

Advanced Endpoint Threat Detection Powered by Red Cloak™

Reduces Time to Detect and Effort to Respond

Secureworks Advanced Endpoint Threat Detection (AETD) and AETD Elite, both with Red Cloak technology, provide the visibility you need to identify threats that slip past other security tools, even threats that use little or no malware.

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 attempt to infiltrate your organization.

Employing proprietary Counter Threat Unit™ (CTU™) research, Threat Intelligence and our Senior Intrusion Analyst (SIA) team, the Secureworks AETD and AETD Elite solutions give you the earliest possible warning that your endpoints may be hosting an advanced adversary. These solutions provide valuable visibility and correlation to quickly identify a potential endpoint compromise, while providing the detail you need to determine

the impact of the threat. We help you accelerate remediation efforts and make more efficient use of your security team by identifying which systems are compromised, how they were compromised and how you can repair them.

AETD Elite with Active Threat Hunting

AETD Elite includes all the benefits of our AETD solution, plus Active Threat Hunting to help you proactively delve even deeper into suspicious activity. Active Threat Hunting focuses on uncovering advanced threat actors through an ongoing hunting process, in collaboration with your security team. This customized program delivers more effective and accurate results.

With AETD Elite our threat hunting team works closely with you to gain an intimate understanding of your business, critical assets and infrastructure. Armed with an

Client Benefits

- Speed time to protection and reduce TCO with a fully managed and hosted solution
- Gain heightened visibility across your endpoints
- Detect threats that may be invisible to other security tools
- Accelerate response with critical event escalation including guidance on how to evict threat actors
- Reduce costly system reimaging by identifying vulnerabilities to patch
- Minimize data loss and other damage by identifying affected systems quickly
- Increase confidence in system integrity and data confidentiality
- Increase the skills of your security team with Active Threat Hunting

Understanding of what is and is not normal for your organization, our threat hunters can often identify threat actor activity that may be too subtle for technology alone to identify. With this solution we hunt continuously and provide up to weekly reports and calls outlining hunting activities and findings. We can do all the hunting and only involve you via regular reports and calls, but we encourage your team to boost their skills and knowledge by hunting with us.

Though threat hunting is an important part of any security program, many organizations find it difficult to prioritize either because they don't have the skills in-house or simply due to a lack of time. If you implement threat hunting rarely or only when there's a specific incident, your security program is not as effective as it can be. Making threat hunting a regular part of your security program helps identify and evict threat actors sooner, which reduces damage and remediation costs.

Proven Intelligence and Heightened Visibility

Our AETD and AETD Elite solutions utilize proprietary systems and Threat Intelligence developed by our CTU Research Team. This combination of supervised machine learning and human intelligence has proven to be effective in detecting advanced threats in Secureworks Targeted Threat

Hunting engagements across hundreds of thousands of endpoints. With AETD Elite you also get Active Threat Hunting to identify and evict even advanced threat actors who often hide inside organizations doing damage for months or years.

Secureworks sensor telemetry combined with our Threat Intelligence allows our experienced analysts to pinpoint when a breach occurred, who may be behind the attack, which endpoints are impacted, where the threat actor and malware may have spread, what else to look for across your organization and what next steps are appropriate for remediation. 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 and reports 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 analysts further enrich alerts and help you see activity from the initial breach of an endpoint by a threat actor to the lateral movement across your organization. We help 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 AETD and AETD Elite allow you to see more, know more and defend faster.

Solution Features

- Secureworks sensors gather security specific telemetry, even when endpoints are disconnected or outside the corporate network
- Secureworks sensors continuously monitor the registry, file system, process tables, memory and other areas for potential compromise
- A combination of supervised machine learning and human intelligence is applied to endpoint telemetry to identify more threats
- Alerts are investigated by our analysts with critical alerts quickly escalated to you
- With AETD Elite, our threat hunters further investigate suspicious activity via Active Threat Hunting, including regular reports and calls

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