CATO
NETWORKS

Cato XDR

A SASE-based Approach to Threat Detection and Response

The Drive to Accelerate Detection and Response with XDR

Imagine you're an overworked security analyst responsible for the security posture of your organization. One morning, you examine your logs and realize there have been abnormal traffic patterns over recent weekends. Your NGFW logs show an unusually high number of SMB flows, but few have been blocked and alerted. Your IPS also shows excessive SMB flows but even fewer have been blocked and alerted. Your SIEM shows no relationship between the NGFW and IPS alerts, so it gives them a low-priority risk score. Since the priority is low, you ignore them and move on to more important tasks. However, these traffic flows had indications of a stealthy malware attack and were communicating with malicious domains. This delay in identifying and investigating these threats has further compromised your organization.

This situation occurs more often than one might think as IT teams face an increasingly fragmented technology stack. Most organizations use prevention tools to identify and block threats in real-time, but not all threats can be detected in real-time. This leaves security analysts in the dark and unaware of threats looming in their environment. This lack of insight into multiple layers of threat data makes it nearly impossible to identify potential threats, especially those that evade or bypass perimeter defenses. This gap in their security leaves their organizations at greater risk.

Extended Detection and Response (XDR) Can Help

Extended Detection and Response (XDR) is an advanced security tool that helps address the challenges that with so many alerts, analysts can't see what's important, and that real-time protection engines can't prevent all threats on their own. XDR provides consolidated visibility across multiple security platforms to bring a holistic view of the security posture. It creates a simple starting point for security operations, highlighting the high priority issues that analysts should deal with first. It also enables a deep analysis of multiple data sources to help find threats that real-time security engines may have missed, and to minimize false positives. This results in a faster, more effective response to security threats. Its improved detection and prevention mechanisms include machine learning and behavioral analytics, Contextual Analysis, Threat Hunting, SOAR integration, and more.

XDR extends beyond endpoints alone to expose complex threats across the entire security landscape. It is an extremely effective tool for security organizations that are suffering from a skills shortage and insufficient resources. The contextual information about attacks allows security analysts to understand and quickly contain the threats.

XDR provides numerous advantages over traditional security tools, and can make security teams both more effective and more efficient. However, it does have limitations. In particular, XDR has a data quality issue, and this can render standard XDR solutions less effective against the most complex and nuanced threats.

Data Quality Challenge for XDR

XDR collects threat data from multiple sources, such as logs, alerts, threat intelligence, and other information that helps map the threat environment. It extracts details such as IP addresses, file hashes, timestamps, and other Indicators of Compromise (IoCs). Correlating this information helps to identify patterns and relationships across multiple sets of data.

However, for XDR to process threat data, it first needs to normalize the data into a consistent structure that it can understand and relate to all the other data. Normalization often results in reducing the usable information in the data, effectively reducing the quality of the data.

This negative impact on the quality of imported data is a major challenge faced by standard XDR solutions. It makes threats harder to detect and increases the time to investigate and respond, placing the network and its users at greater risk.

Data quality is directly related to the type of sensors available to the XDR solution, which we can categorize as follows:

Native Data

Data that is original and built into the XDR.

It results in high-quality data that requires no integration or normalization and suffers no reduction in information content.

Portfolio Data

Data that is part of a vendor's portfolio but not necessarily native to the portfolio or the XDR.

Some integration and normalization is required. Often, only limited quality decrease is encountered because there is direct engineering-to-engineering access between the data sources.

Third-party Data

Data that is external to the vendor's portfolio and XDR.

This requires high normalization effort, which can result in a significant quality decrease since the sensors often speak a completely different language.

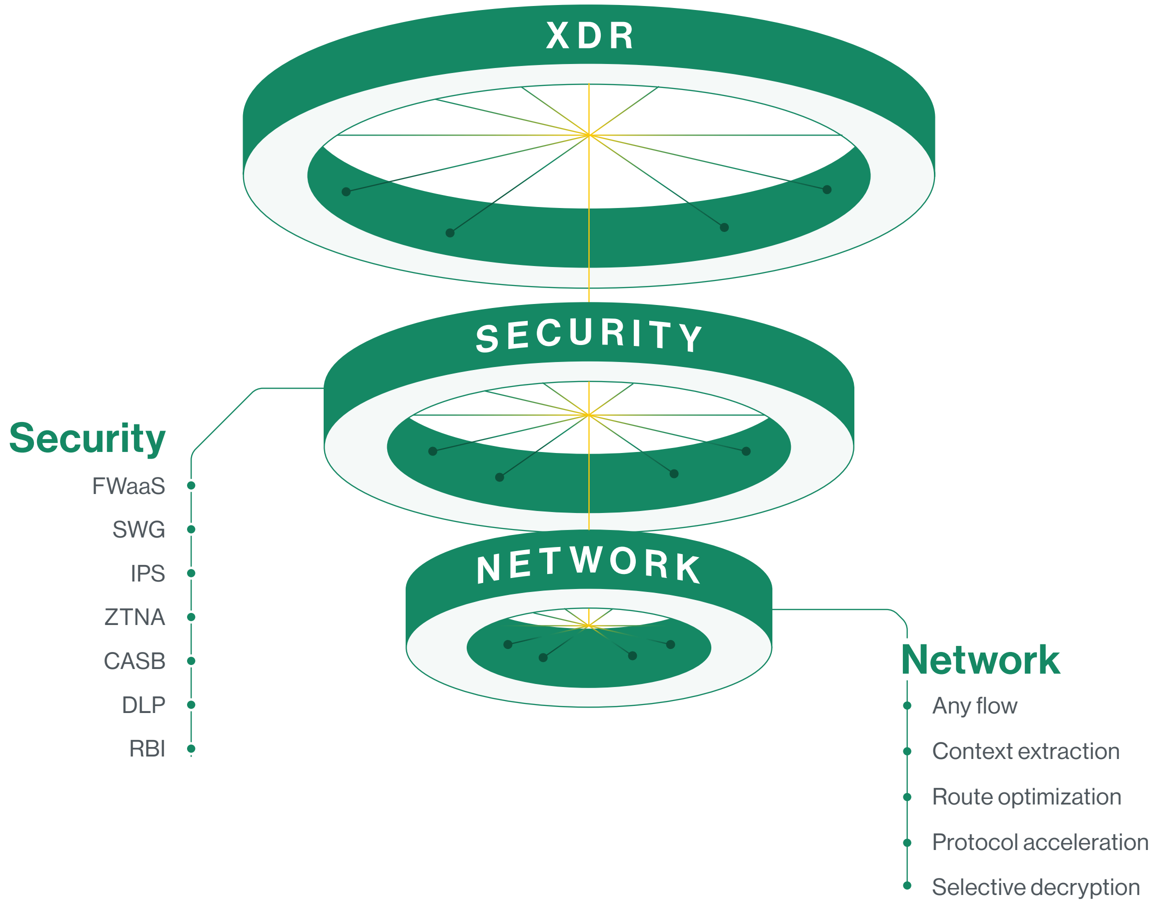
Standard XDR solutions typically consume very limited Native Data; perhaps only one sensor. They will then consume varying amounts of Portfolio and Third-Party data. This creates real data quality challenges concerning the completeness of data used for threat investigations. This, in turn, impacts the detection, identification and remediation of security incidents.

SASE-based XDR: The Game-Changer

In contrast, a SASE-based XDR takes a completely different approach that presents a cleaner, more accurate path to efficient security operations. Since a SASE solution comprises both network and security functions in a single platform, a SASE-based XDR consumes almost entirely Native Data.

A SASE-based XDR overcomes the data collection limitations of standard XDR solutions.

Let's explore this in more detail.



Broader, richer data

Data quality is directly linked to the nature of the available XDR sensors, and this is where a SASE-based XDR shines. The key to this is the native security sensors that are built into the SASE platform and capture data from every inspection engine.

Contact Us

Enhanced AI and Machine Learning

Artificial Intelligence and Machine Learning (ML) techniques are the driving forces behind almost everything accomplished in a modern XDR. Security researchers and data analysts develop ML models that train on petabytes of data and trillions of events from a single data lake. ML algorithms are used to increase the accuracy of attack identification and priority scoring. Advanced ML techniques enhance threat prediction to help identify unknown and stealthy threats that have evaded real-time prevention tools.

These techniques are intensely data driven. We can illustrate this by considering automated threat-hunting capabilities, which complement prevention engines to surface stealthy threats. Threat Hunting leverages Machine Learning to patrol the data lake for suspicious flows based on numerous attributes contained within the data. It correlates between related network flows, geographic data, events, and raw metadata. Additional data is gathered such as threat intelligence, destination popularity, 3rd party feeds, and non-human traffic patterns.

Since these techniques are so underpinned by data, their effectiveness is reduced when standard XDR solutions suffer from limited and poor-quality data. Conversely, the high proportion of native data in a SASE-based XDR enables enhanced ML techniques with more effective detection.

Reduced false positives

A huge challenge facing modern security teams is to identify and stop threats with minimal disruption to the business. A key goal is to minimize false positives, in which security tools identify a problem where none exists, and then interrupt the business when they take action. Security teams rely on Threat intelligence feeds to identify threats. However, even when using industry best practices, analysts can suffer from a significant number of false positives when using them.

A SASE-based XDR contains a very broad range of high-quality data that spans both network and security. This can be used to great effect to reduce false positives.
A good SASE-based XDR can run a reputation assessment filter to all but eliminate false positives. For example, it could use AI/ML to correlate its broad networking and security information with millions of IoCs from hundreds of threat intelligence sources (we use over 250, for example). It could then score them to identify and eliminate false positives using real-time network intelligence gathered by the ML models.

Thus, a SASE-based XDR can minimize disruption to the business, while focusing the security team onto just those threats that are real.

Reduced time to investigate

A primary goal for XDR is to help analysts to investigate quickly. However, threat investigation can be complex, and even more complex because XDR generates many types of incidents that analysts must be able to deal with. For example:

- **Threat Prevention engines** correlate Block event signals from the real-time prevention engines.
- **Threat Hunting engines use ML and heuristics** to detect attacks that have evaded the threat prevention engines.
- **Anomaly Detection engines** detect suspicious usage patterns over time.

To facilitate rapid investigations in the face of so much complexity, every incident needs to be presented simply. It needs a complete narrative from its inception until its final resolution and all the information that is required to investigate. Investigations should be presented as a roadmap to help security analysts understand each detected threat.

Since a SASE-based XDR contains a broad range of high-quality native network and security data, incidents can be presented with all the information required for an in-depth investigation. The information will be rich, accurate, easy to analyze, all in one place and can be presented in a guided order. In this way, a SASE-based XDR can reduce the time to investigate and thus increase analyst capacity.

Why SOC Teams Prefer SASE-based XDR

As enterprises cloudify more of their operations, security teams are under increased pressure to protect the organization from all attack vectors and rapidly detect, understand, and eliminate any threat. Modern SOC operations require an intelligent platform that filters out extraneous noise, accurately links relevant security data, views threats over time, and finds relevant trends to expose all threats. These trends create security incidents that require their immediate attention. Standard XDR was the beginning of strengthening their security posture. However, SASE-based XDR goes much further.Data quality is directly related to the type of sensors available to the XDR solution, which we can categorize as follows:

A SASE-based XDR, built into a SASE cloud architecture presents SOC analysts with a single tool to view their entire security architecture and all XDR incidents with relevant threat details. These details include incidents broken out by risk type and level, Indicator of Attack (IoA), MITRE techniques, and risk scores, to name a few.

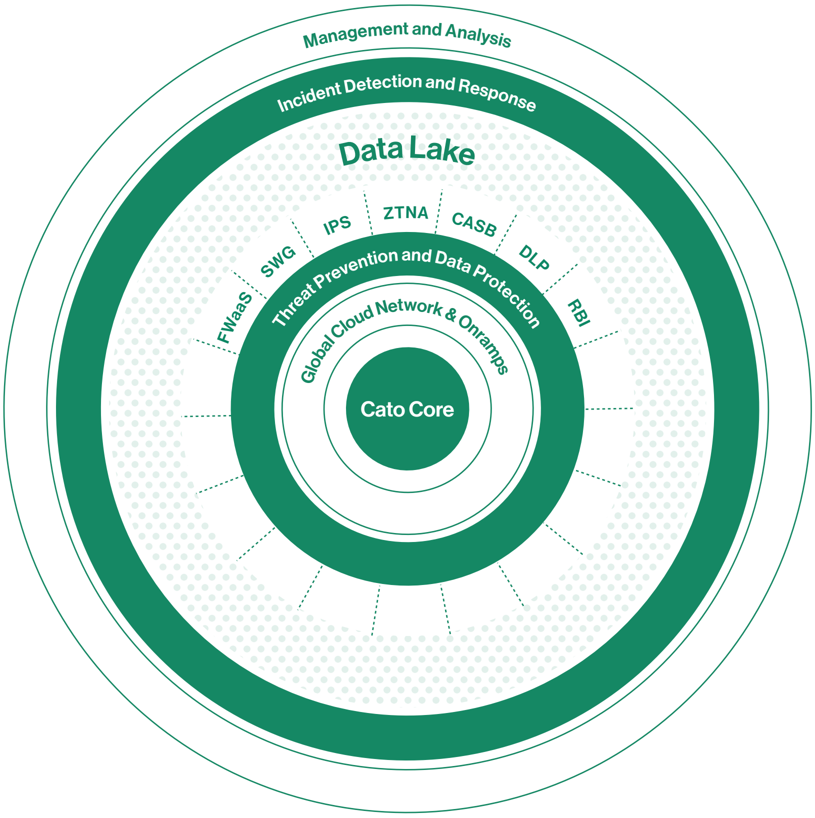
A SASE-based XDR provides SOC teams with extended insight into threat-hunting specifics and provides the necessary details to investigate and triage security events. This makes it easy to follow a threat back to its source to remediate the device at risk.

A SASE-based XDR can enhance security operations by combining all phases of security management into a single management tool. This reduces the overall effort of the SOC analyst, thus reducing their stress as well.

Cato XDR is the SASE-based XDR of the Future

A key strength of XDR is how it facilitates in-depth analysis of disconnected security alerts from multiple data sources. This allows it to deliver more coherent threat identification while filtering out most of the noise. XDR detects security threats across networks and endpoints by enhancing cross-network visibility. This leads to faster responses to security threats and an improved overall security posture. However, a gap in data quality makes standard XDR tools less effective.

This is where Cato XDR technology shines brightly over standard XDR approaches. Data quality is no longer an issue because Cato XDR benefits from multiple built-in native security sensors. The volume and breadth of these native sensors are dramatically greater, spanning all the single-pass inspection engines – NGFW, IPS, NGAM, SWG, CASB, DLP, ZTNA, RBI, EPP, and more. This allows Cato to populate high-quality metadata (that requires no normalization or reduction) into a massive data lake. Advanced AI/ML algorithms train on this metadata to identify malicious attack patterns and generate high-priority incidents more accurately based on scoring. The accuracy and efficiency of these advanced algorithms produce XDR stories, which provide a detailed roadmap for security teams to investigate and remove threats from their network.



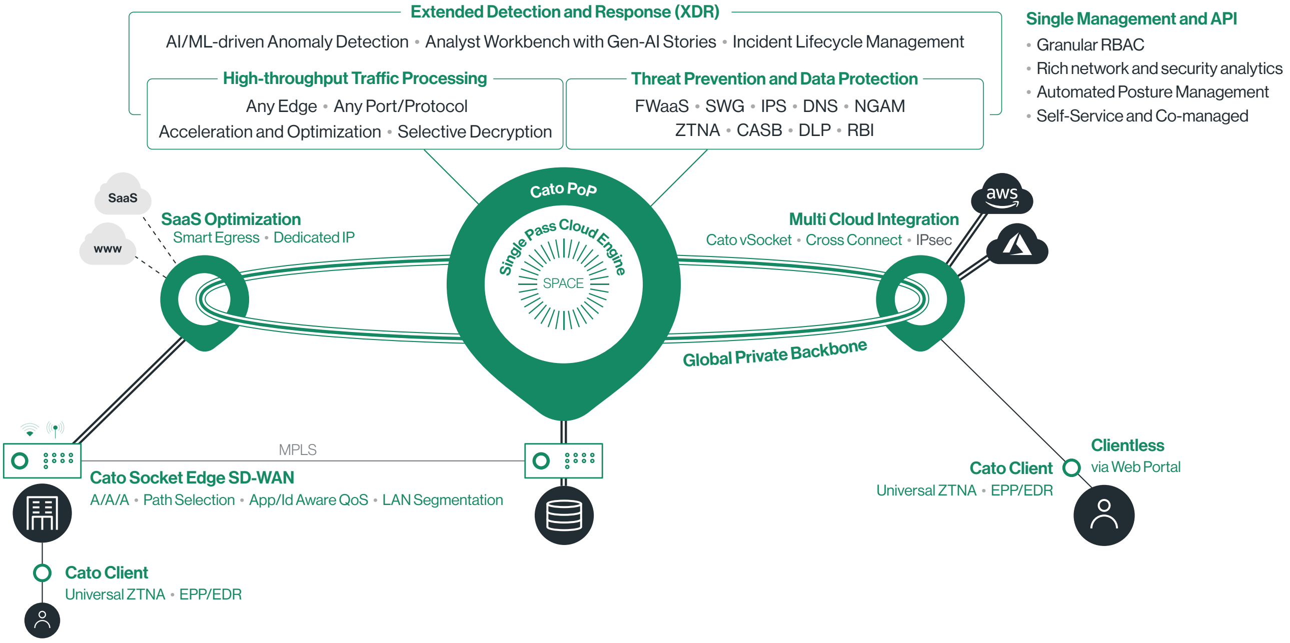
Management and Analysis
Incident Detection and Response
Data Lake
FWaaS
SWG
IPS
ZTNA
CASB
DLP
RBI
Threat Prevention and Data Protection
Global Cloud Network & Onramps
Cato Core

Cato XDR, based on the Cato SASE Cloud, presents a uniquely strong platform for security teams to address threats quickly and effectively, and strengthen their overall security posture.

About Cato Networks

Cato Networks is the leader in SASE, delivering enterprise security and network access in a single cloud platform. With Cato, organizations replace costly and rigid legacy infrastructure with an open and modular SASE architecture based on SD-WAN, a purpose-built global cloud network, and an embedded cloud-native security stack.

Cato SASE Cloud Platform



Extended Detection and Response (XDR)
AI/ML-driven Anomaly Detection • Analyst Workbench with Gen-AI Stories • Incident Lifecycle Management

High-throughput Traffic Processing
Any Edge • Any Port/Protocol
Acceleration and Optimization • Selective Decryption

Threat Prevention and Data Protection
FWaaS • SWG • IPS • DNS • NGAM
ZTNA • CASB • DLP • RBI

Single Management and API
- Granular RBAC
- Rich network and security analytics
- Automated Posture Management
- Self-Service and Co-managed

SaaS Optimization
Smart Egress • Dedicated IP

Multi Cloud Integration
Cato vSocket • Cross Connect • IPsec

Cato Socket Edge SD-WAN
A/A/A • Path Selection • App/Id Aware QoS • LAN Segmentation

Cato Client
Universal ZTNA • EPP/EDR

Clientless
via Web Portal

Cato. WE ARE SASE.

Cato SASE Cloud Platform

Connect
Cloud Network

Cloud On-Ramps

Protect
Network Security

Endpoint Security

Detect
Incident Life Cycle Management

Run
Unified Management and API

Use Cases

Network Transformation
MPLS to SD-WAN Migration

Global Access Optimization

Hybrid Cloud and Multi-Cloud Integration

Business Transformation
Vendor Consolidation

Spend Optimization

M&A and Geo Expansion

Security Transformation
Secure Hybrid Work

Secure Direct Internet Access

Secure Application and Data Access

Incident Detection and Response