EPP

Enhancing Cybersecurity with SASE-Managed Endpoint Protection Platforms

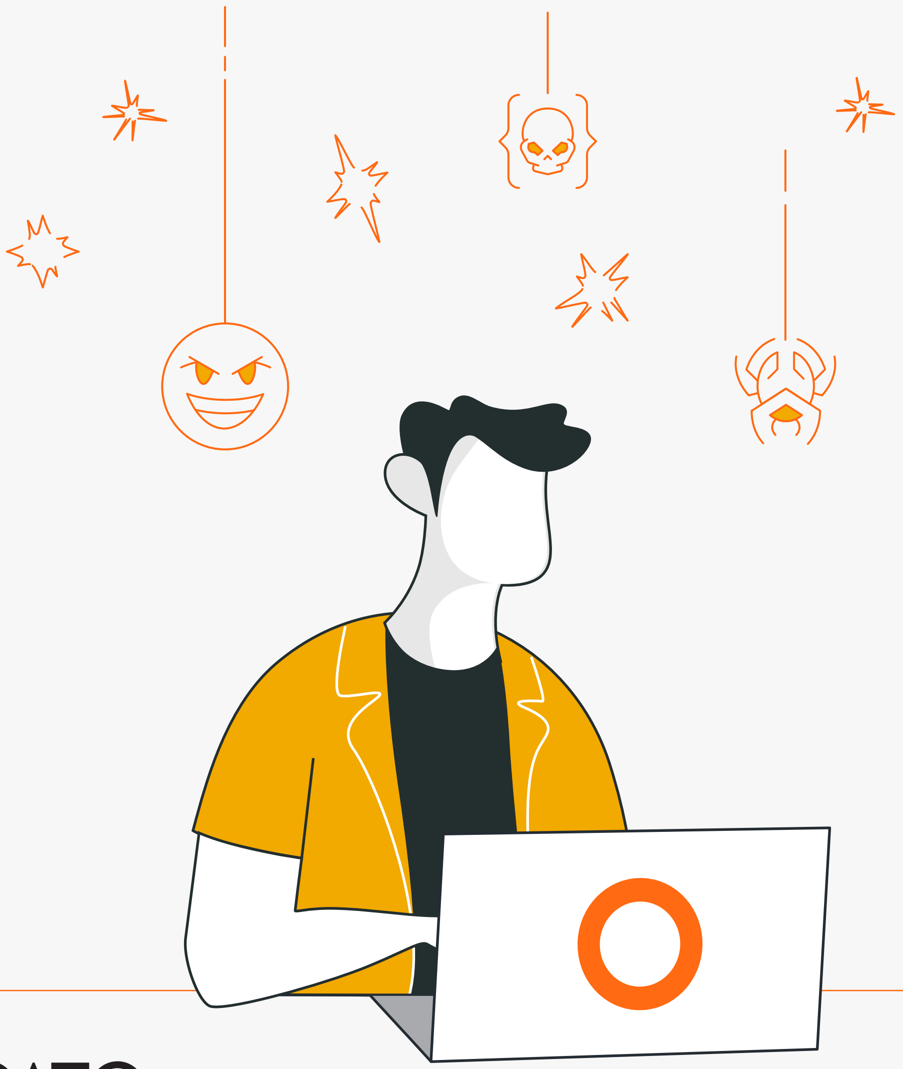
WINDSTREAM ENTERPRISE | CATO NETWORKS

First Line of Attack: Endpoints

As organizations increasingly rely on digital technologies to increase day-to-day productivity, the cyber threat landscape has become more complex and difficult to defend. Enterprises face various risks associated with endpoints, and each risk, while unique, poses a serious threat to an organization's security posture.

Endpoint risks include malware and ransomware, weak authentication and access controls, lack of visibility, unpatched software, and device misconfigurations, to name a few. Malware for example, is an existential threat, and endpoints are ground zero in this battle because they are the easiest attack vectors to exploit. However, any of these risks will expose vulnerabilities in enterprise-wide defenses and adversely impact their security posture.

Protecting corporate endpoints is a universal imperative and, given the dynamic nature of business and employees working from everywhere, is non-negotiable. To mitigate this, modern enterprises require a holistic approach to protecting their users and devices.



EPP on the Front Lines

An endpoint protection platform (EPP) is a cybersecurity solution designed to be the first line of defense against malware and ransomware attacks on endpoints. It detects malicious activities and provides advanced investigation and remediation tools to respond to security threats. Multiple detection techniques, ranging from Indicators of Compromise (IOCs) to heuristic analysis identify endpoint threats and take the appropriate defense measures to protect them.

EPP solutions address a variety of cybersecurity challenges, including

01

Malware and Ransomware Protection advanced threat detection mechanisms, including behavioral analysis and machine learning, help prevent various malware threats. These include fileless ransomware.

02

Zero-Day Exploits – heuristic analysis and anomaly detection identify and block zero-day exploits by recognizing abnormal patterns.

03

Device and Application Control comprehensive control and management are crucial for enhancing the overall security posture.

04

Securing Work-From-Anywhere (WFA) cloud-based management and adaptive security measures easily cater to remote working needs and ensure consistent protection.

05

Regulatory Compliance – security controls, auditing, and reporting help organizations achieve and maintain regulatory compliance.

While this is not an exhaustive list, it demonstrates EPP's importance for organizations that require a comprehensive and proactive defense strategy to protect their users and devices.

EPP is the first layer of defense against common attacks on the digital enterprise and provides the necessary tools to secure endpoints no matter where they reside.

A Look Inside EPP

EPP uses a variety of technologies to ensure continuous endpoint protection, preventing malicious files from being executed and stopping malicious activities at runtime. The pre-execution prevention engine scans hundreds of file types for threats, including archives. It identifies malicious files using advanced signature-based techniques and uses machine learning algorithms to identify polymorphic and zero-day malware based on file behavior.

For elusive threats that may evade pre-execution prevention, a runtime prevention engine employs heuristics and process behavioral analysis to detect malicious characteristics in processes in real-time. It can identify various threats, including fileless malware, Advanced Persistent Threats (APT), evasive exploits and zero-day attacks.

Both pre-execution and runtime automatically monitors and contains detected threats. Containment actions include threat blocking, file quarantine, or process termination.

SASE-Managed EPP:
The New Approach for Endpoint Protection

Typically, EPP management is separate from traditional network and security management, creating numerous challenges for security teams by increasing their level of effort. Managing configurations, updates, and reporting across multiple tools results in activity duplication, delays threat response, and reduces overall effectiveness. Traditional EPP management is also challenged with integration, limited visibility, and potential compliance issues.

A SASE-managed EPP solution is a new approach to managing EPP. It makes deploying, managing, and troubleshooting EPP straightforward and easy. SASE-managed EPP enables a more efficient and effective work when compared to EPPs that are not part of a unified SASE platform. It saves time because there is one less point solution to integrate, one less management application to learn, and when using external SIEM solutions – you have one less product to export and normalize data from.

Traditional EPP vs Cato EPP

	EPP	Cato EPP
Unified Platform	✗ No	✓ Yes
Integration	✗ High Effort	✓ Not Required
Deployment	✗ Complex	✓ Simple
Troubleshooting	✗ Complex	✓ Simple
Visibility	✗ Limited	✓ 360-degree
Compliance	✗ Potential Challenges	✓ Easy to Achieve
Management	✗ Multiple Management Tools	✓ Single Management App
Reporting	✗ Across Multiple Tools	✓ Single Management App
Updates	✗ Update Multiple Tools	✓ Update a Single Platform

SASE-managed EPP also saves time in ongoing security operations, as it requires one less management application to audit and one less product to maintain.

The single SASE management console displays all endpoint activities, making the remediation process logical and streamlined. Additionally, detecting relationships between network security and EPP events is simple, making it easier to identify and respond to related threats.

SASE-Managed EPP and SASE-Based XDR: Better Together

A SASE-managed EPP provides extended value and insights, serving as an additional native sensor to SASE-based XDR.

Together, they enable higher quality threat detections, easier threat investigation process and a broader set of response options. It also enables analysis of complex and hidden threats that span across both endpoint and network events.

For example, events from an infected endpoint that attempts lateral movement to communicate with other hosts in the network. This is an obvious threat for further investigation. SASE-managed EPP and SASE-based XDR strengthen enterprise security by eliminating security blind spots and making security management easier to accomplish. By removing point solution integration and multiple management tools, they reduce the level of effort and streamline security operations. This allows security teams to easily view and investigate threats, remediate them and maintain a strong security posture.

This is possible when SASE-managed EPP and SASE-based XDR work together.

Saves Time

One less

- Point solution to integrate
- Management application to learn
- Data source to normalize into SIEM
- Separate application to audit
- Product to maintain

Gives More Insights

- One more native sensor in Cato XDR
- Single view of all user events from both network and endpoint perspectives

Cato EPP is the Future of Endpoint Protection

Cato EPP is the industry's first SASE-managed EPP solution. It streamlines endpoint security and makes it easier to manage. Based on highly effective threat detection engines, Cato EPP has built-in protections that provide detailed endpoint threat analysis and response capabilities. Its protection engines combine pre-execution scanning for known threats, and runtime prevention to detect anomalous characteristics.

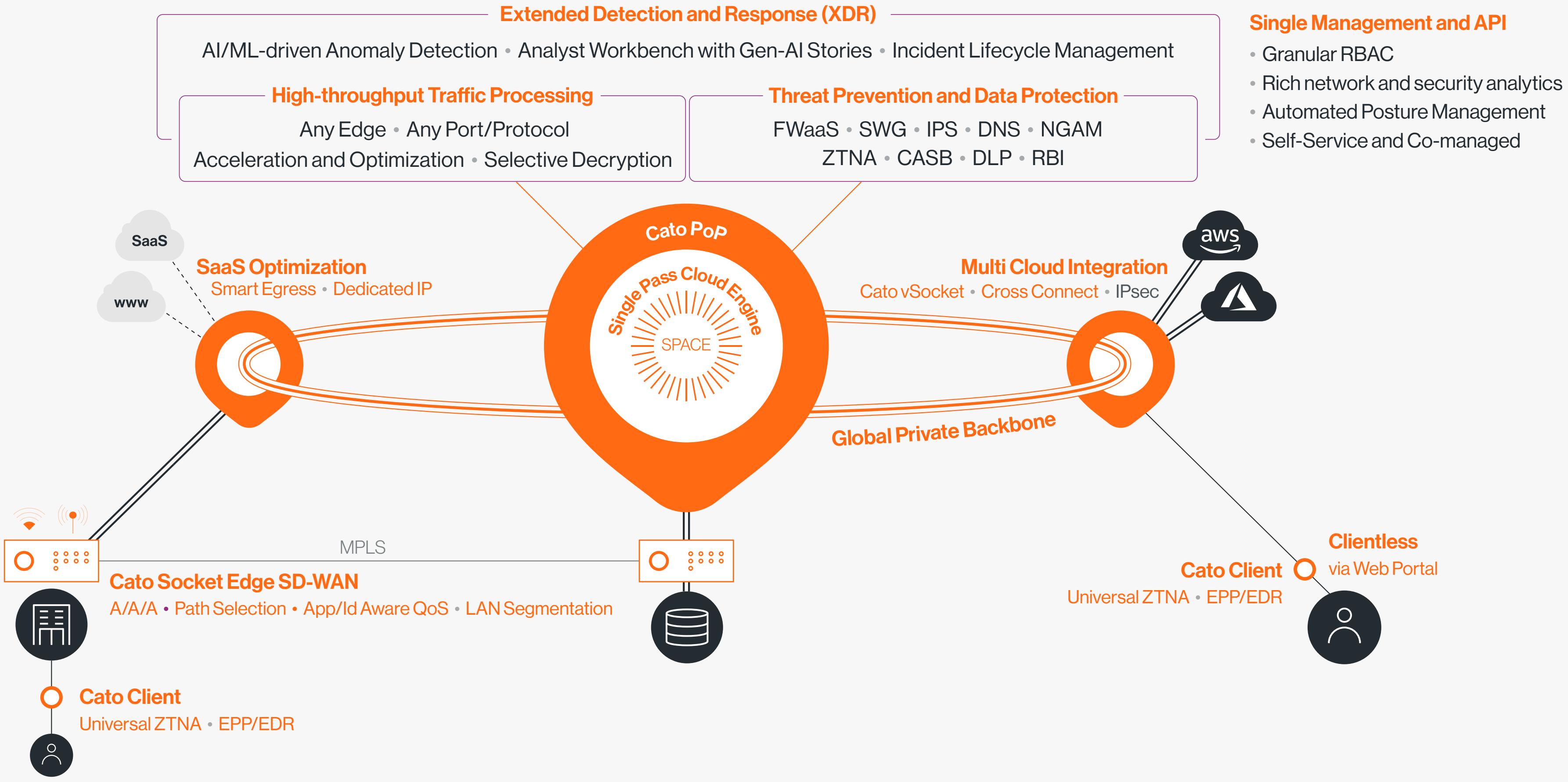
Cato EPP provides the best of everything required to secure modern enterprise endpoints. And when combined with Cato XDR – the industry's first SASE-based XDR platform – it enables instant detection and analysis of complex, hidden and related threats that span across both endpoint and network events.

Together, they deliver dynamic and adaptive protection by delivering greater insight and visibility to capture early indicators of threats and the tools to mitigate them. Being SASE-managed and integral to the Cato SASE Cloud platform, Cato EPP delivers a better security experience and overcomes many of the security management issues that adversely impacts security teams. However, these teams are now better equipped to eliminate endpoint risk with Cato EPP, a holistic EPP solution.

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.

Windstream SASE Cloud Platform powered by Cato


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
www
SaaS Optimization
Smart Egress • Dedicated IP
Cato PoP
Single Pass Cloud Engine
SPACE
Multi Cloud Integration
Cato vSocket • Cross Connect • IPsec
aws
Global Private Backbone
MPLS
Cato Socket Edge SD-WAN
A/A/A • Path Selection • App/Id Aware QoS • LAN Segmentation
Cato Client
Universal ZTNA • EPP/EDR
Cato Client
Universal ZTNA • EPP/EDR
Clientless
via Web Portal

About Windstream

Windstream Enterprise drives business transformation through the convergence of our proprietary software solutions and cloud-optimized network to unlock our clients' revenue and profitability potential. Our end-to-end IT managed services modernize technology infrastructure, optimize operations, eliminate resource constraints and elevate the experience of our clients and their end users, while securing their critical data and brand reputation. Analysts recognize Windstream Enterprise as a market leader for our product innovation, and clients rely on our best-in-class management portal. Businesses trust Windstream Enterprise as their single-source for a high-performance network and award-winning suite of connectivity, collaboration and security solutions—delivered by a team of technology experts whose success is directly tied to our clients' complete satisfaction.