

DATA SHEET

Red Cloak™ Threat Detection & Response

A Threat Intelligence-based Security Analytics Application with Built in Security Content for You to Detect, Investigate and Respond to Advanced Threats Across Your Environment

With Red Cloak™ Threat Detection and Response you can take security into your own hands and transform the way your security analysts detect, investigate, and respond to threats across your endpoints, network and cloud. The application enables you to detect advanced threats, trust your alerts, streamline and collaborate on investigations and automate the right action. Built by security experts with unmatched knowledge of the threat, you'll see value fast with integrated use cases powered by Secureworks continuously updated threat intelligence and advanced analytics.

Wasted Resources

Security environments are now frustratingly fragmented. Data travels in all directions, in unfathomable quantities, and at lightning speed. Even the most modern security stacks are a varied mix of vendors and tools. Most tools are built by software companies rather than security experts with real world experience. Many technologies lack the functionality to collect the right telemetry to provide the visibility you need to detect unknown threats. As such, most SIEM detection use cases miss advanced threats and cause an influx of false positives resulting in wasted resources in responding to them. You're left struggling to build, apply and constantly update customized security content to your environment. In addition, your security talent must also function

as platform administrators managing complex technologies. All the while, threat actors are continuing to evolve their tactics, taking cover in the noise to act with stealth.

Most security teams are now drowning in noise, missing the threats that matter, and burdened with tedious investigations that prevent a fast response. Red Cloak TDR was built to solve these challenges. We've combined 20 years of industry-leading security operations expertise, threat research, incident response experience and proprietary advanced analytics algorithms into a software application that makes security as fast and dynamic as the threat.

Customer Benefits

- See fast time to value with built-in use cases that use proprietary threat intelligence and machine learning algorithms
- Detect unknown and emerging threats that go unnoticed by most SIEMs and EDR tools
- Stop chasing false positives and focus your limited resources on defending against real threats
- Justify the criticality of an alert with automated enrichment from Secureworks Threat Intelligence, entity context, and other 3rd party data
- Quickly understand what happened from a clear timeline of events
- Retroactively identify suspicious activity in your environment as new IOCs emerge
- Collaborate easily to speed up investigations and share knowledge between teams
- Use built-in chat to get advice from our security experts if you get stuck during an investigation
- Speed up response and minimize damage with software-driven responses for common containment use cases
- Benefit from endpoint-based pricing that lets you send us your security-relevant data without fear of hidden charges



Red Cloak™ Threat Detection & Response Architecture

How Red Cloak Threat Detection & Response Can Help

Red Cloak TDR is a cloud-native, SaaS application that is easy to setup and maintain. From day one, you will benefit from use cases built around Secureworks' Threat Intelligence, as well as state-of-the-art data science methodologies that automatically analyze security telemetry to alert you to unknown and known threats. Secureworks' machine learning algorithms drastically reduce false positives and enable you to trust your alerts. We also apply unsupervised deep learning on security event attributes and recurrent neural networks to model and identify even the most subtle and covert adversarial behavior.

We designed intuitive workflows that draw from our two decades' experience in security operations to make collaboration on investigations quick and decisive. Integrated software-driven response allows you to respond and contain the threat more quickly. A built-in chat feature gives you access to our team of experts when you want a second opinion before taking action. And because our goal is to give you enough business and security context to make sense of an investigation and take the right action, we will not charge by the amount of security relevant data you store, so you can budget and scale easily as business grows.

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
redcloak@secureworks.com