Introducing The Zero Trust Edge Model For Security And Network Services

A Secure Access Services Edge (SASE) Is A Zero Trust Edge (ZTE)

by David Holmes and Andre Kindness
January 28, 2021

Why Read This Report

To support the digitalization of a company using cloud and internet of things (IoT), many networking teams turned to SD-WAN. However, SD-WAN doesn't address the new security requirements or the forcing function that security and networking worlds must merge. Both I&O and S&R professionals should read this report so they have a better understanding of an emerging Zero Trust solution that will help unify both the networking and security infrastructure to support the businesswide networking fabric.

Key Takeaways

Security Use Cases Will Lead Companies Into ZTE

The initial use case for most companies on a Zero Trust edge (ZTE) journey will be securing and enabling remote workers while removing the cumbersome user VPNs that plague the industry today.

The Internet-Edge Hosted Security Stack Is The Holy Grail, But It's Still Early Days

The ZTE model aspires to be a cloud- or edge-hosted full security stack, but the technology isn't all there yet since there are other dependencies. As long as bandwidth is a limiting factor in many parts of the world, some elements will need to be localized.

Don't Overlook The Intelligent On-Premises Edge For Efficiency

Use cases for making intelligent decisions on-premises at the edge still apply, especially for IoT/OT, healthcare, and networking-heavy environments.

Introducing The Zero Trust Edge Model For Security And Network Services

A Secure Access Services Edge (SASE) Is A Zero Trust Edge (ZTE)

by David Holmes and Andre Kindness
with Glenn O'Donnell, Joseph Blankenship, Paul McKay, Renee Taylor, and Peggy Dostie

January 28, 2021

Table Of Contents

Related Research Documents

Evaluate SDWAN Services Based On Branch Office Goals, Not Hardware Data Sheets

Now Tech: Software-Defined WAN Hardware/ Software, Q3 2020

Now Tech: Software-Defined WAN Services, Q3 2020

FORRESTER®

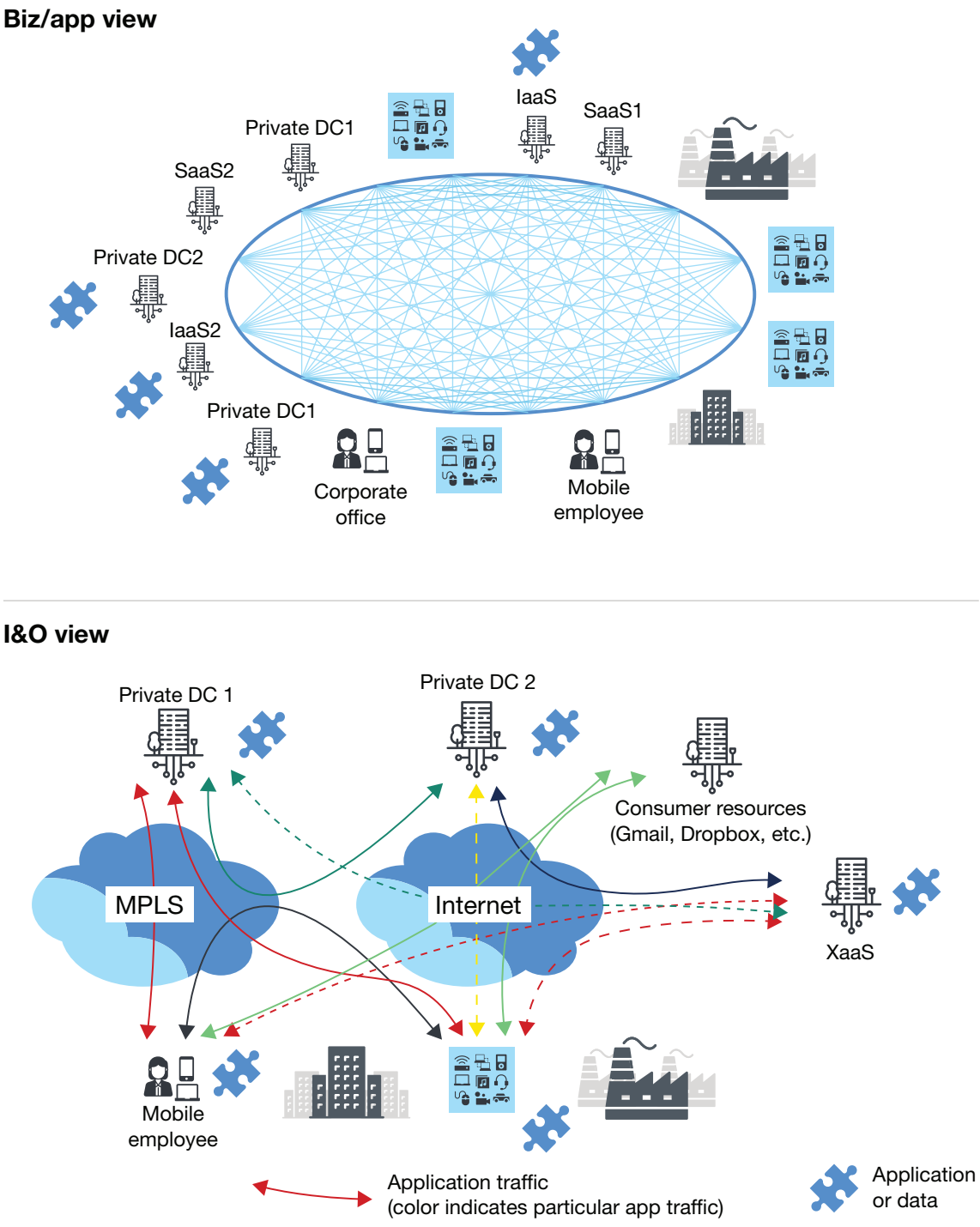
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Merge Security And Networking, Or Sunset Your Business

Networking and security have a long and complicated history together, one that could be described as cordial at best or downright hostile at worst. However, this segregated approach is not an acceptable way to operate and often sabotages the gains from digital initiatives. Siloed networking and security infrastructures and operations are quickly disappearing because:

- **Cloud distributed applications and data sit outside of the data center castle.** Not only are cloud, edge, and IoT redefining the location of data and applications, these components of digitalization sent traditional network hub-and-spoke design to meet its maker.[1] Now a businesswide networking fabric interweaves business assets, customers, partners, and digital assets to connect all parts of the business ecosystem (see Figure 1).[2] As the "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" Forrester report calls out, this can only occur if security is embedded within the DNA of the network.
- **COVID-19 pushed employees outside the controls of a corporate LAN moat.** Consider this simple reality: A lot of enterprise applications exist in the cloud today, and this number is only increasing. Users too, have now left the traditional enterprise perimeter; Forrester's pandemic experience survey found that 53% of the newly remote workers wanted to stay remote even after the crisis passes.[3] With both applications and users no longer behind the moat wall, the utility and value of the wall-based security stack has plummeted.

FIGURE 1 The Dispersion Of Applications And Data Across The Business Resources



Historic Security And Networking Approaches Don't Support The Distributed Enterprise

The 2020 pandemic evicted millions of employees from a comfortable shield within the enterprise perimeter who are now cast out into the howling wilderness of remote work. A CISO at a large European-based insurance company told us that, prior to the 2020 pandemic, the company had 5% remote work. The pandemic flipped the ratio, and home workers now make up 95% of the employee base. For companies like theirs, the already rickety VPN infrastructure could not carry the load. VPN technology is just another fissure in the already eroding castle walls. Both networking and security teams have struggled to meet new requirements for using cloud and supporting home workers, because the old approaches were based on:

- **Onsite dedicated software or hardware appliances.** Gone are the days of introducing a specific type of solution to solve a particular technology issue. Thirty years of attaching devices to the network — such as WAN optimizers or firewalls — introduced more security issues, higher levels of complexity, less flexibility, and lower efficiencies. Every new device exponentially expands complexity and potential security issues.
- **Unreliable on-premises controls and policy repositories.** Onsite management software needs dedicated hardware and personnel to keep the software up-to-date with the latest features, bug fixes, and security enhancements. Management software that resides within a private infrastructure not only costs the company more but hampers resiliency capabilities. The software was typically not built to be relocated to cloud platforms, which limits the effectiveness and options for disaster recovery.
- **Limiting hardware-centric approach.** Aircraft, cars, and trains have fit and form restrictions due to weight or size constraints. Even without those restraints, technology teams can't expect to introduce hardware in every part of the manufacturing site, retail store, or stadium. It's impractical to assume hardware can be created to meet fit, form, and function needed between plastics extruder and heating chamber or survive the temperatures equipment must operate in locations such as a Dubai electrical substation or a Death Valley cellular tower.
- **Disjointed security and networking silos.** The practice of relegating certain types of hardware and operations to certain groups only increases operational inefficiencies, decreases infrastructure resiliency, and potentially opens up new security issues. Many discrete devices, such as firewalls and routers, could be combined to reduce latency by using one table to look up rules for packets and applying both security and networking policies at the port.

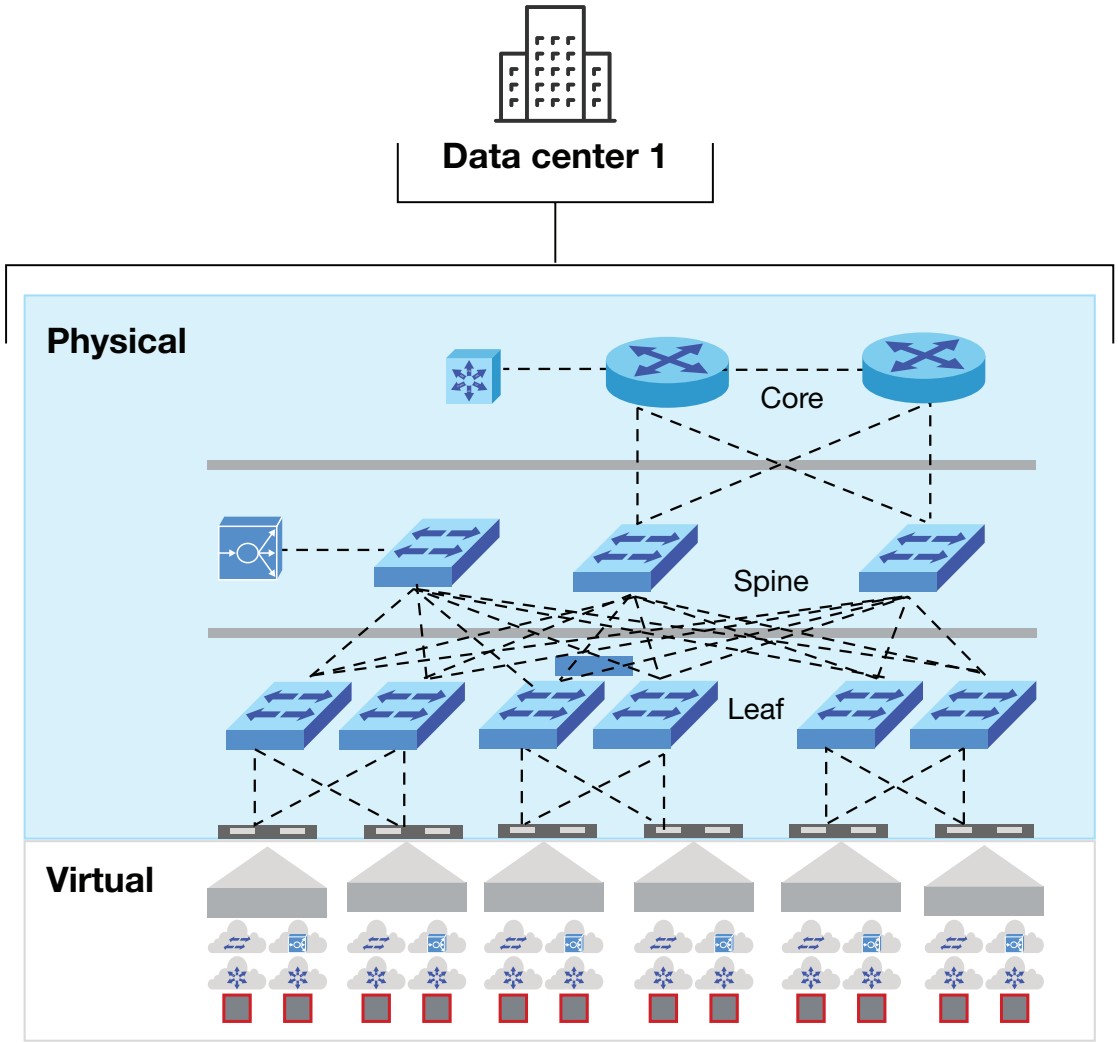
Emergence Of Zero Trust Edge

When COVID-19 forced employees to work from home, a forward-looking minority of security professionals, who felt VPN technology wasn't the best path, invested in Zero Trust network access (ZTNA) solutions to circumvent the issues with VPNs; some of those that went down the ZTNA path

asked if there were other ZT approaches they could adopt since many security and I&O professionals perceived Zero Trust as mainly a data center concept (see Figure 2).[4] However, the security framework laid out in Forrester's "The Zero Trust eXtended (ZTX) Ecosystem" shows how ZT is more than a data center concept. ZT protects businesses from customers, employees, contractors, and devices at remote sites connecting through WAN fabrics to a more caustic, open, dangerous, and turbulent environment (see Figure 3). Forrester sees this concept as Zero Trust edge (ZTE) and defines it as:

> *A Zero Trust edge solution securely connects and transports traffic, using Zero Trust access principles, in and out of remote sites leveraging mostly cloud-based security and networking services.*

FIGURE 2 Earlier ZT Adopters Associated Security Microperimeters To Only Be Around VMs



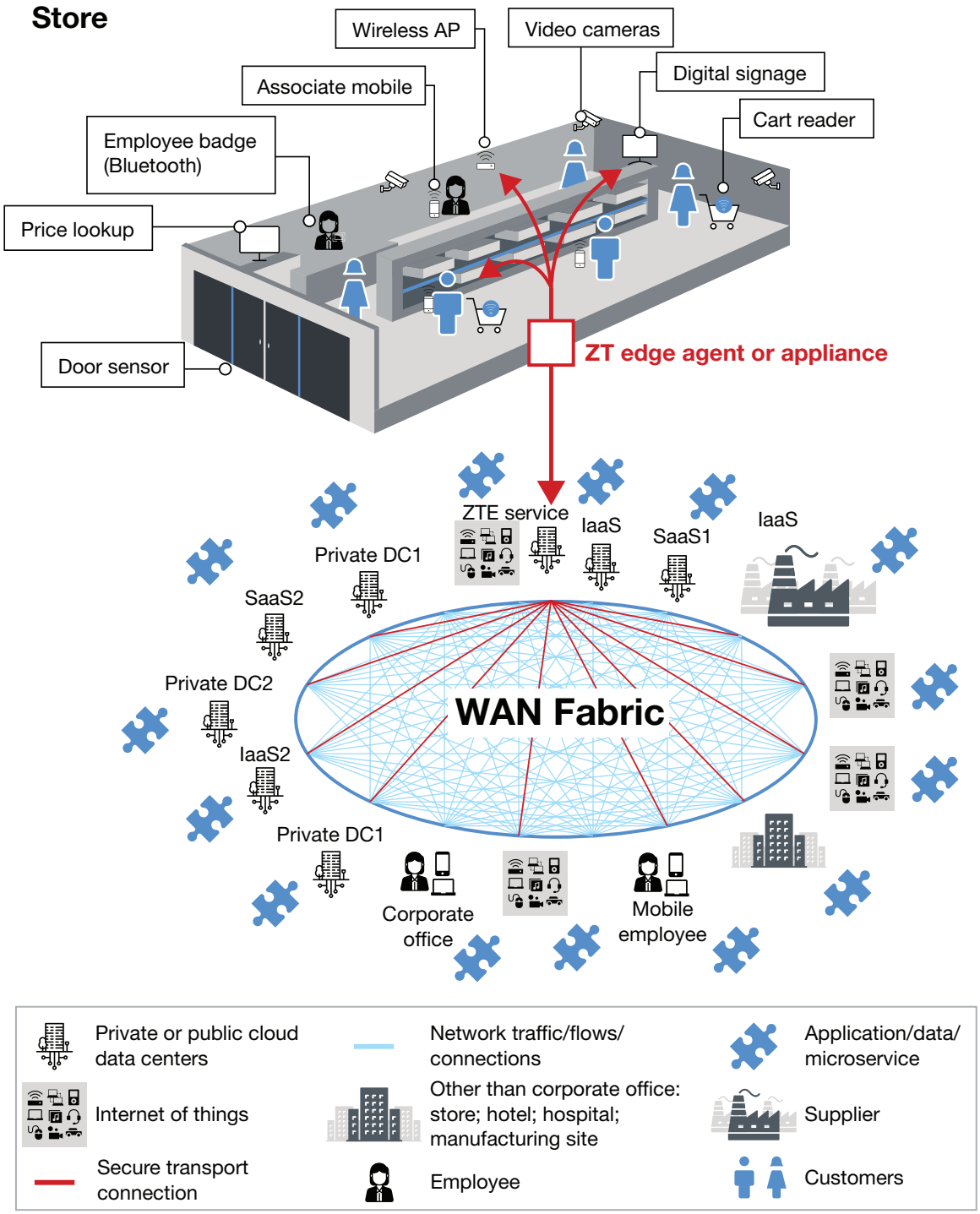
Virtual services

- Virtual machine
- Virtual security appliance
- Virtual switch
- Virtual router
- Hypervisor

Physical infrastructure

- Switch
- Advance network service (segmentation gateway, load balancer, and other services)
- Server
- Network component (router gateway)
- Security controls

FIGURE 3 ZTE Provides The Security Controls And Networking Policies To Secure All Connections Onsite



Surprise! ZTE Starts In The Cloud

ZTE sets up the security and networking framework around the traffic and services coming from remote locations into the businesses and the services going back to the locations or users. While ZTE addresses the distributed enterprise, the solutions, delivering on a faster and more agile set of services, have to be built on two fundamental elements:

- **Cloud-based network and security management.** Historically, device configurations and security policies existed in different tools. For example, network access controls would have security policies for users while management solutions for firewalls and networking components would contain the device configurations. This increases the amount of configuration errors and reduces operational efficiencies as personnel set up similar policies across multiple systems. Cloud management allows these disparate back-end systems to be merged, and configurations can be altered, added, or deleted based on a single configuration management solution.
- **Cloud-based monitoring and analysis.** Networking and security monitoring are typically independent of each other and fundamental requirements of existence of ZTE. Google is a good example — it uses its software-defined WAN to drive utilization on links up to 100%. Monitoring identifies irregularities in traffic — often security issues — all the way out to the peering metros and far from the company data centers.[5] The amount of information that needs to be collected and synthesized forces ZTE monitoring to be cloud based. It needs such an extensive compute platform to obtain the full scope of analysis.

Use ZTE To Deploy 18 Security And Networking Services

From anywhere in the world, organizations can centrally manage, monitor, and analyze the set of security and networking services that reside within ZTE solutions (see Figure 4). Some of the services will remain exclusively located in the cloud (or cloud-edge), and others will need to be hosted in the remote location.

FIGURE 4 Type Of Services Available Within A ZTE Solution

Network

Bandwidth guarantee	Sets a minimal amount of bandwidth for particular traffic
Content caching	Provides localized copies of data
Link balancing and utilization	Leverages multiple links simultaneously to increase traffic bandwidth and overall WAN utilization
Quality of service	Prioritizes network traffic
Resiliency	Delivers and maintains an acceptable level of service in the face of faults and challenges to normal operation.
Routing/best path	Selects the right path for layer 3 transport even from the remote worker to a cloud-hosted application
Software-defined WAN (SD-WAN)	Chooses the best paths, links, or connections based on higher level metrics, such as jitter, dropped packets, and affinity to an application profile
WAN connection	Establishes the physical connection to/from a facility
WAN optimization	Provides deduplication, packet coalescing, and other WAN optimization features

FIGURE 4 Type Of Services Available Within A ZTE Solution (Cont.)

Security

Basic firewall	Offers simple network firewall capabilities (layer 3 and 4 rules) that can be split off and moved locally to reduce the amount of traffic exiting the remote facility
Cloud access security broker (CASB)	Controls and reports on cloud application access
Firewall as a service (FWaaS)	Provides cloud-based advanced firewall features and functions
Intrusion detection system/intrusion prevention system (IDS/IPS)	Analyzes network traffic based on signatures to detect and deflect specific malicious content
Link encryption	Encrypts and decrypts all network traffic at each network routing point
Identity and access management (IAM)	Ensures that the proper people in an enterprise have the appropriate access to technology resources
Secure web gateway (SWG)	Prevents unsecured traffic from entering an internal network of an organization. URL filters must be constantly updated, and the trend was already to have these configured, hosted, and maintained in the cloud
Advanced malware analysis	Runs programs in a secluded environment (sandboxing) to screen and contain zero-day malware types
Zero Trust network access (ZTNA)	Enables the remote worker to connect to enterprise applications based on their identity regardless of where the workers or the applications reside. It is the signature security service that must exist in the ZTE.

Use Cases Will Dictate The Types And Locations Of ZTE Services

Network and security architects must ensure maximum utility as they are drawn into the Zero Trust edge. The types of services being used depend on the location, devices, people, and other elements (see Figure 5). Three use cases show increasing levels of forcing functions (which means an increased amount of networking and security services that get turned on within the ZTE solution):

- **Secure remote workers as the initial use case.** The 2020 pandemic and its ensuing mass exodus has punted millions of knowledge workers from the office to working from home. Providing secure access to corporate services and applications for these homeworkers is the initial use case bringing organizations into the Zero Trust edge. Due to many of the challenges outlined in Forrester's research, "Key Considerations For Network And Capacity Management When

Operationalizing A Home-Based Workforce," most companies forgo placing any type of networking software or hardware inside the home. Instead, software agents are deployed on the workers' work devices, and their connections are linked to cloud-edge security services (see Figure 6).

- **Prioritize business application traffic that dominates the branch WAN.** The number of WAN connections has exploded due to home workers. Still, remote office connections have been the bulk of WAN traffic for an enterprise, mostly coming from employees, their applications, and business-owned devices. SaaS traffic, such as O365, has recently become a major factor, and it may also contain some customer traffic. SaaS-based application traffic needs straight-to-internet connections, and customers may need to connect to remote office LANs. To deal with these challenges, enterprise architects are increasingly directing this traffic through firewall as a service (FWaaS). This is either done through remote office routers and/or SD-WAN solutions highlighted in the "Now Tech: Software-Defined WAN Hardware/Software, Q3 2020" Forrester report or from a service provider listed in the "Now Tech: Software-Defined WAN Services, Q3 2020" Forrester report (see Figure 7). Some vendors, like Forcepoint, support SD-WAN functionality integrated with multiple security services.
- **Finally, secure the internet of all the things.** In addition to home workers and generic branch offices, IoT and edge devices and business partners are riding the network. The industrial control system (ICS) architect will have to onboard related locations that force increased attention to security and network policies. For example, an engineer at an automobile manufacturing facility considers traffic from employees and contractors but must also account for traffic from Siemen's programmable logic controllers (PLCs) or Bosch's inventory control shelf weights. Due to the location and lack of bandwidth available to the site, some basic security elements have to be hosted onsite, along with all the networking services, to decrease the amount of traffic steered to cloud security services (see Figure 8).

FIGURE 5 Each Case Has A Different Set Of Security And Networking Factors To Consider

	Remote work	Small office	Hetero site
Assets	Laptop	Desktops, printers, conference rooms, webcams	Heterogenous physical network
Gateway to ZTE	Endpoint agent	WAN device with required onsite network services or overlay via agent	WAN device with required onsite network services
IoT	No	Low	High
Edge compute	No	Low	High
Contractors	No	No	Yes
Business and technology vendors	No	Low	High

FIGURE 6 Home Workers Benefit From ZTE Cloud-Based Security Services

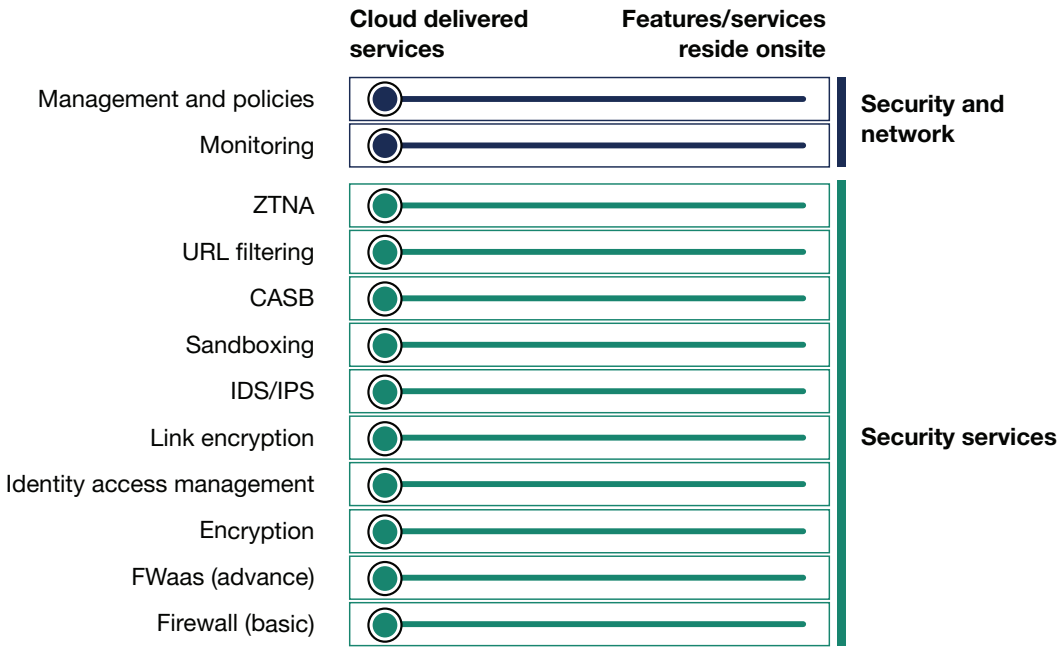


FIGURE 7 Generic Business Offices Steer Traffic To Cloud-Based Security Services

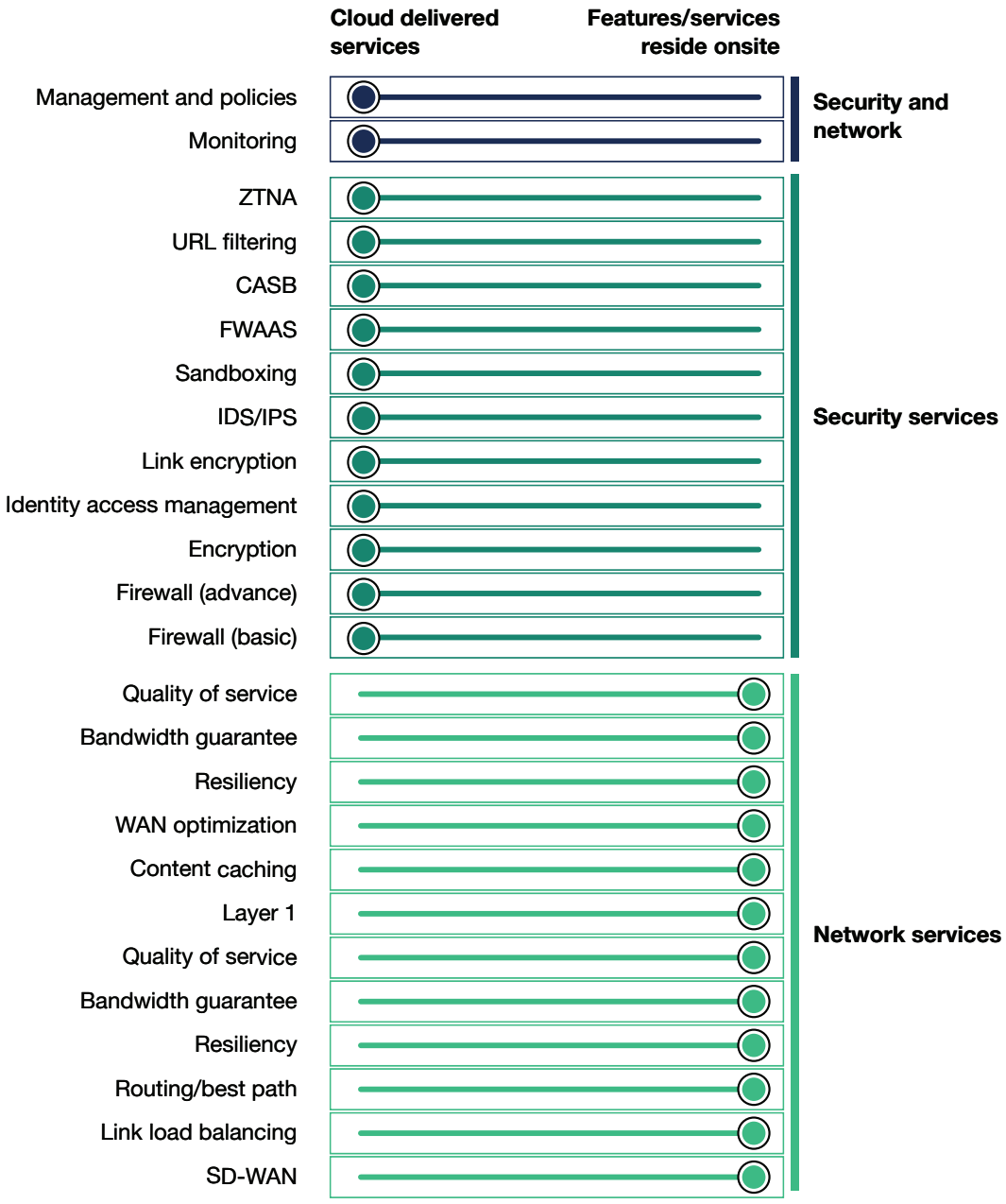
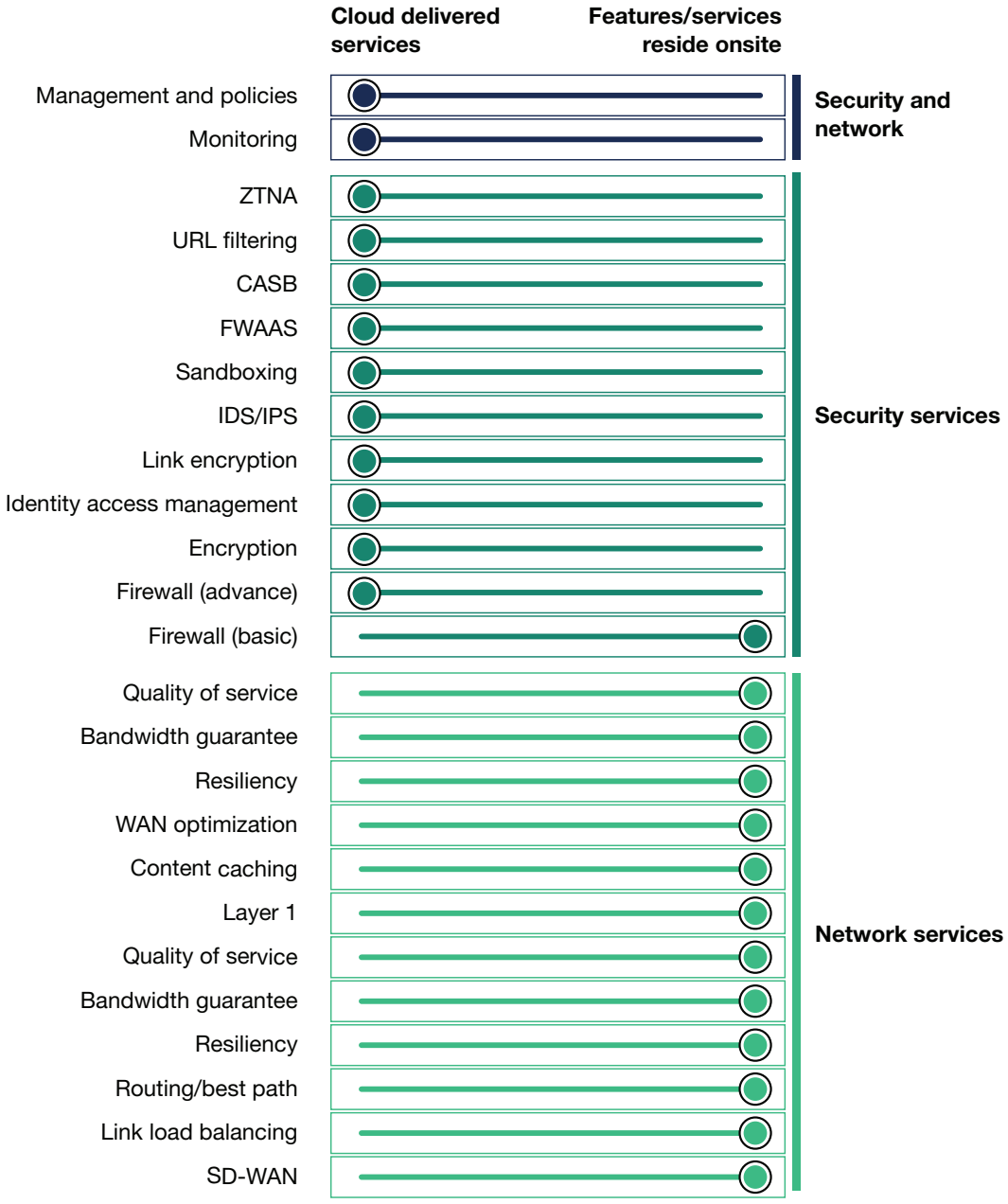


FIGURE 8 Complex Sites With Limited WAN Bandwidth Force Some Localized Security Capabilities



The Market Offers Different Types Of ZTE Choices

Technology professionals can leverage ZTE from three different methods:

- **A cloud-delivered service.** A relatively new set of vendors, ZTE cloud-based services come from a vendor-run service like Cato Networks, using a third-party network with dozens — or in some case hundreds — of POPs delivering cloud-edge ZTE capabilities. This approach offers all the value that organizations can get from software-as-a-service solutions. However, no company can provide all the features found in best-of-breeds solutions. Of course, Forrester has found that organizations don't normally use all the features found in on-premises solutions. Cloud solutions will often fit the needs of many organizations.
- **ZTE services wrapped around a WAN connection service.** Others will include an existing enterprise carrier provider connecting its customers directly to ZTE networks for outsourced security functions. Comcast Enterprise and Akamai already perform this function today. Many SD-WAN hardware and software vendors, such as Versa Networks, will have partnerships with Zscaler or other security vendors. Teams can choose the best-of-breed products to ensure they get the most from both networking and security services. However, these teams won't get the operational agility or efficiency of cloud-based systems. An SD-WAN plus ZTE wrapper approach requires extra steps from technology teams such as setting up policies for each independent services. There isn't a single management and orchestration system for an SD-WAN and ZTE wrapper strategy.
- **A do-it-yourself (DIY) approach.** A sufficiently large and agile organization could build its own ZTE platform using cloud service providers as the POPs and a cloud-hosted service like Barracuda's enterprise firewall as the security service in Microsoft's Azure cloud. This ensures services match the business demands more closely, but it requires that teams have the good pulse on business requirements and the skills to create the infrastructure and manage it. Forrester's "Evaluate SD-WAN Services Based On Branch Office Goals, Not Hardware Data Sheets" report shows that most teams are missing one or the other aspects.

Both Multivendor And Single-Vendor Stacks Have Their Place

ZTE represents an existential threat to many on-premises security solutions, so a ZTE strategy is now critical for these vendors. Ambitious vendors would like to sell you the entire turnkey package (when they have it), and the idea of having a single vendor for all security solutions on an opex basis will be compelling for the SMB/midmarket. Your own choice depends on your firm's size and complexity, as:

- **Larger organizations will opt for a multivendor approach in the short term.** Larger enterprises have more complicated requirements and more heterogeneous services. A heavier burden of legacy applications makes them less likely to adopt a single-vendor approach. Interviewees for this research were in broad agreement on this analysis. For the organizations that have already started on a Zero Trust edge journey, a typical multivendor approach may use Silver Peak Systems for SD-WAN connecting to Zscaler for URL filtering and ZTNA. This will work for the initial use case

(securing remote workers), but the migration of other security stack elements into a multivendor stack will require serious service chaining, and the APIs between the components need to work consistently and reliably.

- **Smaller organizations will pioneer the full security stack approach.** Forrester expects to see smaller companies try out full stack ZTE vendors, such as Netskope. Typically they will have a lower set of requirements and may find the one-shop vendor easier to engage. Historically, it takes larger enterprise technology groups time to adopt those types of solutions. For example, this has occurred in the Wi-Fi market with cloud-based solutions from Aerohive Networks, now part of Extreme Networks, and Meraki, now part of Cisco.

Complexity Also Determines Whether You Use An Agent Overlay Or Agentless Gateway

Connecting all users and applications is the aspirational end state for the Zero Trust edge, whether systems are on-premises, in the cloud, in a private cloud, or working remotely. However, connecting a complex, heterogeneous network is clearly a nontrivial endeavor. Therefore, the market currently supports two kinds of deployments, one to support the strategic end state and one to support a tactical entry into the Zero Trust edge. Some vendors, like Zscaler, can support both models simultaneously, and more vendors are moving to do the same.

- **Model one: A gateway is a single point of security.** This model becomes your singular entry point to the internet. Think of an SD-WAN controller with a GRE tunnel to a vendor-hosted edge network. All outbound traffic then goes to the edge network, which can then immediately assign security policies to that tenant's traffic in their network. The origin's threat surface shrinks dramatically, making attacks like DDoS someone else's problem. This option, while cleaner, is more likely to be adopted in the midmarket; it may not be possible for complicated heterogeneous environments in the short term.
- **Model two: An overlay distributes security, usually via agents.** In this model, endpoints connect to the edge network via an overlay, typically facilitated by an endpoint agent that determines which connections get rerouted to the ZTE network. The overlay model can be implemented without changing the underlying network, but a significant drawback is that installing agents may not be feasible due to policies in sensitive environments like healthcare, manufacturing, and IT/OT. Axis Security has an innovative approach that ultimately uses the overlay model without requiring agents on devices that want to join the network. We interviewed one significant customer that chose the Axis Security solution for exactly this reason.

Obstacles On The Road To The Zero Trust Edge

The Zero Trust edge model is disruptive — nay, transformative — to the way security and networking have traditionally been consumed. Always in a constant state of evolution, cybersecurity functions have been quicker to move to the Zero Trust edge. Legacy networks will be much slower. Companies are getting pulled into the Zero Trust edge by proxy of the remote worker security problem, but significant challenges lie ahead to achieve the full promise of the model, including:

- **Legacy applications and services.** Modern web applications understand identity federation, making them (relatively) easy to configure in a ZTE. However, applications based on nonweb protocols, especially RDP/VDI and SIP/VoIP, will not be so easy. Even these two very common types of applications suffer from the lack of a standardized way to be consumed in ZTE environment.
- **Legacy networking apparatus.** Once the laptops, servers, and applications are joined to the Zero Trust edge, the architect will have to consider the thousands — and in some cases hundreds of thousands — of OT and IoT devices on which no agent software can be installed. These must join en masse, using accepted networking protocols, and it is here that security and networking teams will have to cooperate.
- **Capacity and trust.** Organizations can use ZTE to tactically solve problems like secure access for remote workers, but they aren't ready yet to replace high-capacity network and security services that front their existing data centers. Organizations with heavy existing investments in their own data centers will wait until a larger effort — like a cloud migration of their critical applications — before they transition those services to Zero Trust edge protection.

What It Means

Security And Networking Finally Combine Against A Common Enemy

With security being embedded into the network and becoming part of its DNA, Forrester sees the following happening to the two organizations:

1. **Security organizations setting the security policies and test.** The types of traffic and the services needed to meet acceptable trust levels will be set by the security team. With monitoring and analysis tools, the teams will ensure policies are being followed and they will routinely test and audit the traffic and connections — together.
2. **Networking after security.** Networking professionals will be executing through ZTE policies set up by the security team. While this arrangement significantly advances the ideology of Zero Trust, it is a reversal of the past 25 years of security overlaying networking.

3. **Finally, a safer internet on-ramp.** When asked, the designers of the original internet will freely admit that security was never part of its design. In the 30 years since its inception, the global internet has become a dangerous network to cross. Zero Trust edge finally provides a safer path through it.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

419 Consulting
Akamai
AT&T
Axis Security
Barracuda
BlackBerry

Cato Networks
Cisco Systems
Citrix
Deutsche Telekom
Edelweiss Financial Services
Famous Supply
Fortinet
Infoblox
IronNet
Jefferies
Juniper
Lightstream
Marriott Vacations Worldwide
Menlo Security
Mentor Graphics
Netskope
Nuspire
Palo Alto Networks
Silver Peak
SKF
VMware
Windstream
Zentera Systems
Zscaler

Endnotes

[1] A private data center is the hub of data, applications, and security with remote locations; restaurants, acute care centers, manufacturing sites, to name a few, connect to the hub for all company resources.

[2] See the Forrester report "Emerging Technology Spotlight: Businesswide Networking Fabric."

In a networked business model, the ecosystem's members cocreate customer value in a distributed manner. See the Forrester report "Customer-Obsessed Businesses Need Digital Ecosystems."

[3] Our pandemic experience (PandemicEX) surveys asked respondents, "How much is your company/organization taking these steps to manage the risk associated with the coronavirus?" Source: Forrester's Q1 2020 US PandemicEX Survey 1 (March 3 to March 6, 2020); Forrester's Q1 2020 US PandemicEX Survey 2 (March 17 to March 19, 2020); and Forrester's Q2 2020 US PandemicEX Survey 1 (April 1 to April 3, 2020).

See the Forrester report "The State Of Remote Work, 2020."

[4] Marketing materials from vendors in the early days of ZT only highlighted solutions for the private data center. For example, Palo Alto highlighted in various whitepapers how ZT can protect data center assets. Source: "Best Practices - Data Center Security," Palo Alto Networks, June 1, 2016 (https://www.paloaltonetworks.com/resources/whitepapers/best-practices-data-center-security).

[5] Source: Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jonathan Zolla, Urs Hölzle, Stephen Stuart, and Amin Vahdat, "B4: Experience with a Globally-Deployed Software Defined WAN," Proceedings of the ACM SIGCOMM 2013 Conference, August 2013 (https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41761.pdf).

FORRESTER®

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.