

Advanced Endpoint Threat Detection *Powered by Red Cloak™*

**Reduces Time to Detect and Effort to Respond
with CrowdStrike 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 a 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,

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

analysts are able to pinpoint threats and 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.

CrowdStrike Falcon Insight: Setting the New Standard in EDR

Falcon Insight is CrowdStrike's endpoint detection and response (EDR) solution. It allows you to quickly uncover attackers in your organization and remediate the situation with the help of real time visibility, forensic data and response tools.

Key product capabilities include:

- Automatic behavioral indicator of attack (IOA) detection and accelerated investigation work flow
- Gain full-spectrum visibility across all endpoints in real time
- Five-second search to discover and investigate current and historic endpoint activity

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.™

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.

Solution Features

- Lightweight sensors gather security specific telemetry, even when endpoints are disconnected or outside the corporate network
- Sensors continuously monitor the registry, file system, process tables, memory and other areas for indicators of compromise
- A combination of supervised machine learning and human intelligence is applied to endpoint telemetry to identify more threats faster
- Alerts are investigated by Secureworks with critical alerts quickly escalated to you



For more information, call
1800 737 817 to speak to
a Secureworks security
specialist.

secureworks.com.au