Secureworks

DATA SHEET

Advanced Endpoint Threat Detection *Powered by Red Cloak™*

Reduces Time to Detect and Effort to Respond With Carbon Black Technology

Endpoint Detection and Response

Security teams are increasingly aware of the risk posed by advanced threat actors bypassing existing security controls and threat prevention tools via phishing, social engineering and exploitation of unpatched vulnerabilities in servers, laptops and desktops. As a result, your security strategy must include 24x7 endpoint protection to identify advanced threats and threat actors who may infiltrate your organization with little or no malware.

Employing strong technology, the Secureworks Counter Threat Unit™ (CTU™) Research Team and Threat Intelligence, the Secureworks Advanced Endpoint Threat Detection (AETD) solution gives you the earliest possible warning that your endpoints may be hosting an advanced adversary. The solution elevates your security situational awareness by warning you when endpoints may have been compromised and accelerates remediation efforts by identifying which systems are compromised, how they were compromised and how you can repair them.

How AETD Works

Our AETD solution utilizes lightweight sensors to gather security specific telemetry from your servers, laptops and desktops. The sensors continuously monitor the registry, file system, process tables, memory and other areas for potential compromise. The “always-on” nature of the solution with 24x7 protection gives you the earliest possible warning when threat indicators are detected, even when your endpoints are disconnected from the corporate network.

Sensor telemetry is sent to powerful analytics systems that apply a combination of supervised machine learning and human intelligence to identify more threats faster. Threat Intelligence from our CTU research team helps eliminate time wasted on minor issues or false positives, so your security team can focus on what’s important. If a threat is detected, an alert is automatically generated.

Alerts and suspicious activity are investigated in more depth by Secureworks. Because sensors record a wide range of activity taking place on each endpoint, analysts are able to pinpoint threats and

Client Benefits

- Gain heightened visibility across your endpoints
- Detect threats that may be invisible to other security tools
- Accelerate response with critical event escalation including remediation guidance
- Fortify defenses and increase the value of your other security tools by helping to validate their output
- Minimize data loss and other damage by identifying affected systems quickly
- Increase confidence in system integrity and data confidentiality

determine how and when they entered the environment. AETD can even identify threats that use no malware and threats that slip past security technology alone.

Our analysts use a variety of public and proprietary tools, combined with information from your environment to add enriched context to the alert, such as who may be behind the attack, which endpoints are impacted, what else to look for across your organization and what next steps are appropriate for remediation. Once we have determined the severity of the issue, critical alerts are promptly escalated to you.

Carbon Black Cb Response

Cb Response is a highly scalable Endpoint Detection and Response (EDR) technology that provides visibility for top security operations centers and incident response teams. No prevention technology can stop all threats and an attacker only needs to breach one endpoint to infiltrate your organization so endpoint visibility is critical. Cb Response captures detailed security related information from your Windows, macOS and Linux endpoints, giving analysts and incident responders a more complete understanding of the threat. Isolation of infected systems helps prevent lateral movement and enables removal of malicious files. Cb Response allows you to see what happened with clear attack chain visualizations that help uncover the root cause, so you can quickly address gaps in your defenses.

Proven Intelligence and Heightened Visibility

AETD leverages strong EDR technology and Threat Intelligence developed by the Secureworks CTU Research 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.

Sensors record all pertinent activity on your endpoints so our security analysts can pinpoint when a breach occurred, the cause and to where the threat actor and malware may have spread. This precision means you can eradicate threats earlier in the kill chain with response efforts that are targeted, more effective and less costly.

Detailed alerts with business context help reduce costs by allowing your security team to patch exploited vulnerabilities versus reimaging entire systems in hopes of evicting threat actors. Insights from our experienced analysts help you see activity from the initial breach to lateral movement across your organization. We help eliminate time wasted on minor issues and false positives, so you can focus on what's important to your business. This is how AETD allows you to see more, know more and defend faster.

"AETD offers unique and comprehensive detection capabilities built on CTU Threat Intelligence. We deploy thousands of tripwires that allow us to identify threats in many different ways. The concept is similar to defensive strategies employed by physical security practitioners for years. The adversary may observe and evade some detections successfully, however, it's very difficult to evade them all. It only takes one detection to call attention to an adversary's activity and allow the defender to take action."

Justin Turner
Senior Director, Counter Threat Unit

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 **1800 737 817** to speak to a Secureworks security specialist.
secureworks.com.au