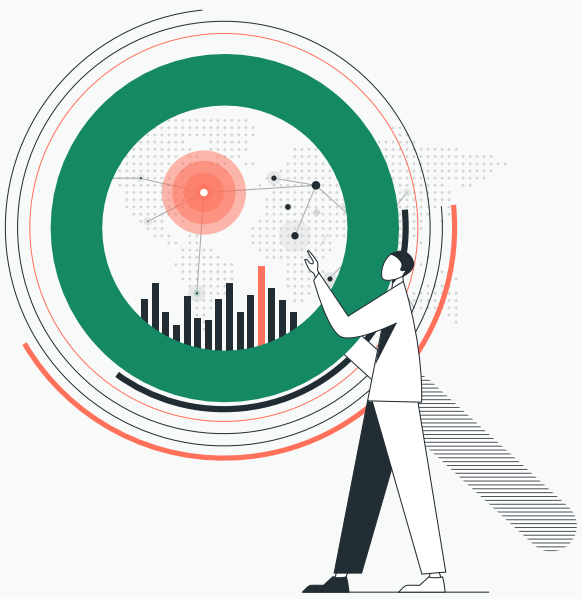
Cato MDR

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 Cato MDR

Cato 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. Cato MDR leverages AI and ML, combined with human threat verification, to hunt, investigate, alert, reduce risk of breach, and improve security posture.

Cato MDR is built-in to Cato's SASE platform. This means Cato 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 HW/SW. 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

Cato MDR helps enterprises break the endless cycle of increasing threats and adversaries by detecting infected endpoints, sending alerting, and providing guidance for remediation.

- **Immediate service activation, no additional HW/SW 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

Cato MDR automatically collects, indexes, and stores the metadata from all sites, VPN and cloud environments 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 Cato 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

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

Guided Remediation

Cato provides the context of threats and recommended actions for remediation. Cato's SOC team is available for further assistance on required incidents.

Reporting and Tracking

Cato generates monthly custom reports, summarizing security posture, all detected threats, descriptions, risk levels, impacted endpoints, and more.

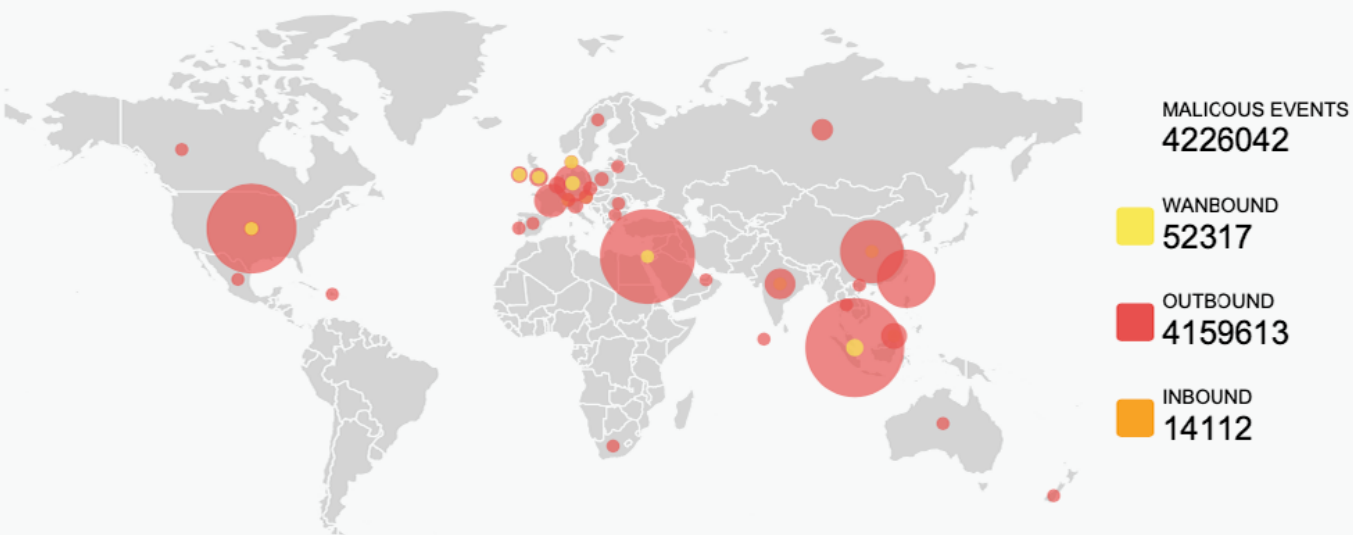
Assessment Check-Ups

Cato offers a designated security expert alongside assessment reviews for ensuring customers maintain a strong security posture.

How Does it Work?

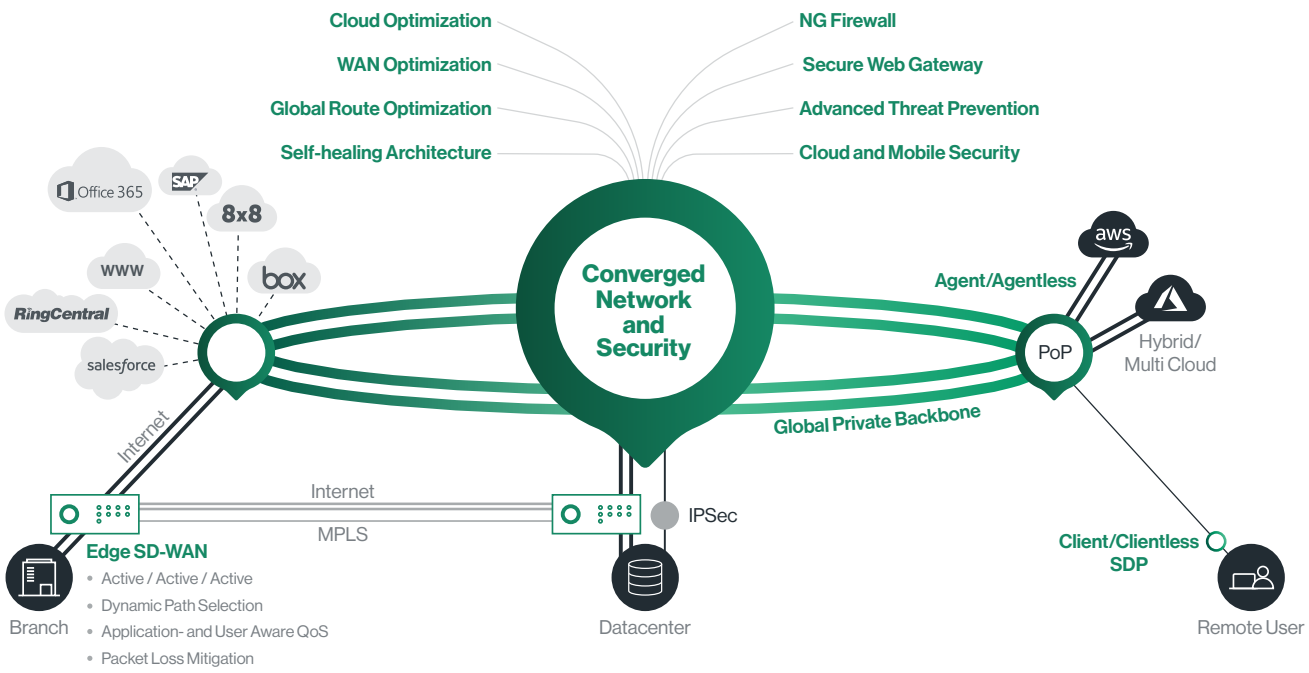
As with all other Cato services, customers simply obtain a Cato MDR license, and Cato's SOC team takes it from there:

- 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 is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations. Using Cato, customers easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into the network with a zero trust architecture.



Cato. The Network for Whatever's Next.

Cato Cloud

Global Private Backbone

Edge SD-WAN

Security as a Service

Cloud Acceleration and Control

Mobile Security and Optimization

Work from Home

Cato Management Application

Managed Services

Managed Threat Detection and Response (MDR)

Intelligent Last-Mile Management

Hands-Free Management

Site Deployment

ISO 27001 Certified

SOC2 Approved

GDPR Compliant