DATA SHEET

Advanced Endpoint Threat Detection

Enhanced with SecureWorks Counter Threat Unit™ Research Team Endpoint Intelligence

Advanced Visibility into Endpoints

Security teams are increasingly aware of the risk posed by advanced threat actors bypassing existing security controls via phishing, social engineering and exploiting vulnerabilities in endpoints (servers, laptops and desktops). As a result, security leaders must adopt detection capabilities to monitor endpoints for advanced threats as part of their defense-in-depth security posture.

Employing proprietary SecureWorks Counter Threat Unit™ (CTU) research team Endpoint Intelligence technology, the SecureWorks Advanced Endpoint Threat Detection service gives you the earliest possible warning that your endpoints may be hosting an advanced adversary. The service heightens your security situational awareness by warning you when endpoints may have been compromised and accelerates remediation efforts by pinpointing exactly which systems are compromised, how they were compromised and how you can repair them.

Benefits

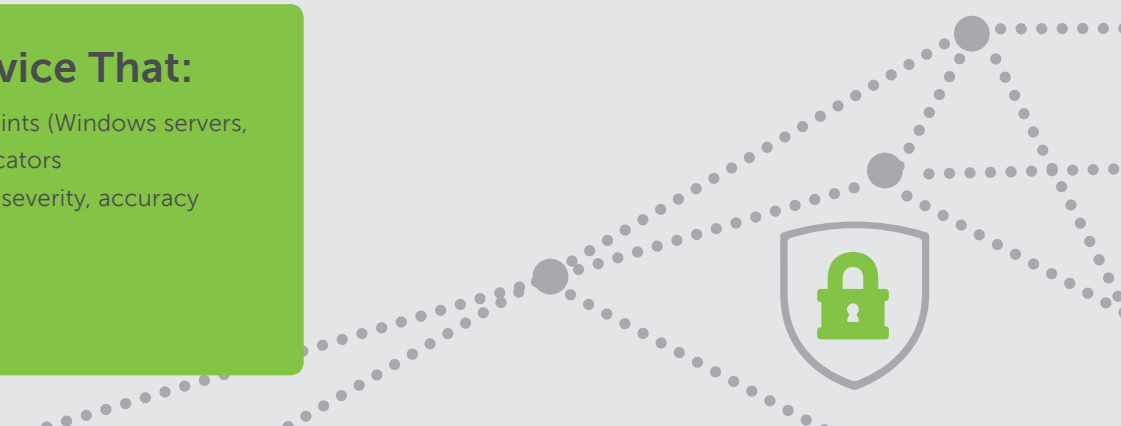
- Improves situational awareness by detecting signs of endpoint compromise
- Accelerates response times by pinpointing affected systems quickly
- Reduces costs by allowing patching of systems versus reimaging
- Reduces exposure to targeted threats and fortifies defenses
- Minimizes the extent of data loss
- Increases confidence in system integrity and data confidentiality

How it Works

The Advanced Endpoint Threat Detection service utilizes lightweight sensors across your servers, laptop and desktop. The sensors continuously monitor registry, file system, process tables, memory and other areas of operation for signs of compromise. The "always-on" nature of the solution gives you the earliest possible warning when threat indicators are detected.

A Fully Managed Service That:

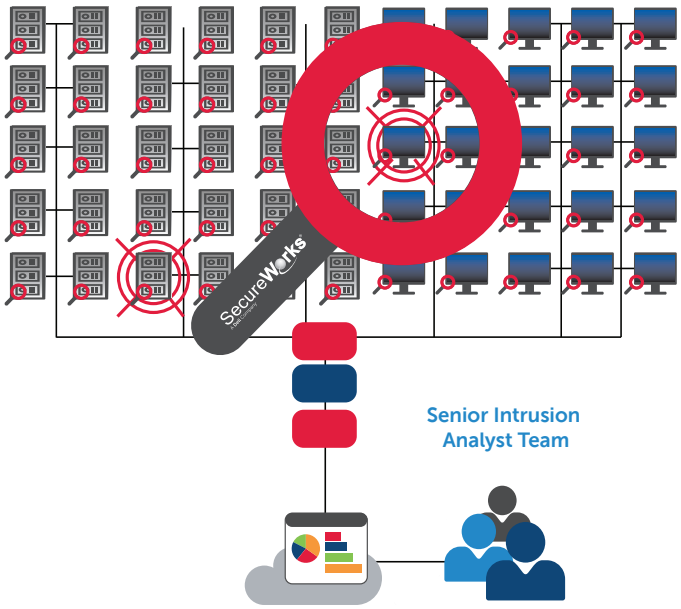
- Monitors the state of your endpoints (Windows servers, laptops, desktops) for threat indicators
- Investigates events to determine severity, accuracy and context
- Quickly escalates critical events



Telemetry is sent to a powerful analytics console that applies tactical and strategic intelligence from our CTU research team. If a threat is detected, an alert will be generated.

Alerts are investigated by our Senior Intrusion Analysts within the Counter Threat Operations Centers (CTOCs). Because sensors extensively record activity taking place at each endpoint, analysts are able to pinpoint any threat and determine how and when it entered the environment.

The Senior Intrusion Analyst then conducts research using our Threat Intelligence Management System (TIMS) and other available information from your environment to add richer context on the threat — who may be behind it, what else to look for and what next steps are appropriate for remediation. Once the advanced analysts have determined the severity of the alert, they escalate critical alerts to you promptly.



Proven Intelligence

The Advanced Endpoint Threat Detection service utilizes proprietary Endpoint Intelligence technology developed by the CTU research team. This technology has proven to be effective in detecting advanced threats through its use in Targeted Threat Hunting engagements across hundreds of thousands of systems.

Enhanced Visibility

Combined with advanced network threat detection, Advanced Endpoint Threat Detection sensors let SecureWorks analysts and responders see activity from initial breach of an endpoint by a threat actor to the actor's lateral movement across your network environment.

Optimized Response

Advanced Endpoint Threat Detection sensors record all pertinent activity taking place on endpoint devices. This allows our Senior Intrusion Analysts to effectively go back in time to pinpoint exactly when a breach occurred, its cause and where any malware may have spread. This precision means that any response efforts are targeted and less costly because Incident Response teams are able to eradicate threats sooner in the threat actor kill chain. In addition, detailed sensor information allows security teams to patch an exploited vulnerability versus reimage entire systems.

SecureWorks provides an early warning system for evolving cyber threats, enabling organizations to prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform – our advanced data analytics and insights engine – SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.

より詳細な内容に関しては下記のメールアドレスにご連絡ください
SWRX_PreSales@Dell.com
代表03-6893-2317
www.secureworks.jp/
SecureWorks Japan株式会社