is more expensive and requires onsite administration
   - Scales to accommodate your ever-changing user population—whether it's growing or shrinking—you only pay for what you need
   - Eliminates server maintenance so you don't have to worry about patches or fixes

<Right column>

2. Virtual Appliance

   A virtual appliance is also cost-effective, scalable,

secure, and easy to deploy, but for different reasons:

- Reduces security risks with a cut-down virtual appliance that does just what is needed, avoiding unnecessary exposure to other apps
- Runs only the bare necessities to optimize efficiency and eliminate the need for manual tuning
- Comes with the OS and SentinelOne application installed, preconfigured, and ready to go, making it easy to deploy
- Lowers costs by allowing you to use spare capacity on an existing server when needed to scale

See a Demo >

END Category Pages

Product and Solutions Pages

View Archived Product Page – Note: some graphics do not appear
http://web.archive.org/web/20140827183920/http://www.sentinelone.com/product/

SentinelOne Endpoint Detection and Response

A true breakthrough in IT security, SentinelOne EDR is the first and only solution designed to predict threat behavior and block attacks the instant they strike. Powered by our predictive execution modeling engine and military-grade cyber defense technologies, this cross-platform endpoint suite provides unparalleled protection against today's advanced threats and future attacks.

True Behavioral Detection and Real-Time Protection

- Monitors endpoint activity and gives you full visibility at all times, using a lightweight client that never slows performance
- Detects threat behavior and predicts the next move with phenomenal accuracy
- Blocks and removes advanced threats automatically, in real time—unlike products that just alert you to threats
- Secures the most platforms, so you can unify protection across Windows, OS X, Android, and soon iOS and Linux
- Works with your existing endpoint antivirus security and integrates with your firewall, IPS, network security, and more
- Improves security, speeds response time, and minimizes management with one automated solution for desktops, laptops, tablets, smartphones, servers, VDI, critical infrastructure, like SCADA, and embedded systems, like point-of-sale

WHY IT'S REVOLUTIONARY

Dynamic Prediction

SentinelOne EDR is the first and only solution to predict the attack sequence—a giant leap in security innovation. The predictive execution modeling engine determines what the threat is likely to do next, based on attack patterns, malware techniques, and up-to-the-minute crowdsourced threat intelligence. With dynamic behavioral patterning, SentinelOne security is able to sort, optimize, and match the type of attack with superior accuracy.

Faster Detection

Unlike antivirus solutions that focus on static signatures and known binaries, SentinelOne EDR is focused on threats and how they behave. The lightweight native client monitors all endpoint activity, both on and off network, tracking each newly-created process from beginning to end. By building a full context around every process execution path in real time, our predictive execution modeling engine detects, predicts, and blocks threat behavior—instantly.

Automated Defense

By predicting threat behavior, SentinelOne EDR can move ahead of the attack and block its next move. This proactive defense system is fully automated to stop and remove malware without delay. In most cases, it prevents infection and eliminates the need for incident response—delivering much more than other EDR solutions <link to competitive matrix> that stop short of remediation.

Full Remediation

SentinelOne EDR goes the full distance, automating remediation and threat removal. By rapidly responding to active malware infections, it reduces dwell times and minimizes damage. Other EDR products will just alert you to a new attack and provide recommendations on how you might be able to block and remove the malware yourself. This will significantly add to your costs in terms of prolonged data theft and administrative overhead.

Hacker Proof

SentinelOne EDR is immune to evasion techniques used to bypass network security because our core detection engine runs on the endpoint, the attacker's target. It sees what is happening on your device and responds based on dynamic real-time data versus static signatures, IOCs, or whitelists. It doesn't need prior knowledge of a specific binary to block an attack, making it the first true defense against one-of-a-kind advanced threats and targeted attacks.

Extensive Coverage

SentinelOne covers all vectors and detects all variants based on behavior patterns and techniques, like heap spray, memory modification, and disk payload drops. Using behavioral logic, it even detects new patterns of attack to catch zero-day and polymorphic malware designed to slip past AV security, breach detection systems, and sandboxing.

No Delays

A thin client runs on every endpoint without slowing performance. Unlike high-volume antivirus scans that interrupt system processes, our agent simply observes, trailing the processes, not delaying them. SentinelOne EDR is also fully distributed, since each endpoint is secured by its own client. This turns every endpoint into a detection sensor, improving protection and eliminating throughput issues, a common problem with network-based security.

Low Maintenance

Every step is automated—to speed response times, minimize damage, and reduce administration. All infections are signed, pushed to your endpoints, and shared with the crowdsourced SentinelOne community. This intelligent, built-in response chain minimizes the time and cost to manage security across all endpoints, local and remote. A central management console and real-time reports give you full visibility and forensic tools, accessible from any device, anywhere.

Custom Fit

With the broadest platform support available, SentinelOne ensures universal protection across all endpoints on Windows, OS X, iOS, Android, and soon, Linux. Depending on your needs, it can be deployed in a private cloud or as

a virtual appliance. Sentinel's IT pros do the installation and configure the agents for you—so security is optimized for your IT environment. SentinelOne EDR also integrates with your existing SIEM or logging solutions and can be configured to communicate with your firewall or IPS to block attacks at the gateway.

<Insert platform logos here>

<Insert final competitive matrix – caption and image TBD>

<RIGHT SIDEBAR>

Our Solutions

Adaptive Threat Protection **>**

Automated Response and Mitigation **>**

Universal Platform Protection **>**

Key Features

- True behavioral detection
- Social engineering protection
- Drive-by download prevention
- Targeted attack detection
- Exploitation prevention
- Automated threat removal
- Cross-platform support
- Endpoint remote control
- Real-time forensics
- Lightweight client
- Unified console
- Integration with SIEM or logging solutions
- Complementary to existing security

Support Forum >

IT experts say…

Netflix

"Signature-based endpoint security solutions were never a great solution, and the convergence of cloud, consumerization and always-mobile means that endpoint protection is more important than ever. SentinelOne's unique lightweight agent-based solution, combined with the management console and global threat feed, is the solution that we've been waiting for."

Netflix
Former VP of IT Operations, Mike Kail

Yahoo!

“I believe SentinelOne represents the future of APT detection. Targets of APTs that have deployed the leading centralized solutions are starting to deal with their serious downsides. SentinelOne solves these problems by running on the targeted host and detecting successful compromise.”

Yahoo
CISO, Alex Stamos

Box

“With the onslaught of malicious actors deploying advanced malware and the limitations of existing antivirus software, SentinelOne is providing a critical solution to this problem. A solution that will benefit the entire industry.”

Box
Chief Trust Officer (former Symantec CISO and SentinelOne advisor), Justin Somaini

<END PRODUCT PAGE>

SentinelOne - **SOLUTIONS PAGE**

View web archive:
http://web.archive.org/web/20140827192828/http://www.sentinelone.com/solutions/
Note: accordions and other a few other elements don’t appear on the archived page

Reinventing Endpoint Security

Advanced Threats: The Dramatic Shift

Targeted attacks and advanced threats are more sophisticated than ever. They are specifically designed to infiltrate your organization and slip past security, using one-of-a-kind polymorphic malware and obfuscation techniques to avoid detection. Once inside, they set up command and control (C&C) communications, open backdoors, and steal your valuable data.

Endpoints Are the Initial Target

Most attacks start by targeting your endpoints, where your organization is most vulnerable. It may take many attempts, but your attackers will keep trying until they find a way to penetrate via apps, browsers, operating systems or social engineering—any way they can.

Antivirus Security is Obsolete

Conventional signature-based antivirus (AV) is no longer working. It was moderately effective 25 years ago when it was first developed, but for too long it has failed on many levels**…>** <Click to expand bullets in accordion>

- Each static signature file only protects against one threat; it cannot detect variants nor unknown threats
- New malware must first be identified by the AV lab, leaving you vulnerable to zero-day and targeted attacks
- With a million new threats created every day, AV security cannot keep pace
- High volume signature-file scanning slows endpoint performance and productivity to a crawl
  <End accordion>

Network Monitoring Falls Short

Network-based monitoring and sandbox analysis once offered hope for detecting advanced threats, but too often they fail to prevent and remediate damage. Attackers have developed anti-virtual machine techniques to create sandbox-aware malware that will act benign until it is running on an unprotected device. Other reasons breach detection systems are not as effective**…>** <Accordion>

- Encryption, packers, and other tricks can prevent you from gaining access to the binary
- Malware may sleep for a long time before it executes to avoid detection
- Most network monitors stop short of remediation, leaving you with the task of threat removal
- Slows throughput due to long queues for sandbox analysis and processing time
  <End accordion>

Reinventing Cyber Security

It's clear we need a new approach to endpoint security—one that doesn't rely on static signatures, whitelists, or static IOCs. We also need faster, ongoing incident response to reduce dwell times and costly damage. Prevention alone is not enough. Analysts and security pros agree: we have to assume some threats will slip past even the best security.

A Total Defense System

To overcome these challenges, the cyber defense experts at SentinelOne built a dynamic endpoint security platform to continuously monitor, predict, block, and remove threats at every stage of attack.

A new class of Endpoint Detection and Response (EDR) solutions <link to competitive matrix> attempts to do some of this, but only SentinelOne EDR <link to product page> provides a fully integrated adaptive defense system to address the entire threat lifecycle—before, during, and after attack.

<Insert **Gartner** circle graphic here>

Four Layers of Adaptive Protection

1. Prevents initial exploits
2. Stops threats as they attempt to execute
3. Detects and removes hidden infiltrations
4. Continually learns and improves security based on the latest threat data

Real-Time Threat Prediction

A few security vendors claim to "predict" threat behavior, but in most cases they are not doing it in real time. Instead, they are researching the hacker underground to anticipate new types of attacks and then adding hardened defenses and addressing exposures.

SentinelOne does this too, but we take prediction much further than that. Our patent-pending predictive execution modeling engine predicts threat behavior in real time, as the threat unfolds. This allows us to move ahead of the attack and block its next move—instantly. Our researchers do not have to identify it first.

Set It and Forget It

Most EDR solutions require dedicated IT staff to effectively sort through massive amounts of data. In contrast, SentinelOne endpoint protection is fully automated, requiring almost zero administration. Up-to-the-minute threat intelligence, contextual data, and threat activity are correlated automatically in real time—to deliver faster protection and minimize or prevent damage.

True Remediation

SentinelOne endpoint protection goes the full distance, automating cleanup and threat removal. This is a significant advantage over network and endpoint monitoring products that stop short of remediation. In most cases, they will

alert you to a new attack and provide recommendations on how you might be able to block and remove the malware yourself. This is no easy task and will add to your administrative overhead.

Bridge the IT Silos

SentinelOne endpoint protection secures all major platforms—more than any other endpoint security. With a single pane of glass, you can now unify protection across Windows, OS X, Android, and soon iOS and Linux.

There's no need to manage multiple disparate products to secure each platform. This only increases costs and decreases effectiveness. By closing the gaps that separate platforms, SentinelOne endpoint protection improves security and visibility across all endpoints, from data centers to smartphones.

See how it works > <Link to EDR product page>

<RIGHT SIDEBAR>

Our Solutions

Adaptive Threat Protection **>**

Automated Response and Mitigation **>**

Universal Platform Protection **>**

One single solution secures:

- Desktops
- Laptops
- Virtual desktop infrastructure (VDI)
- Tablets
- Smartphones
- Physical and virtual servers
- Embedded systems, like PoS
- Critical infrastructure, like SCADA

Supports the most platforms:

- Windows
- OS X
- iOS (coming soon)
- Android
- Linux (coming soon)

Detects and Blocks Malicious Activity

Anti-exploitation

- Memory modifications
- Heap spray detection
- Advanced randomization
- Java sandbox breaches
- Disk payload drops

- Memory payload executions

Behavioral-based detection

- Low level and kernel-based monitoring
- Malware execution patterns
- Phishing attacks
- Browser based attacks
- Exfiltration attempts, and more

Support Forum >

IT experts say…

Netflix

“Signature-based endpoint security solutions were never a great solution, and the convergence of cloud, consumerization and always-mobile means that endpoint protection is more important than ever. SentinelOne’s unique lightweight agent-based solution, combined with the management console and global threat feed, is the solution that we’ve been waiting for.”

Netflix
Former VP of IT Operations, Mike Kail

Yahoo!

“I believe SentinelOne represents the future of APT detection. Targets of APTs that have deployed the leading centralized solutions are starting to deal with their serious downsides. SentinelOne solves these problems by running on the targeted host and detecting successful compromise.”

Yahoo
CISO, Alex Stamos

Box

“With the onslaught of malicious actors deploying advanced malware and the limitations of existing antivirus software, SentinelOne is providing a critical solution to this problem. A solution that will benefit the entire industry.”

Box
Chief Trust Officer (former Symantec CISO and SentinelOne advisor), Justin Somaini

<END Sidebar>
<END Solutions Page >