CATO
NETWORKS

Which SSE Can Replace All of Your Physical Firewalls?

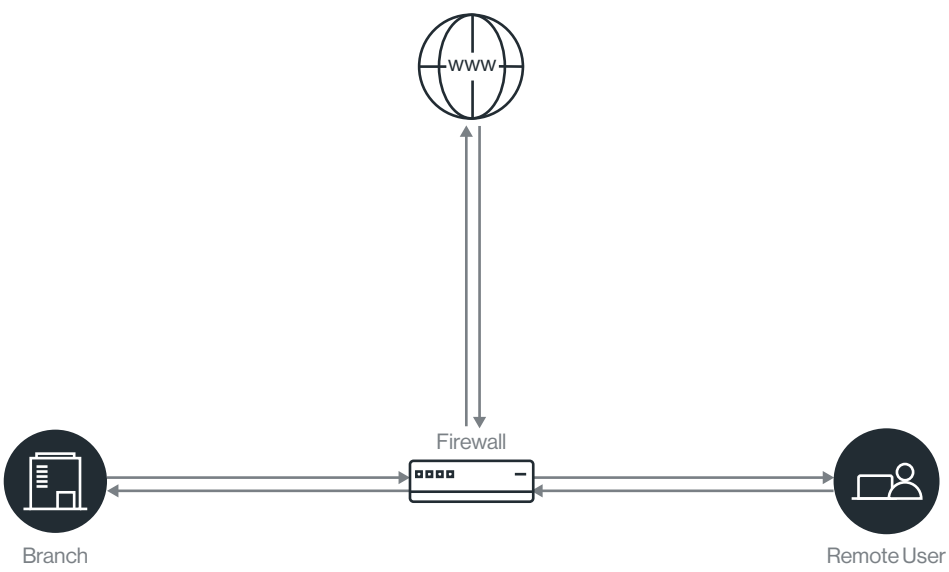
The Datacenter Firewall Migration Challenges

When it comes to moving security to the cloud, enterprises often start at the branch. That's because branch firewalls are typically only focused on securing Internet access, and mosty Security Service Edges (SSEs) can easily meet that requirement.

But when we turn to the datacenter FW, things get a lot more complicated. Why? Because datacenter FWs address so much more than just secure Internet access. They are also used to manage WAN traffic, maintain strict datacenter LAN segmentation, and to assure reliability and high availability to network traffic.

So how can SSE replace a physical datacenter FW? To understand that, we need to better understand the role datacenter FWs play.

The Multi-function Datacenter Firewall



1 Secure Access to the Internet

First, just like a branch FW, the FW at the datacenter secures access to the internet. It makes sure applications hosted in the datacenter are accessing internet-based resources securely. This security functionality can extend to any users who backhaul to the datacenter for secure internet access.

2 Secure Access from the Internet

Second, the datacenter FW secures access from the internet. Publicly facing services that are hosted in the datacenter must have ports open to inbound traffic. The datacenter FW applies security to that inbound traffic, protecting the network behind the FW.

3 Secure WAN Access

Third, it provides WAN access security. The datacenter FW controls access to specific servers and applications from specific users or teams. It also provides full monitoring and event logging for business and regulatory compliance purposes.

4 LAN Segmentation

Finally, it provides LAN segmentation, securing access between the datacenter LANs and subnets. In this role, the datacenter FW ensures that network separation within the datacenter is enforced, managed and monitored.

The Right SSE to Replace the Datacenter Firewall

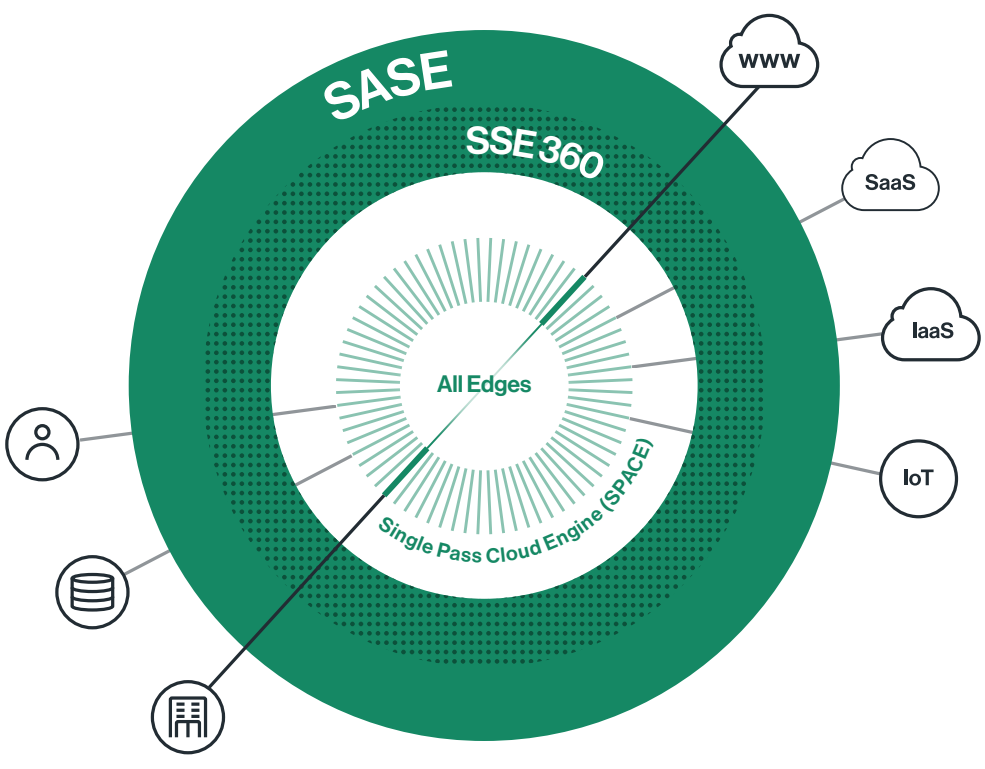
Now that we understand all of the roles a datacenter FW can fill, we can start to think about how a SSE could deliver that functionality.

Secure Access to the Internet

All internet bound traffic should pass through the SSE for protection. You should be able to set allow or block rules between network entities such as sites, individual users, subnets, and more to various applications, services, and websites. Remote users shouldn't have to backhaul to the datacenter to access the internet securely, they should just go directly through the SSE from wherever they are in the world.

SSE includes SWG as an essential component, allowing allow you to monitor, control and block access to websites based on predefined and customizable categories. You should also be able to configure access rules based on URL categories. And, of course, you'll need an event log of security events on each access to specific configurable categories.

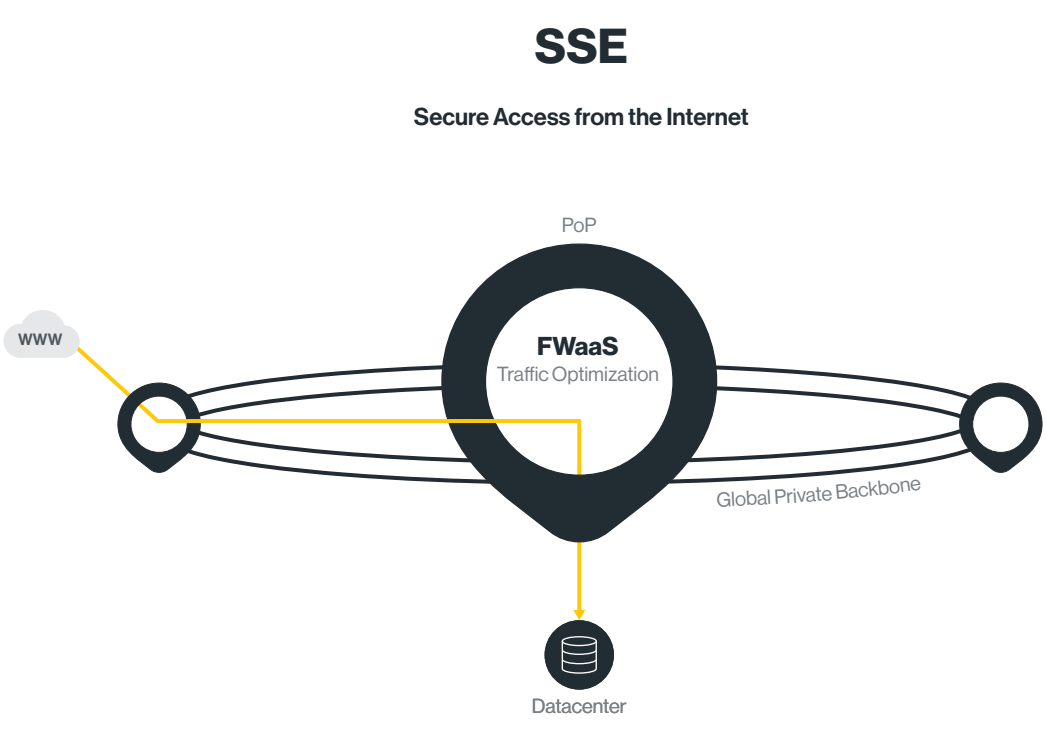
With built-in threat prevention, SSE can also provide anti-malware and IPS capabilities as a service. The as-a-service delivery ensures that signatures are always up to date, and because it's delivered in the cloud, it wouldn't be subject to the compute constraints of edge appliances. Instead, it would enable unlimited TLS inspection and IPS signature processing.



Secure Access from the Internet

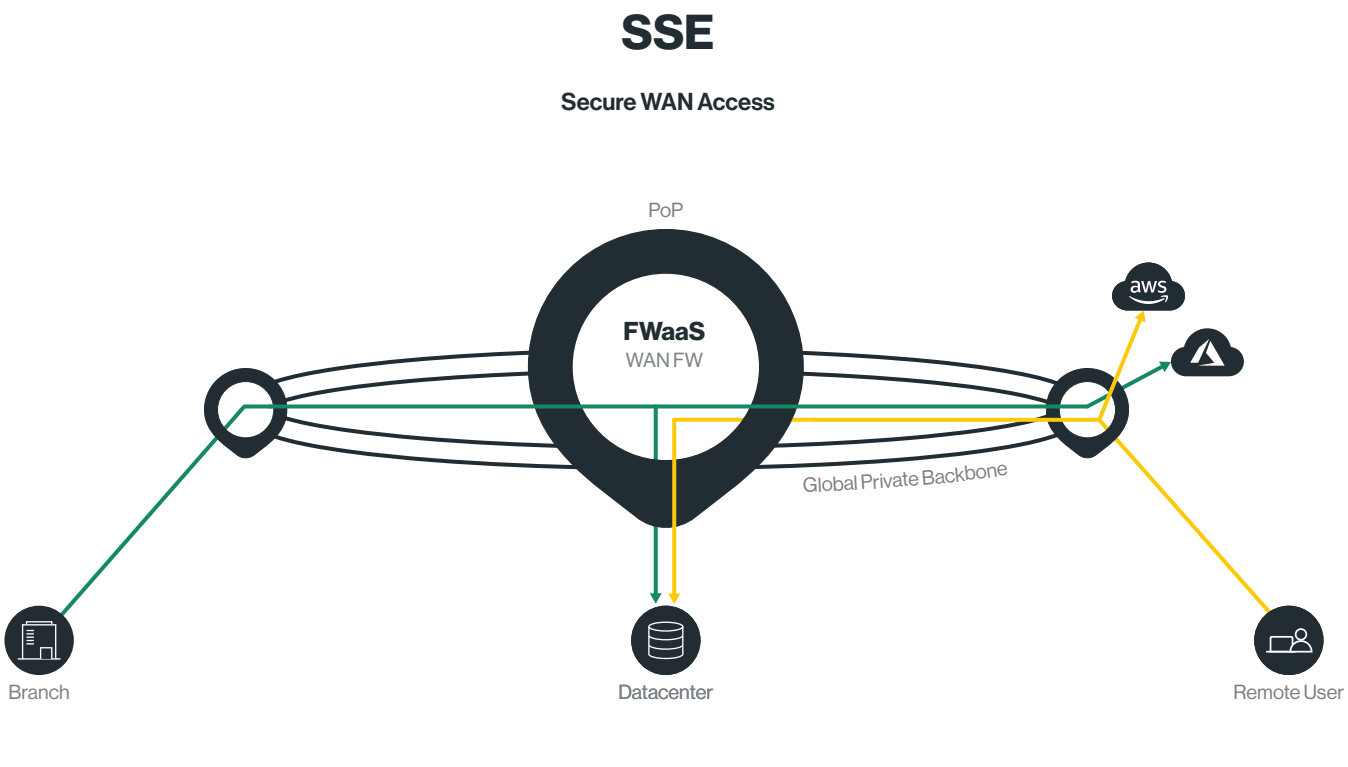
Many SSE's are designed using proxy architectures and can only secure outbound Internet traffic, even if they offer basic FWaaS capabilities. SSE's built from the ground up using a NGFW architecture can also secure traffic destined for applications hosted in the datacenter. These SSE's deliver NGFW as a cloud service and aren't limited to the legacy and physical constraints of on-premises firewalls. Instead, you would be able to set port forwarding rules on a remote PoP, and the SSE will automatically steer the traffic to the right server and application in your WAN.

A more detailed overview on how to create a DMZ within your datacenter using a SSE can be found in the Appendix.



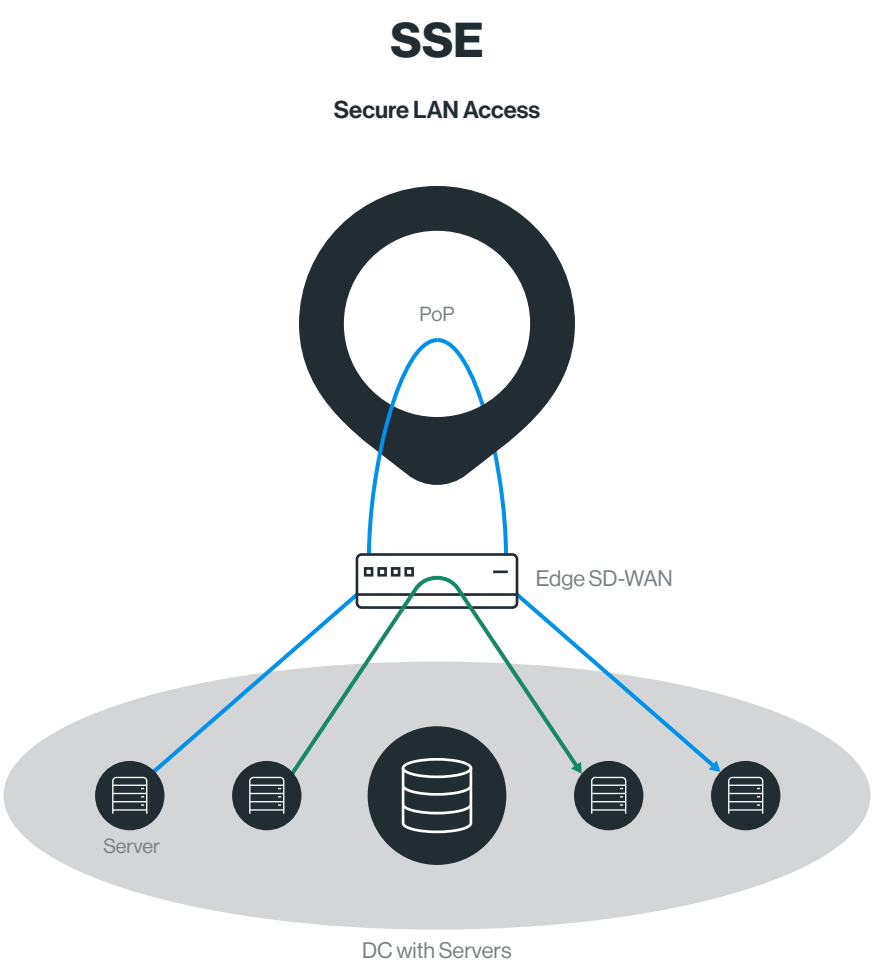
Secure WAN Access

To secure WAN traffic, the SSE must include a WAN firewall so that traffic can be allowed or blocked between organizational entities such as sites, users, hosts, subnets, and more. And, unlike a network FW, a WAN FW can take advantage of user awareness capabilities and advanced threat prevention.



Secure LAN Access

VLAN traffic should be secured like any WAN traffic, by sending traffic to the nearest SSE PoP and inspecting it with all access control and threat prevention engines. To avoid any latency issues, it's important that the PoP be close to the datacenter, ensuring a minimal round trip time. And, for trusted, high-volume, latency-sensitive traffic, you should have the option to route that traffic locally on an on-premises edge appliance. No traffic should be allowed between different segments without the creation of local routing rules or inspection in the SSE.

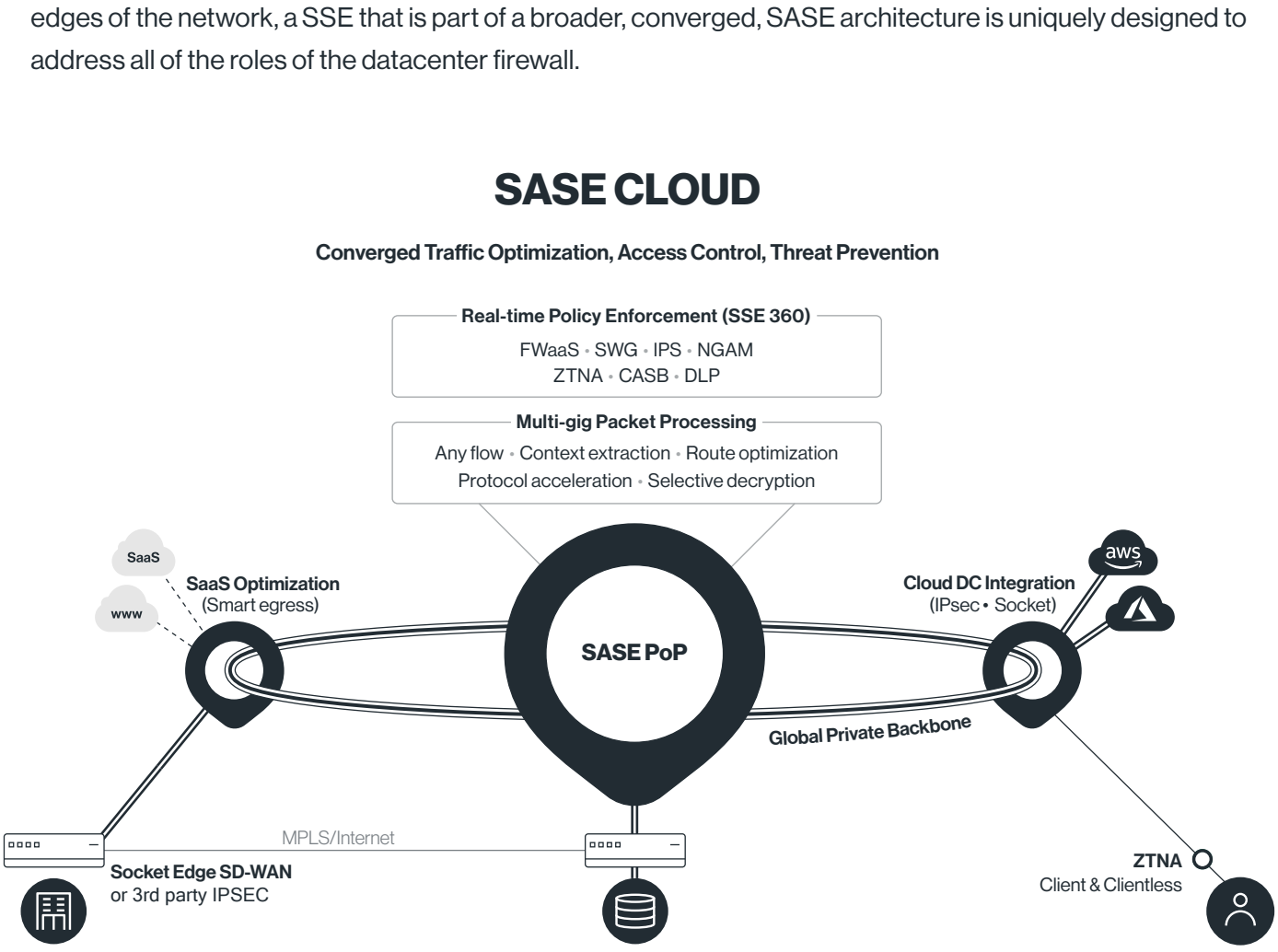


The Right SSE Needs the Right Architecture

The challenge with leveraging a SSE to meet all of the datacenter firewall requirements goes beyond just functionality – it needs to have visibility into the entire network. That's simply not possible with architectures built on legacy notions of an enterprise perimeter. Today's enterprises are no longer contained within physical offices and datacenters, and now rely on applications and datacenters in the cloud, with mobile users distributed all over.

Unfortunately, most SSE offerings are designed to address Internet traffic only, primarily covering users accessing cloud applications. They typically lack the visibility to protect WAN traffic, including remote users accessing internal applications. Moreover, unless the SSE provider has a large network of PoPs, the distance from the user to the nearest PoP is often too great, causing latency issues and impacting performance. So, while moving security to the cloud can solve many issues, we still need to make sure the SSE solution can govern all applications, ports, and protocols while accounting for traffic in all directions.

This is why architecture is a key factor in Gartner's definition of the Security Service Edge. The delivery of security an ZTNA capabilities as a cloud-native services requires a true single-pass engine and global presence. SSE is a subset of Gartner's Secure Access Service Edge (SASE) and a converged SASE platform can offer enhanced SSE capabilities as well as a future path to full SASE. With full visibility into all edges of the network, a SSE that is part of a broader, converged, SASE architecture is uniquely designed to address all of the roles of the datacenter firewall.



Transitioning on Your Time

When it comes to transitioning away from your legacy architecture, it should be easy to migrate on a timeline that makes sense for you. In fact, the architecture should support leaving the datacenter FW in place and still allow you to take advantage of most of the other benefits of the SSE.

Since replacing the branch firewall with SSE is the easiest step, any SSE deployment should start with the basic configuration of securing access to the internet. This is achieved with connectivity through an IPSec tunnel to the SSE PoP. From there, the SSE should support gradually transitioning rules, enforcement and inspection, eventually enabling you to remove the datacenter firewall.

Cato's SSE 360 as Your Datacenter Firewall

Replacing a datacenter firewall is fraught with challenges because it serves so many purposes. Simple security solutions like a cloud firewall or a SWG are designed to address single use cases and cannot completely replace all of the functionality of the datacenter firewall. That's why you need a new approach to your entire networking and security. Cato's SSE 360 solution, built on a cloud-native architecture, is uniquely designed to meet that challenge. Cato's ability to secure traffic to all of your edges while providing full visibility and control, gives you all of the functionality you need from your datacenter firewall.

As a cloud-native architecture, with full visibility across the entire network, Cato's solution includes:

NGFW

Our NGFW provides full application awareness with the ability to inspect the payload of packet data and distinguish between different types of web traffic. The NGFW inspects both WAN and Internet traffic and can enforce granular rules based on network entities, time restrictions, and type of traffic. The Deep Packet Inspection (DPI) engine classifies the relevant context, such as application or services, as early as the first packet and without having to decrypt the payload. Cato provides a full list of signatures and parsers to identify common applications. In addition, custom application definitions identify account-specific applications by port, IP address or domain.

Secure Web Gateway

Cato provides a SWG to give you granular control over your Internet-bound traffic, enabling enforcement of corporate policies and preventing downloads of unwanted or malicious software. We provide predefined policies for dozens of different URL categories and support custom rules, enhancing the granularity of web access control. As with the rest of our service, the SWG is easily managed through Cato's management portal and covered with full event logging.

Advanced Threat Prevention

As part of Cato's Advanced Threat Prevention, Cato offers anti-malware and Intrusion Prevention System (IPS) capabilities. Both services inspect WAN and Internet traffic. Cato PoPs inspect TLS-encrypted traffic in the Cato Cloud, so there is no scaling constraints or additional latency.

Managed Threat Detection and Response to Reduce Dwell Time

Cato's Managed Threat Detection and Response Service (MDR) enables enterprises to offload the resource-intensive and skill-dependent process of detecting compromised endpoints to the Cato SOC team. Cato seamlessly applies a full MDR service to customer networks. We automatically collect and analyze all network flows, verify suspicious activity, and notify customers of compromised endpoints. This is the power of networking and security convergence to simplify network protection for enterprises of all sizes.

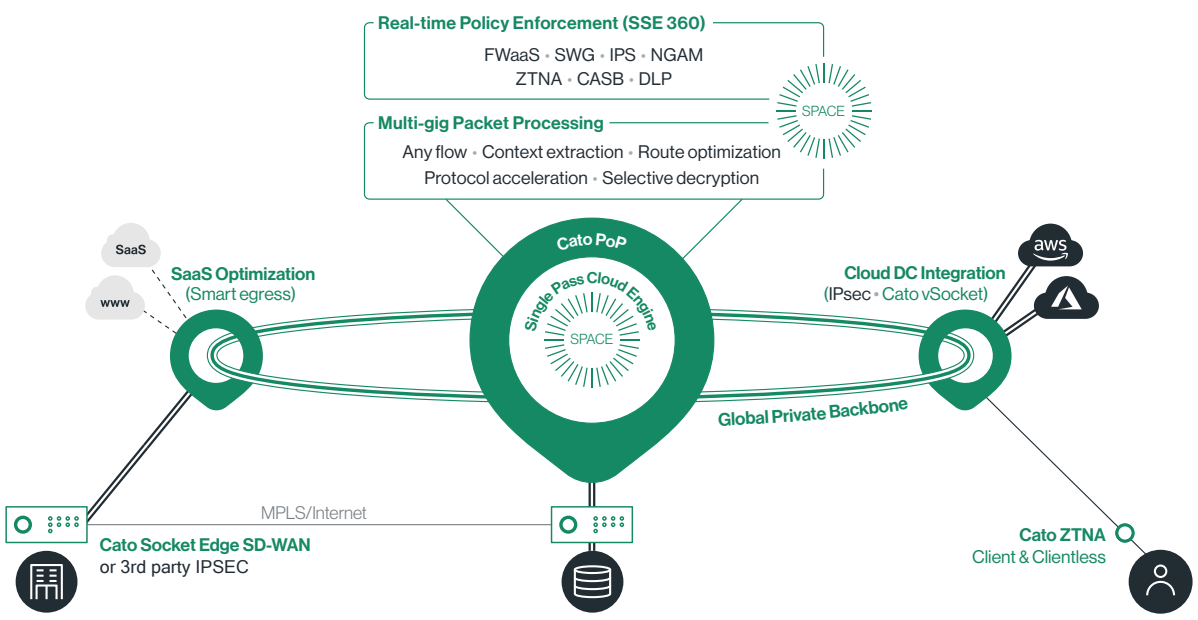
Event Discovery

Event Discovery (called Instant*Insight) provides any IT team with the advanced hunting and research capabilities of a high-end operations center. Event Discovery organizes more than 100 network and security events into a single, queryable timeline. Complex queries can be easily built by selecting from the types and sub-types of events presented on the screen. The data warehouse is stored and maintained by Cato.

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. Using 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.

Cato SASE Cloud with SSE 360



Cato SASE Cloud

SSE 360
Secure Remote Access
Edge SD-WAN
Global Private Backbone
Multi-cloud / Hybrid-cloud
SaaS Optimization
Cato Management Application

Use Cases

MPLS Migration to SD-WAN
Secure Remote Access
Secure Branch Internet Access
Optimized Global Connectivity
Secure Hybrid-cloud and Multi-cloud
Work From Home

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.

Additional Reading

The Network for the Digital Business Starts with the Secure Access Service Edge (SASE)

Download →

SASE: The Architecture for the New Enterprise Perimeters

Download →

Cato Networks Security as a Service

Download →

A Practical Guide to SASE Migration

Download →

Appendix

Where Did My DMZ Go?

Internet-facing services and applications used to be hosted in a DMZ that was bounded to the physical location of the datacenter Firewall. But a SSE allows you to migrate servers and applications that used to be in the datacenter to the cloud or disparate locations – with minimal risk and policy changes. SSE doesn't care where the DMZ is physically, it only needs the DMZ to be defined, so if you move it (or parts of it) to AWS or Azure, all the access controls to it (from the internet and from the WAN) will just follow, With Cato Cloud, your DMZ now becomes just another VLAN. You have full visibility and control over the traffic. With our SSE 360 architecture, traffic always goes through the SSE cloud PoPs and security inspection first, rather than directly to your LAN. If you don't have to put your DMZ on a separate physical port, you can even move your DMZ anywhere in your network – because Cato gives you uniform firewall security strength across the network.

And since Cato is a Security as a Service solution, it is always up to date, keeping your security at the optimum posture.