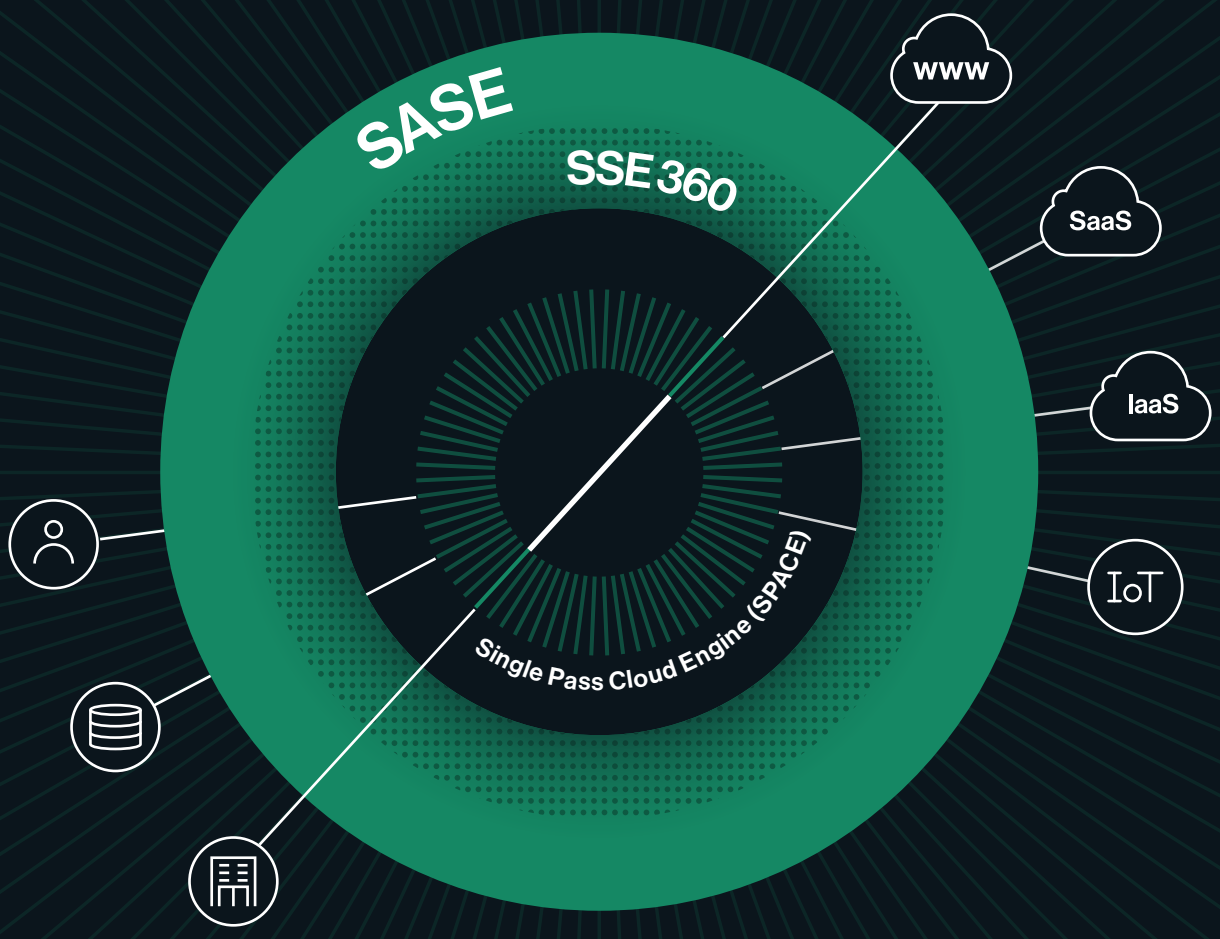
CATO
NETWORKS

The Business Case for Security Transformation with Cato SSE 360



Executive Summary

Enterprises are moving more of their security operations, including remote access, to the cloud. Cato SSE 360 is a single security stack that converges network security and remote access technologies into a scalable, globally distributed, cloud-native platform. This provides the security, performance and cost efficiencies that today's digital enterprises are demanding.

This document will analyze a simple total cost of ownership model of Cato SSE 360 vs. a traditional network security product. There are 4 buckets to analyze:

Products

These include network security appliances (Firewalls, NG Firewalls, IPSs, UTMs and URL Filtering).

Services

This includes Managed Security Services for extended network security.

People

The IT staff needed to maintain the IT infrastructure. The main driver here is relieving staff of unproductive tasks designed to keep the lights on to more valuable strategic activities that improve security and address emerging threats and business needs.

Risk

The organization's exposure to the overall security risk, considering the impact of the factors above (products, services and people) on the security posture.

Products

In this section, we will look into the cost associated with network security products that are targeted for replacement by Cato. There are 3 primary cost items:

Purchase/Refresh

The cost of purchasing or refreshing security appliances. This cost is eliminated with Cato. In the table below, we also included capabilities you may have today, which could be avoided with Cato.

Subscriptions and maintenance

Recurring cost for software and hardware maintenance. This cost is typically eliminated by Cato.

Forced upgrades

Device capacity constraints, rapid growth, or the need for more capabilities can force an upgrade (outside the normal lifecycle). Since this cost cannot be anticipated, we added a Forced Upgrade column for your consideration. This cost is typically eliminated by Cato.

3-Year Cost	Purchase/ Refresh	Maintenance/ Subscription	Forced Upgrade	Current Costs	Cato Costs
Firewalls					
UTMs					
URL Filtering					
IPS					
Anti-Malware					
Sandbox					
Total					
Savings					

Services

In this section, we will investigate a key service used to run your security operations.

Managed services

For security monitoring and policy changes, organizations typically have 2 options: hire a Security Operations Center (SOC) or build it themselves, neither of which is simple nor inexpensive to launch and manage. Cato or its partners can offer a managed security service based on Cato's platform that is simple, easy to manage, and requires less friction with the customer premises. Our Managed Detection and Response MDR services provide ongoing security monitoring of your network for compromised endpoints, and we will notify you daily and guide you on how to remediate the malware infection.

3-Year Cost	Current Costs	Cato Costs
Security Operations Center (SOC)		
Total		
Savings		

People

This section will investigate the various activities and required headcount to run security operations. You typically need to estimate the current headcount needed and what can be reassigned to higher-value tasks. Headcount savings tend to be soft and are associated with better response times to business needs and overall reduced risk. These are the categories where time and resources are needed to run the infrastructure:

Planning and project management

This is the time and resources to spend on performing capacity planning for appliance purchases and upgrades and the process of deploying them into the network. Some of these activities are part of a normal cycle and some are crash projects. With Cato, we are responsible for capacity planning to ensure our services can handle any customer capacity as the business scales.

Configuration management

Time and resources were spent addressing change requests from the business, like new SDP users, new policies, and security changes. With Cato, a simple rule change can adapt the enforcement of corporate-wide policies as the threat landscape evolves. No need to manage complex multi-site hardware appliances or plan the deployment of policies to relevant firewalls.

Patch management

Upgrading appliance software and applying security patches, including addressing failures and user impact. Cato eliminates patch management requirements for IT. All software maintenance is done by Cato.

Network security troubleshooting

Addressing security policy, protection schemes, and remote access problems. Cato provides simple end-to-end visibility for all users, applications and their activity, drastically simplifying troubleshooting.

Productivity loss

End-user productivity is directly impacted by the user experience of the provided security services. This includes complicated policy configurations and longer lead times to provision access to suboptimal security services. Cato provides consistent policy enforcement to all users worldwide, improving their overall experience and productivity.

3-Year Cost	Current Costs			Cato Costs		
	HC Rate	HC Count	Total	HC Rate	HC Count	Total
Planning and project management						
Configuration management: new users, policy changes & errors						
Software management: patches, updates and upgrades						
Troubleshooting						
Productivity loss: outages due to security threats, ransomware, etc.						
Total						
Savings						

Risk

In this section, we will look into the risk factors that can be reduced by moving to Cato SSE 360. Risk is a soft ROI element that is typically calculated by the value of the exposure times the probability of the risk materializing. These are the risk elements for consideration:

Outdated defenses

Not using the latest capabilities due to slow upgrades and patches. Cato keeps the service up to date.

Capacity constraints

Weakened security posture due to equipment capacity constraints, forcing minimal security coverage. Cato enables all security services licensed by the customers and takes care of the needed capacity to deliver them.

Configuration errors

Higher exposure to attacks due to policy misconfiguration across appliances and solutions that increase attack surfaces. Cato's converged security platform and unified policies reduce exposure to configuration and integration errors.

3-Year Cost	Exposure $ (est)	Reduced Exposure with Cato (%)	Reduced Exposure Impact ($)
Outdated defense against current and emerging threats			
Reduced security posture due to capacity constraints			
Configuration and policy errors			
Total			
Risk reduction value ($)			

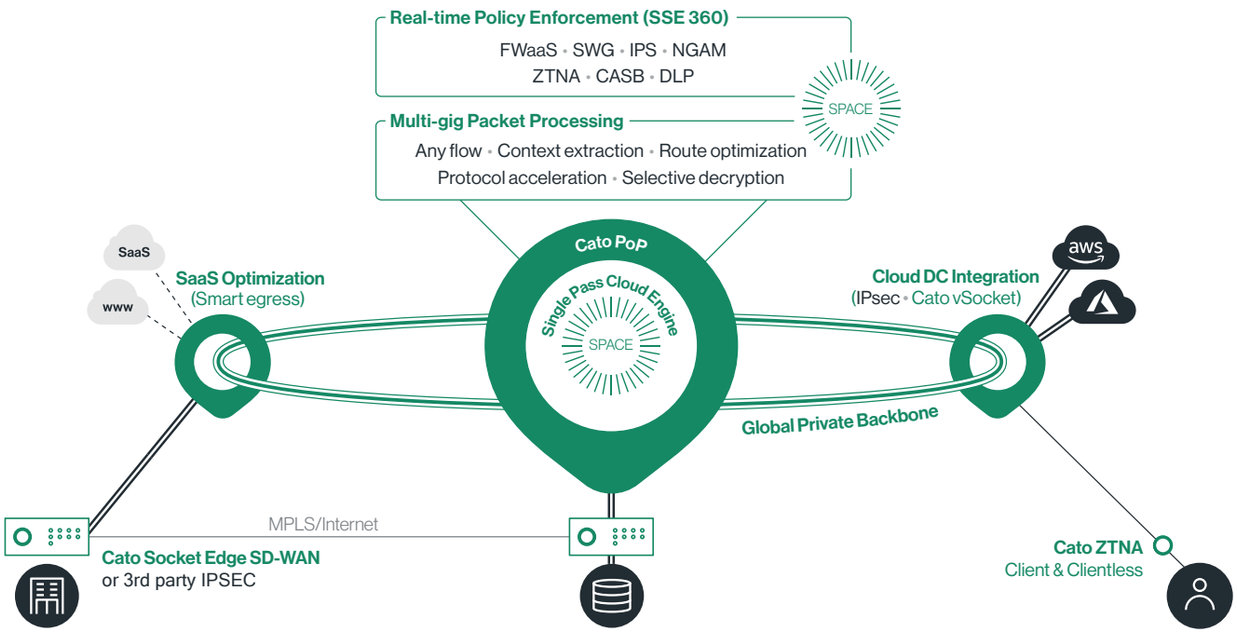
Summary

3-Year Cost	Current Costs	Cato Costs
Products		
Services		
People		
Risk		
Total		
Savings		

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. Ready for Whatever's Next.

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

Contact Us

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