CATO
NETWORKS

Outcomes vs. Tools

Why Cato SASE is the Right Strategic Choice vs. Legacy Appliances

The Future of IT Is In The Cloud

Cato has envisioned networking and security delivered as a cloud service since its inception in 2015. It was the evolution of an appliance-centric architecture that dominated IT since the mid 90s. In many ways, this evolution followed a similar path to the way Amazon Web Service (AWS) has evolved the legacy datacenter architecture.

AWS's global cloud service, built and maintained as a common shared infrastructure, enabled organizations of all sizes to tap into a unique set of capabilities, previously available only to the largest organizations. Scalability, resiliency, elasticity, security, connectivity, and global distribution are a few of these capabilities. AWS, and later Azure has evolved so much in the past 20 years, that even organizations that could build a similar infrastructure had decided to migrate over to the new cloud platforms. The rate of evolution of the cloud providers platforms and capabilities, as well as their people, skills, and resources, created an unmatched value that couldn't be ignored by IT leadership.

AWS was never the lowest cost provider. It remained cheaper to host commodity servers in regional hosting facilities and maintain them, instead of paying for virtual servers running on AWS. Yet, companies chose AWS because the comparison wasn't just between server instances, but rather on the implications of owning and running them. Businesses wanted to focus IT on critical projects and strategic initiatives rather than the mindless grunt work of infrastructure upkeep. Cloud migration helped IT to increase business responsiveness and become an enabler to the business, rather than a cost center. In short, AWS became an extension of the IT team in running the infrastructure that powers the business.

Cato is following the footsteps of AWS, in global networking and network security. The Cato SASE Cloud is a purpose-built platform for high performance routing and security inspection of enterprise network traffic. Cato is built around its cloud service that is continuously maintained and optimized for high availability and maximal security posture by world class experts in DevOps, networking, and security. Our technical teams are a natural extension of the customer's IT team with our resources, skills, and 24x7 availability.

This is the Cato difference. We own the outcome of secure and resilient infrastructure; we don't just leave boxes behind for the customer to sort them out. Cato is offering a partnership with the best people, skills, technology, and focus for the best business outcomes.

Consider

What is the business value of a partnership that extends your IT capabilities to effectively deliver what the business needs, while keeping IT in full control?

Cato vs. Appliances: The Right Way to Compare

We often meet customers that compare quotes from Cato and appliance vendors. Cato can be more expensive, which begs the question how we justify the value. Here are some points for consideration.

Cato is Built for Outcomes, Appliances Are Tools

Cato is built as an organization and technology platform to ensure highly available, scalable, and secure connectivity for all locations, users, and applications. You onboard your resources into the Cato SASE Cloud and your networking and security shift into autopilot.

No brainer capacity planning

Up to 500mbps, or larger. Choose the right edge. No matter what capabilities you sign up for, the extent of SSL decryption needed, Cato will handle it without disruption.

No infrastructure maintenance

No patching, no upgrades, no maxed-out equipment.

24x7 NOC

Making sure the full set of capabilities are available 99.999% of the time. Helping you identify root cause of problems, even when they aren't related to Cato.

24x7 SOC

When new, critical vulnerabilities and threats show up, our SOC builds the mitigations, validates they don't break traffic, and deploys them globally, in matter of hours.

24x7 Support

Support is as effective as the engineering organization that backs it up. As our team is built around the service, the path to get the right expert to analyze a particular service issue is extremely short, so troubleshooting is accelerated. Furthermore, the support included in Cato's service is about how our service is working towards the outcome you want to achieve.

Appliances are tools that require continuous IT support to achieve the business outcome.

Deployment and capacity planning complexity

Appliances need to be sized, deployed, and maintained. Maintenance windows must be identified and coordinated across sites, often leading to late night and weekend work.

The capacity vs. usage tradeoff

Appliance performance depends on what they are tasked to do and how much heavy lifting is needed with decryption and inspection. If you disable or avoid activation of demanding security features, you put the business at risk. If they are maxed-out they need to be replaced which leads to service disruption and unexpected costs for buying new hardware and software.

The security posture maintenance challenge

When new security mitigations are created by the appliance vendor, IT needs to validate them for performance impact and ensure no business traffic stops. Since resources are scarce, and this is a recuring task, it often leads to sub-optimal security posture and reduced threat prevention effectiveness. It is a small gap that can lead to a breach – especially when it is created by a known vulnerability.

The extended attack surface of appliances

When appliances experience software vulnerabilities of their own, customers are on the hook to upgrade all appliances on the network or risk a breach. These fire drills task your IT resources and could impact support for critical business initiatives.

Support effectiveness with limited customer environment access

When networking or security functionality doesn't work as expected, vendor support have limited visibility and awareness of the customer environment which prolongs troubleshooting.

When you measure Cato's value, you consider the outcome of fully maintained, highly available, and optimally secure network for the business. When you measure appliances' value, it is tied to how much pain and headaches they caused your team in achieving the business outcome and how well your resources and skills are aligned with running the appliance infrastructure to achieve it.

Consider

What is the value of partnering with a vendor around an outcome vs buying a tool?

Cloud-Delivered vs. Appliance-Delivered Software: The Feature Difference

Features aren't created equal. They are different in their deployment, management, scalability, and effectiveness, based on the way they are delivered and consumed. Let's go over several examples.

Managed vs. Standalone Features

Cato's Intrusion Prevention System (IPS) is a fully managed security offering. Cato security experts own the outcome of always keeping the IPS in a fully optimized security posture. This includes evaluating new threats and vulnerabilities, developing the mitigations, and deploying them in full prevention mode after ensuring traffic isn't broken and performance isn't impacted.

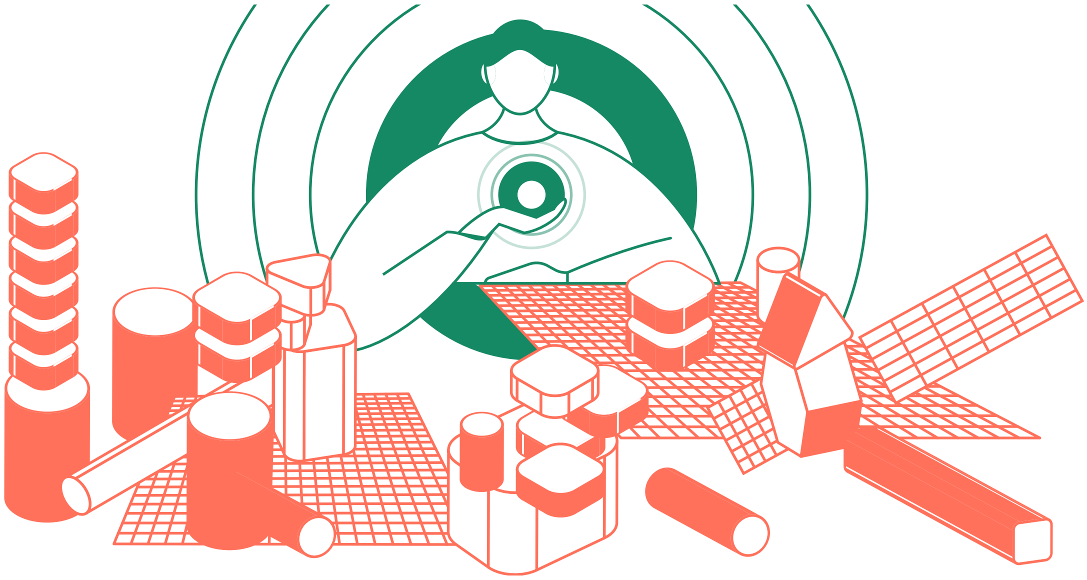
Compare this with a similarly named IPS from an appliance vendor. A big chunk of the process described above falls on your team. While the vendor creates the mitigations, the responsibility of deciding if and when to deploy a mitigation, assessing its impact on appliance performance and business traffic, and then ensuring all appliances in the environment are kept up to date falls on IT. This isn't a theoretical issue. The load this process creates, and the risks associated with it, makes many IT organization shift their IPS to "detect mode" instead of ensuring it helps defend the organization against attacks in "prevent mode". IT organizations can partner with managed security service providers (MSSPs) for that process, but this will dramatically increase the costs of keeping optimal security posture.

Consider

What is the value of having optimal security posture without ongoing investment in the resources and skills needed to maintain it?

Adaptable vs. Rigid Features

Having a particular feature activated needs to be analyzed in the context of inspection capacity and location. For example, if a group of sites from acquisition is added to the network with centralized firewalls, they may not be able to handle the additional load. If the remote access VPN solution was built to handle 10% of the workforce, and it suddenly needs to support 100% of the workforce overnight, it may not be able to scale to do it.



Using appliances that are both location bound and capacity constrained, customers must be able to predict what inspection capabilities they need today and will need in the future and at what geographical locations. These predictions are thrown off by unpredictable changes to the volume of expected traffic, and the distribution of branches, users, and applications. This is the context of being able to support the business instead of being perceived as a blocker to the business.

The value of using Cato's cloud-native architectures is to make inspection capabilities available at any scale and at any location in a seamless fashion. You will not be caught off-guard with a misaligned infrastructure due to changes in load or requirements in specific locations, or for specific features.

Consider

What is the value of having an infrastructure that can accommodate ANY change in the business environment and support ALL new growth initiatives?

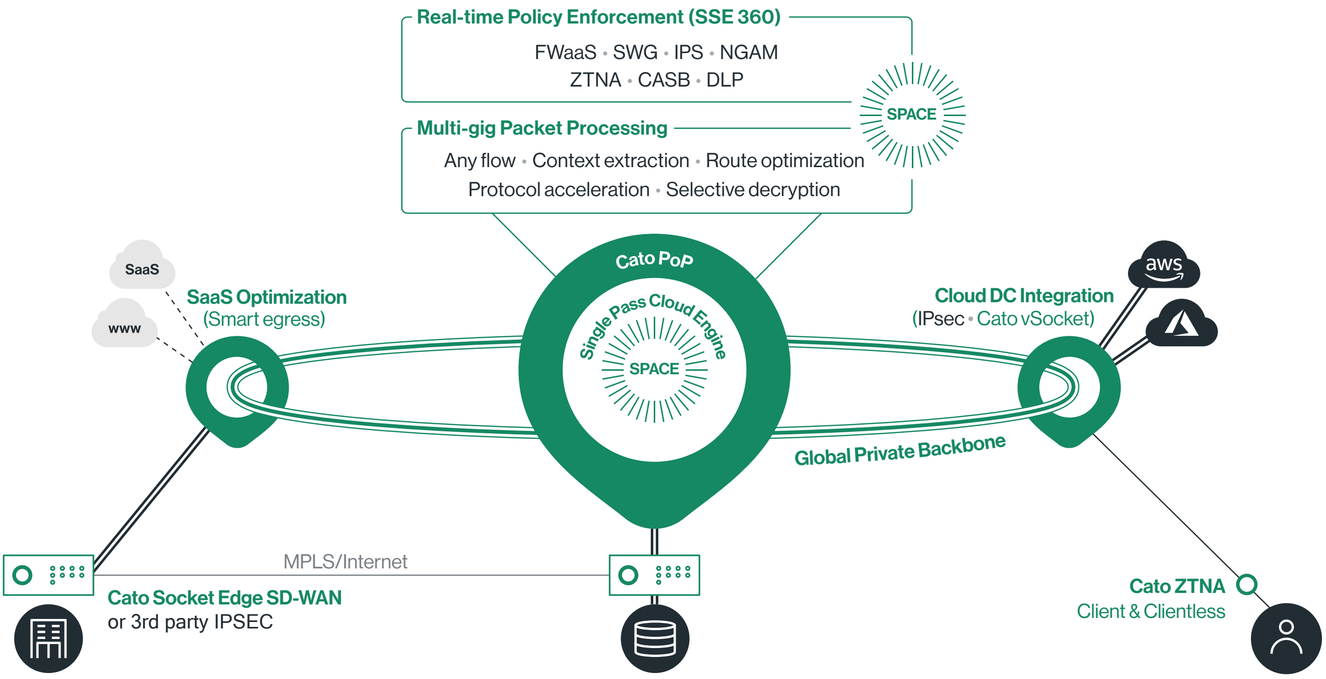
Conclusion

Agile and flexible networking and security infrastructure is essential for achieving the outcomes needed to drive the modern business. The long-established legacy of "do it yourself with tools" is hard to sustain over the long haul because the expertise and resources needed to support and optimally run complex infrastructure is becoming increasingly scarce. Budget constraints and skill scarcity are driving organizations to build relationships with technology-as-a-service providers that combine the agility of the cloud and world-class technical talent to expand their capabilities beyond what they could achieve on their own. This new partnership model is essential to achieving the business outcomes that are the strategic goal of all organizations.

About Cato Networks

Cato provides the world's most robust 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 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.

CATO NETWORKS

Contact Us