Secureworks

DATA SHEET

Advanced Endpoint Threat Detection and AETD Elite

Reduces Time to Detect and Effort to Respond with CrowdStrike Technology

Secureworks Advanced Endpoint Threat Detection (AETD) and AETD Elite, both with CrowdStrike 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 infiltrate your organization with little or no malware.

Employing strong technology, the Secureworks Counter Threat Unit™ (CTU™) Research Team and Threat Intelligence, the Secureworks AETD and AETD Elite solutions give 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.

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 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

Customer 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
- Increase the skills of your security team with Active Threat Hunting

to detect. 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.

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 workflow
- Gain full-spectrum visibility across all endpoints in real time
- Five-second search to discover and investigate current and historic endpoint activity

Proven Intelligence and Heightened Visibility

AETD and AETD Elite leverage strong EDR technology and Threat Intelligence developed by the Secureworks CTU Research Team. This combination of supervised machine learning and human intelligence has proven effective in detecting advanced threats across hundreds of thousands of endpoints.

Agents 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 and AETD Elite allows you to see more, know more and defend faster.

Solution Features

- Lightweight agents gather security specific telemetry, even when endpoints are disconnected or outside the corporate network
- Agents 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
- 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 customers, 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 customers 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