NETWORKWORLD FROM IDG

SPONSORED CONTENT

eBook

HOW TO ENABLE AN ELASTIC NETWORK PERIMETER WITH **SECURE SD-WAN**

IDG COMMUNICATIONS INC.

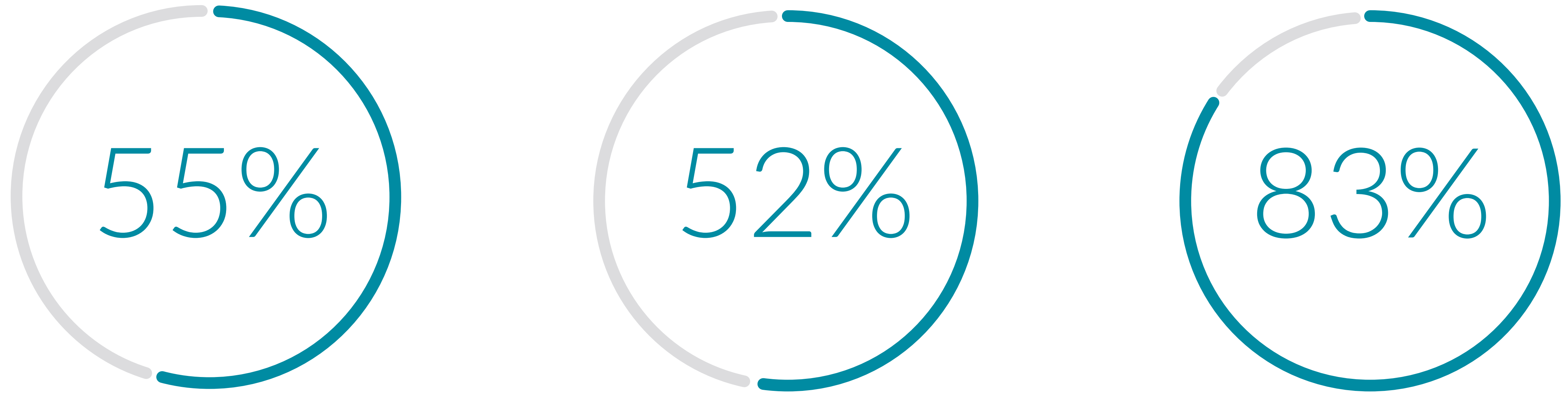
IN 2020, millions of employees around the world became remote workers overnight, and once the pandemic finally recedes, many of them won't be returning to the office, at least not completely.

In fact, more than half (55%) of employees expect to continue working from home at least three days a week, according to the 2021 PwC Remote Work Survey. And it's likely their employers will support them. In the same survey, 52% of managers said employees have been more productive working from home, and 83% said that remote work has been a success. A hybrid work model will likely become the new norm.

This change in the workplace has also changed the networks enterprises use to conduct business. Providing services to employees inside the relatively safe confines of the corporate firewall is very different from connecting end users to the applications and data they need from outside the network perimeter.

Supporting remote workers is not the only challenge. The pandemic accelerated enterprise adoption of cloud and software-as-a-service (SaaS) applications. More than half (55%) of organizations expect to be mostly or entirely in the cloud by 2022, according to the 2020 IDG Cloud Computing Survey. On average, they expect 36% of their applications to be SaaS by 2022.

WORK FROM HOME SUCCESS STORY



Employees who expect to continue working from home

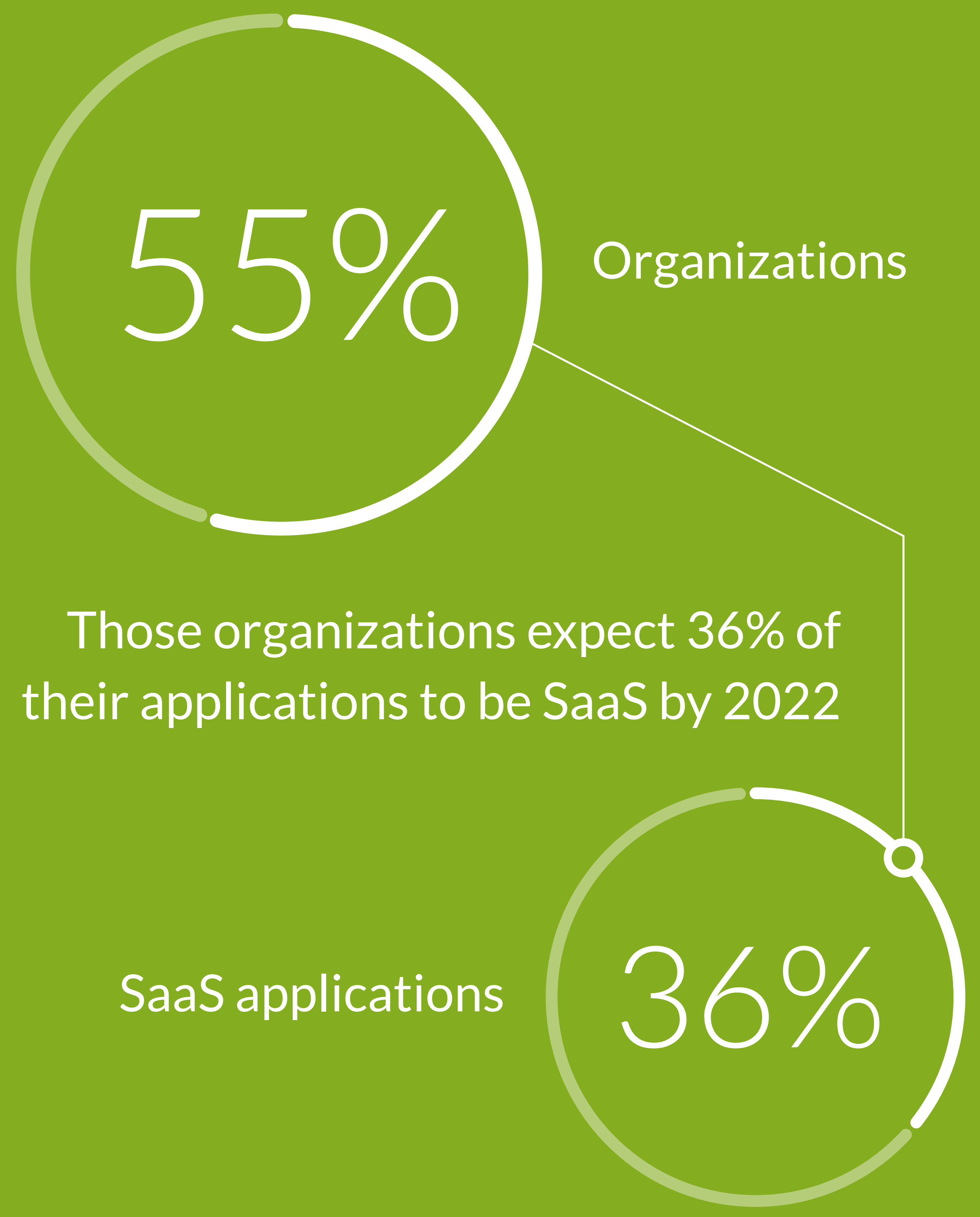
Managers who feel employees are more productive when working from home

Managers who believe remote work has been a success

SOURCE: 2021 PWC REMOTE WORK SURVEY

CLOUD ADOPTION

Organizations that expect to be mostly or entirely in the cloud by 2022:



Those organizations expect 36% of their applications to be SaaS by 2022

SOURCE: 2020 IDG CLOUD COMPUTING SURVEY

NETWORK PERIMETER PROBLEMS

This rapid change in the enterprise network has profound implications for the traditional network perimeter security model. For starters, the massive increase of remote workers significantly expands the attack surface. If employees are in the corporate office, IT can deploy managed desktop security, manage firewall settings, and ensure there is only one way in and out of the network.

When employees work from home, IT may still control their laptops and other devices, and some may require employees to connect via a virtual private network.

But IT has no control over what other devices may be connected to an employee's home "network": TVs, home routers, cameras, or thermostats. Any of these devices could have security flaws, and they're sharing the same network as the employee's corporate laptop. So, even if the laptop is connected via VPN, the enterprise still faces risks with the work-at-home setup.

In addition, encrypted tunnels are complex and cumbersome to manage and scale. They add processing overhead that can degrade users' experience. And if the VPN experience is too detrimental for employees to work efficiently, they can start doing end runs around corporate policies, in which case there may as well be no VPN at all.

If the VPN experience is too detrimental for employees to work efficiently, they can start doing end runs around corporate policies, in which case there may as well be no VPN at all.

SECURITY OUTSIDE THE PERIMETER

The other significant change is proliferation of workloads in the cloud and SaaS applications. Each cloud and service will have its own security, which must be configured and protected. In the end, more than half of a typical company's users will be located outside of the firewall—as will many of its workloads.

Network security has not kept up with these changes, and cybercriminals have taken advantage. In April 2020, for instance, the FBI announced it was receiving three to four times the usual volume of cyberattack complaints. Hackers' methods also grew more sophisticated. In 2020, 35% of cyberattacks used previously unknown malware or methods, compared to 20% prior to the pandemic, according to a report from Deloitte.

The pandemic is also forcing organizations to rethink their internal network architecture. For example, the explosion in the use of videoconferencing has a significant impact on network bandwidth. In 2020, 30% of organizations started using web conferencing for the first time, according to a report from Twilio.

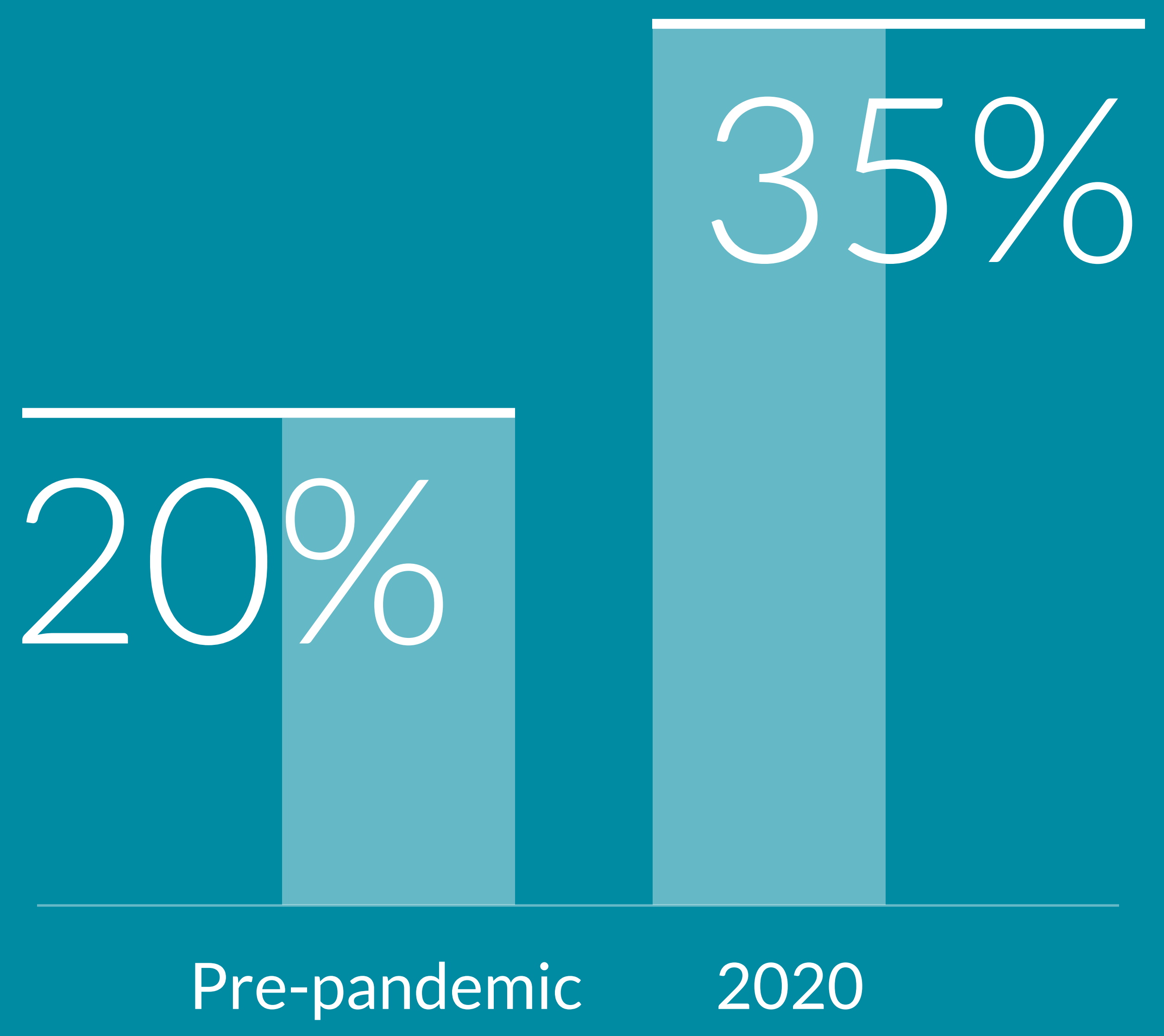
Live video streaming is a bandwidth-hungry application, and with employees holding remote conference calls, that effect is magnified. Without an architecture that can support peer-to-peer video streams, the incoming internet pipe will quickly become overloaded. Not surprisingly, in light of all these changes, 70% of executives plan to make investments in IT infrastructure to secure virtual connectivity.

Requirements for a modern secure network

In a nutshell, the traditional perimeter-based model for enterprise IT security is no longer sufficient. IT can't deploy a firewall around each employees' house, and backhauling everything—employee desktop connections, SaaS, and cloud traffic—to a corporate data center for inspection would introduce an extreme amount of latency. Also known as "traffic tromboning," this would make the network completely unusable because of poor performance and incur extra costs. Building a hub-and-spoke architecture out of that many VPNs would become far too complex to manage effectively.

CYBERCRIMINAL SOPHISTICATION ON THE RISE

Use of previously unknown malware or cyberattack methods



SOURCE: DELOITTE

THE NEW NETWORK REQUIREMENTS

Even though the world has changed, employees, partners, and customers still need immediate, consistent, and fast access to applications and data no matter where they are located. To meet end user expectations, keep costs manageable, and reduce complexity, the new network architecture must fulfill a number of critical requirements.

Base authorization on identity, not location

With so many devices, users, and applications outside the firewall, authorization and access based on IP address will not work, especially since IP addresses are ephemeral in autoscaling environments such as the cloud. Instead, the network must be able to leverage a system that authenticates the identity of every user, device, and workload.

Employ a zero trust approach

In this model, all traffic is treated as untrusted and denied by default unless it is identified, authenticated, and authorized. Zero trust follows the principal of least privilege, so each user, device, and workload are governed by policies that only grant users access to assets they need to do their jobs. No more, no less.

Zero trust must be inherent in everything you do. Enterprise IT cannot continue with an "anywhere to anywhere" mindset. Trust nothing and make security inherent in the network path. Zero trust is a powerful security framework. In fact, with 40% of IT and security leaders researching zero trust for their environment last year, it was the top technology solution of interest in the **IDG 2020 Security Priorities study**.

Make the network session-aware

At its most basic definition, a session is a temporary connection formed between two network assets so they can communicate. Sessions are bi-directional, meaning there are two related information flows. They have directionality, which relates to the asset that initiated the session. And finally, they have state.

These characteristics make every session unique, so the network can associate packets and flows with a session. Instead of simply sending packets, a session-aware network makes dynamic routing decisions based on sessions that can enforce policies and securely extend across network boundaries. It's a far simpler and agiler approach to secure networking.

The ability to build an elastic network is one of the big advantages of being session-aware. As noted earlier, many enterprises plan to move workloads to the cloud—so the enterprise must be able to enforce policy when connecting to assets on networks that IT does not control. In a very real sense, IT must extend the perimeter in an elastic way to encompass these assets. This flexibility enables IT to secure sessions even when they take place across networks that are constantly changing.

Build a network architecture that is edge-based

Processing can no longer be confined to a central core. Users, devices, and workloads are now widely distributed, sometimes with hundreds, even thousands of miles between them and the data center. At those distances, not even the speed of light is fast enough to overcome latency, and performance will suffer. Instead, processing must take place at the edge, close to the end user. As hyperscale cloud providers build out the cloud edge, this is rapidly becoming easier to do.

SASE, THE SECURE ACCESS SERVICE EDGE

Enter the Secure Access Service Edge, a network architecture better known as SASE (pronounced "sassy"). SASE converges unified security management, SD-WAN, firewall as a service, cloud access security broker, secure web gateway, and zero trust network architecture (ZTNA) to create a single, cloud-delivered service model that brings security closer to the edge.

But while SASE incorporates a number of functions, a secure, session-based SD-WAN solution is critical to the SASE-based architecture; one that can collapse multiple middlebox functions such as DPI, firewall, and load balancing into a single form factor, reducing complexity and cost.

The result is a much simpler and more agile platform capable of expanding and contracting in line with constantly changing business requirements. After all, it's far easier to scale software than it is to scale the myriad middleware boxes that have been bolted on to routing in order to provide session awareness. And where zero trust has proven extremely complex and cumbersome to enable on traditional perimeter-based networks, this paradigm is achievable by baking security into the network pathway with the right SD-WAN solution in place.

It's far easier to scale software than it is to scale the myriad middleware boxes that have been bolted on to routing in order to provide session awareness.

This SD-WAN design provides protection from attack no matter where digital assets are located. The network understands network services and routes them to the right security device whether it's in the corporate branch office or in the cloud.

That's not to say there isn't a place for traditional perimeters and firewalls. Small firewalls may still make sense for protecting a corporate campus, for example, and any good networking vendor should be able to support a hybrid model. But by themselves, they cannot provide sufficient protection, agility, and flexibility in a geographically dispersed, constantly changing network. That requires an SD-WAN solution with a SASE mindset.

SIDEBAR

SESSION SMART™ SD-WAN FROM JUNIPER NETWORKS

If SASE handcrafted an SD-WAN solution, it would be Juniper Networks Session Smart™ SD-WAN (formerly 128 Technology).

Powered by Secure Vector Routing instead of a tunnel-based architecture, Session Smart™ routers initiate each session with metadata to identify whether it comes from a trusted source, which can then be extended to any number of routers at any time. Its 100% deny-by-default approach to routing can easily segment traffic by groups and users to enable zero trust, and there's no need for a point-to-point encrypted tunnel. As a result, it's highly scalable, highly secure, and cuts down on network congestion by upwards of 60%. That's especially important when IT is dealing with expensive satellite connections or skinny home networks. Session Smart™ offers IT unfettered visibility into network traffic, enabling management of a global network from client to cloud with a single source of the truth.

One of the features that sets Session Smart™ SD-WAN apart from others is adaptive encryption. Approximately 80% of internet traffic is already encrypted, so there's no need to encrypt it a second time, especially because this adds unnecessary processing overhead that increases latency and hurts performance. But that's exactly what VPNs and many other traditional network security systems do. Through Session Smart™'s management console, called "the Session Smart™ Conductor," IT can easily set policies so encrypted traffic from sources like Zoom or Microsoft 365 isn't re-encrypted. Instead, it recognizes when data from these and other SaaS applications can be safely routed directly to the internet for an optimal user experience.

> "We evaluated the speed, the simplicity, the network orchestration, really everything around the product, and we built it out in all of our data centers and offices." MARK MARQUEZ Executive VP of Technology, Momentum

With Session Smart™ SD-WAN now under the Juniper Networks umbrella, customers can tap into the machine learning and AIOps engine to self-heal the network and use the Mist Marvis Virtual Network Assistant to quickly and easily identify network disruptions to sharply reduce downtime and fatal manual errors. Session Smart™ handles much of the routine work of networking so IT personnel can focus their time on value-add projects.

"Once you have that hyper segmentation of the user, policies, etc., you can take advantage of what Juniper has created with our AI-based model," says Sue Graham Johnston, VP/GM at Juniper. "You feed that data into the cloud, the operator sets policies, and the network is self-driving."

All these advantages have led organizations like Momentum Telecom, a VoIP and unified communications service provider, to deploy Session Smart™.

"We were looking for an SD-WAN solution that would really fit our customers' needs and improve how their businesses work," says Mark Marquez, Momentum's executive VP of technology. "Because of their applications, everything was going towards the cloud. We looked at the security around Session Smart™, and we looked at the adaptive encryption it offers. We evaluated the speed, the simplicity, the network orchestration, really everything around the product, and we built it out in all of our data centers and offices." Learn more at **juniper.net**.

THE MANY BENEFITS OF SECURE SD-WAN IN A SASE ARCHITECTURE

The powerful combination of a secure SD-WAN solution in a SASE-based architecture can benefit organizations in multiple ways.

Optimal User Experience

Experience is the new uptime. If the user experience is poor, security is a moot point. IT needs a network solution that monitors experience, makes real-time decisions to self-diagnose and self-heal, and applies global policies for security and performance regardless of user location.

Simpler WAN Management

Not all SD-WAN solutions are the same. IT should test drive and pilot a variety of solutions. Is the solution truly innovative and capable of modernizing the network? Or is it “lipstick on a pig?” Understanding the differences is key to ensuring favorable ROI.

Cost savings

The right SD-WAN solution allows IT to reduce costs in several ways. IT can take advantage of more cost-effective forms of connectivity such as broadband over MPLS; use a software-based approach to deploy it on commodity, white-box hardware; and collapse multiple middlebox functions into a single solution.

THE BOTTOM LINE

The new world of work, SaaS, and the cloud require a new model for security that’s more flexible, elastic, and agile than ever before. A secure SD-WAN solution must employ a ZTNA for far-flung end users, devices, and workloads outside the network perimeter; ensure strong performance and minimal latency; and help to meet the requirements of a SASE-based architecture.

To learn more visit **www.juniper.net**.

PN 7400138-001-EN June 2021

JUNIPer®
NETWORKS