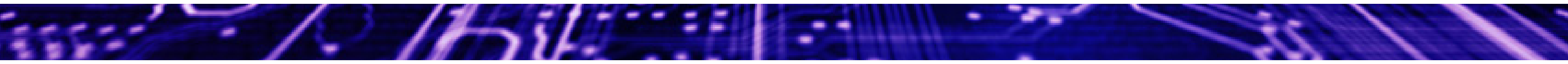
Secureworks®

DATA SHEET

Advanced Endpoint Threat Prevention

Managed Next-Generation Antivirus



Gaps in traditional, signature-based antivirus are driving many organizations to move to more effective Next-Generation Antivirus (NGAV). While NGAV provides more robust protection for your endpoints, you may struggle with how to best implement this new technology and sort alerts that require attention from the noise. Managed NGAV provides stronger threat prevention with less effort.

The Evolving Threat Landscape

Malicious activity continues to increase despite the widespread use of traditional antivirus, with over 250,000 new malware-based threats registered daily by the AV-TEST Institute[1]. The rapid evolution of new and existing threats, combined with the difficulty of ensuring your software and hardware are properly patched against known and new vulnerabilities, creates security gaps. As a result, you must be aware of new threats and those that use pre-existing, business-critical software and applications to achieve their malicious ends. You need a new approach to better protect your organization.

How Secureworks Helps

Traditional endpoint threat protection technologies, like signature-based antivirus, simply can't keep up with the constantly evolving threat landscape. NGAV identifies more threats without the need for signature updates, but requires skills and time to properly configure the technology and investigate alerts.

The Secureworks Advanced Endpoint Threat Prevention (AETP) service empowers you to adopt new and better security technologies. We enhance advanced NGAV technology with Secureworks supervised machine learning and human intelligence to identify more threats faster. Our proven Threat Intelligence and skilled analysts help you reduce risk and identify the signal through the noise.

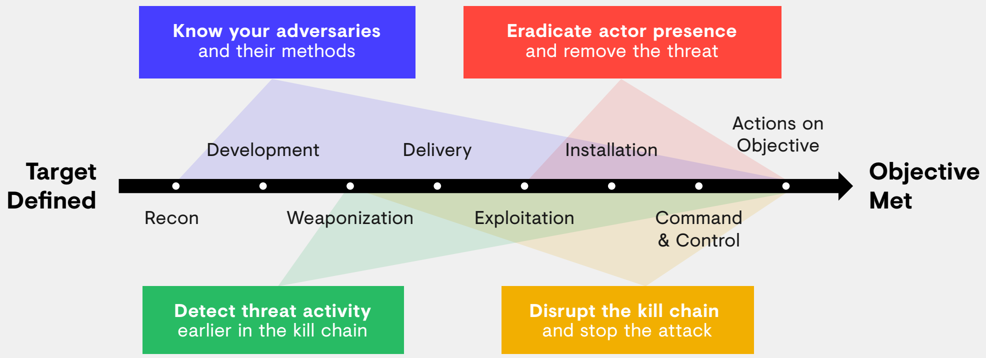
Client Benefits

- Speed time to protection and reduce TCO with a fully managed and hosted solution
- Prevent advanced attacks that evade traditional antivirus
- Eliminate time wasted investigating false positives and noncritical events
- Certified as an antivirus replacement for PCI and HIPAA compliance

Solution Features

- Lightweight sensors continuously monitor endpoints for indicators of compromise
- Streaming prevention analyzes the entire attack sequence to stop threats before they execute their payload and compromise your system
- Threats are blocked where possible and alerts are generated for investigation
- Secureworks Senior Intrusion Analyst team investigates alerts and escalates critical issues

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.


Know your adversaries and their methods
Eradicate actor presence and remove the threat
Target Defined
Development
Delivery
Installation
Actions on Objective
Objective Met
Recon
Weaponization
Exploitation
Command & Control
Detect threat activity earlier in the kill chain
Disrupt the kill chain and stop the attack

The Kill Chain

Speed Matters

The Secureworks AETP service utilizes proprietary systems and Threat Intelligence developed by our Counter Threat Unit™ (CTU™) researchers and Senior Intrusion Analyst team. This combination of supervised machine learning and human intelligence has proven to be effective in detecting advanced threats across hundreds of thousands of endpoints. The faster you detect and stop threats, the lower the costs to your business.

The Kill Chain[2] is the high-level framework or workflow employed by threat actors to compromise a target. Threat actors may have time and a toolbox of exploit techniques and intrusion tools at their disposal, but disrupting any part of this chain thwarts their efforts.

The further along the chain that a threat actor gets, the more difficult and expensive it is to defeat them. The key to breaking the kill chain is to identify and stop threats as early as possible, because costs rise as soon as the threat actor expands beyond the endpoint and into your environment. This is why replacing outdated antivirus with the more effective NGAV is so important.

Streaming prevention and NGAV protection move beyond signatures, helping you identify more threats, including those that use little or no malware and often evade traditional antivirus. Secureworks Threat Intelligence and experienced analysts enhance this technology to eliminate time wasted on minor issues and false positives, so your security team can focus on what's important to your business. This is how the Secureworks Advanced Endpoint Threat Prevention service allows you to see more, know more and defend faster.

> ***"Speed is always a factor when it comes to security. If the adversary can outpace us, they can outmaneuver us."***
>
> **Jon Ramsey**
> Senior Vice President
> Chief Technology Officer,
> Secureworks
>
> Cybersecurity Trends: What to Expect in 2018 and Beyond →

Source:

[1] AV-TEST, Malware Statistics, https://www.av-test.org/en/statistics/malware/

[2] Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains; Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.; Lockheed Martin Corporation; http://papers.rohanamin.com/wp-content/uploads/papers.rohanamin.com/2011/08/

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com

Secureworks®

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.