Red Cloak™ Threat Detection & Response

A Cloud Native security analytics application with built-in security content for you to Detect, Investigate, and Respond to advanced threats across your endpoints, network, and cloud environments.

Security software used to mean missed threats, useless alerts, and tedious investigations that burdened your staff. Not anymore.

How Red Cloak Threat Detection & Response Can Help

Red Cloak Threat Detection and Response, (TDR), is a cloud-native, SaaS application that is easy to set up and maintain. From day one, you will benefit from 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 across your endpoints, network, and cloud environments.

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.

Customer Benefits

- See fast time to value with built-in use cases that leverage proprietary threat intelligence and machine learning algorithms.

- Stop chasing false positives and focus your limited resources on defending against real threats.

- Detect unknown and emerging threats that go unnoticed by most SIEMs and EDR tools. Quickly understand what happened quickly correlating events across your security controls.

- Justify the criticality of an alert with automated enrichment from Secureworks Threat Intelligence, entity context, and other 3rd party data.

- Use ask an expert chat to get advice from Secureworks security experts if you get stuck during an investigation.

Key Features

Integrated Threat Intelligence

Give advanced threats nowhere to hide with knowledge from the Secureworks Counter Threat Unit™ research team.

AI-Based Detections

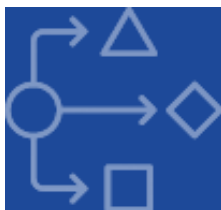Advanced analytics reduces meaningless alerts and detects threats your current tools miss.

Secureworks Network Effect

Benefit from insights taken from over 4,200 diverse customer environments.

MITRE ATT&CK™ Mapping

See attacker activity with security alerts mapped to the MITRE ATT&CK™ framework.

Intuitive Investigation Workflows

Get to conclusion quicker with collaborative investigation workflows designed by seasoned security pros.

Contact your dedicated Dell Endpoint Security Specialist today at, endpointsecurity@dell.com, about the SafeGuard and Response products that can help improve your security posture.

Learn more at Dellemc.com/endpointsecurity

Secureworks®