DATA SHEET

AETD Red Cloak™

Reduce Time to Detect, Reduce Effort to Respond

The industry's definition of defeat is different from the adversary's definition of winning. Network defenders do not lose when they have been breached. The battle is just beginning. If you know what to look for, there are plenty of opportunities to catch the adversary.

Reduce Time to Detect

The best way to deal with advanced threat actors "living off the land" on your endpoints is not simply endpoint security software, host intrusion detection or any other device protection on the market, but rather a 24x7 managed security service that can:

- Monitor endpoints for signs of threat actor activity
- Scan for specific threat indicators as conditions change
- Keep threat intelligence data up to date
- Apply deep-level detection and behavioral analysis to find threat actors who do not use malware
- Alert clients with specific recommendations on how to proceed should an endpoint compromise be indicated

SecureWorks Advanced Endpoint Threat Detection (AETD) service with Red Cloak will improve your security situational awareness by continuously monitoring your endpoints and warning you when endpoints may have been compromised. Red Cloak delivers Counter Threat Unit™ (CTU) threat intelligence directly to the endpoint, providing valuable visibility and correlation with network level controls to determine the potential impact of a threat and reduce the time and effort to respond.

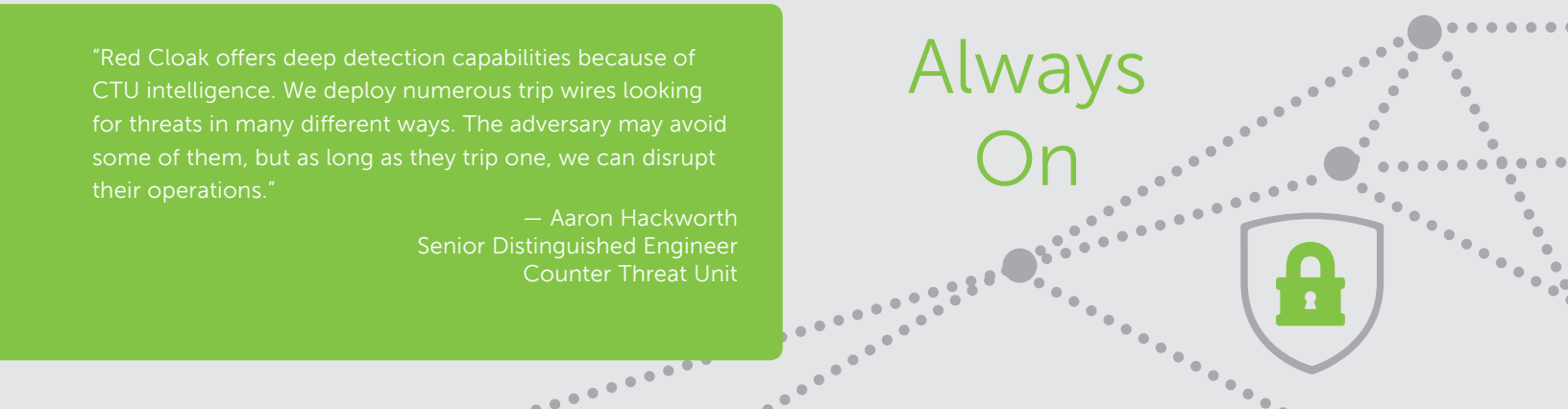
What Is Red Cloak?

Red Cloak is a SecureWorks-developed endpoint technology that was originally invented by our CTU team to support our Targeted Threat Hunting and Targeted Threat Response services.

AETD Red Cloak is an always-on endpoint monitoring service that continuously monitors your endpoints for signs of adversary activity, and maintains a record of key forensic activity necessary to make response activities as efficient as possible.

"Red Cloak offers deep detection capabilities because of CTU intelligence. We deploy numerous trip wires looking for threats in many different ways. The adversary may avoid some of them, but as long as they trip one, we can disrupt their operations."

— Aaron Hackworth
Senior Distinguished Engineer
Counter Threat Unit



Reduce Effort to Respond

Red Cloak sensors record all pertinent activity taking place on endpoint devices. This allows our security analysts to effectively go back in time to pinpoint exactly when a breach occurred, its cause and where the threat actor may have spread to. This precision means that any response efforts are targeted and less costly as 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.

Service Features

- Always-on endpoint monitoring
- Uses proprietary CTU Endpoint Intelligence technology
- Senior Intrusion Analysts (Level 2)
- Real-time and historical visibility into your endpoints
- Specific data around attack vector
- Deep-level forensics
- Fully managed (and hosted)
- Comprehensive view of activity and analytics in the Red Cloak Portal

Client Benefits

- Provides the earliest possible warning that your endpoints have been compromised
- Detects more types of threats by leveraging CTU intelligence to detect advanced malware and adversary behavior
- Reduces incident response costs by pinpointing exactly which endpoints are compromised
- Provides actionable guidance to remediate, which helps you eradicate the threat earlier in the kill chain to prevent or minimize data loss
- Makes existing investments more effective by helping to determine if alerts from your IDS/IPS/Firewall is a real threat
- Hosted solution that works with a mobile workforce and reduces client total cost of ownership (TCO)
- Integration with SecureWorks Incident Response Services

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