Windstream Enterprise MDR, powered by Cato

An extra pair of eyes to watch over your network

Despite investment in firewalls and other prevention capabilities, attackers continue to penetrate enterprise networks. Dwell time—the time from compromise to detection—exceeds 200 days. Reducing this period, while identifying threats quickly, is critical for keeping enterprises protected. Yet, installing more and more security and data analysis tools to achieve this, is no longer manageable, affordable, or sufficiently reliable.

Introducing MDR

Managed Detection and Response (MDR) is an advanced security service that offers continuous threat detection and guidance on how to respond to malicious events, quickly and effectively. MDR leverages AI and ML, combined with human threat verification, to hunt, investigate, alert, reduce risk of breach, and improve security posture.

MDR is built-in to Cato's SASE platform. This means MDR monitors all sites, VPN and cloud environments connected to Cato SASE Cloud, enabling users to benefit instantly from the service without having to install additional hardware and software. Customers can offload the process of detecting compromised endpoints to Cato's SOC team. The team has unmatched expertise in SecOps, handling thousands of incident engagements per year.

Key benefits

MDR helps enterprises break the endless cycle of increasing threats and adversaries. Cato SOC detects infected endpoints and notifies the Windstream Enterprise Cyber Security Operations Center (CSOC) which provides customers with guidance for threat remediation.

- **Immediate service activation, no additional hardware and software needed**
- **Dwell time reduced from 200+ days to 1-2 days!**
- **Real-time alerts for confirmed threats, no false positives**
- **Network-level containment and guided remediation for effective response**
- **Designated security expert alongside security assessments**

Key capabilities

MDR automatically collects, indexes, and stores the metadata from all sites, VPN and cloud environment in its big data repository.

Zero-footprint data collection

Cato can access all relevant information for threat analysis since it already serves as the customer's (SASE) network platform. This eliminates the need for further installations, and once customers subscribe to MDR they instantly benefit from the service.

Automated threat hunting

Cato leverages AI and ML to mine the network for suspicious flows based on the many attributes available to Cato. These include accurate client application identification, geolocation, risk assessment of the destination based on IP, threat intelligence, URL category, frequency of access, and more.

Human verification

Cato's SOC team inspects suspicious flows on a daily basis and closes an investigation for benign traffic.

Network-level threat containment

The Windstream Enterprise CSOC alerts customers in case of verified active threats, applying network-level threat containment by blocking the network traffic.

Guided remediation

The Windstream Enterprise CSOC provides the context of threats and recommended actions for remediation. The team is available for additional assistance on specific incidents.

Reporting and tracking

Customized reports are generated, summarizing security posture, all detected threats, descriptions, risk levels, impacted endpoints, and more.

Assessment check-ups

The Windstream Enterprise CSOC offers a designated security expert alongside assessment reviews to ensure customers maintain a strong security posture.

How does it work?

Customers simply obtain an MDR license, and the Windstream Enterprise CSOC takes it from there:

- Monitors network on a daily basis
- Verifies real threats and sends alerts
- Helps customers with remediation
- Detects anomalies
- Contains threats to customer's network
- Sends detailed investigation reports each month

About Cato Networks

Cato provides the world's leading single-vendor SASE platform, converging Cato SD-WAN and a cloud-native security service edge, Cato SSE 360, into a global cloud service. Cato SASE Cloud optimizes and secures application access for all users and locations everywhere. Windstream Enterprise SASE, powered by Cato, customers easily replace costly and rigid legacy MPLS with modern network architecture based on SD-WAN, secure and optimize a hybrid workforce working from anywhere, and enable seamless cloud migration. Cato enforces granular access policies, protects users against threats, and prevents sensitive data loss, all easily managed from a single pane of glass. With Cato your business is ready for whatever's next.

SASE Cloud with SSE