



Merger and acquisitions (M&A) and divestitures secure access service edge (SASE) enablement approach

Deloitte’s joint offering with leading cybersecurity technology company, Palo Alto Networks, provides an integrated approach to addressing cyber risks.

We help clients solve challenges leveraging Zero Trust Network Access (ZTNA) principles with SASE capabilities via advise, implement, and operate to enable a cost-effective transition to operate.

The reality of our client’s challenges during M&A

The nature and speed of M&A activities can expose the participating organizations to a multitude of information and technology security threats and vulnerabilities

- Insider threats**  
Child company extracting mission-critical and sensitive data prior to a workforce reduction

**Visibility gap**  
Overly exposed sensitive data sharing to external resources by the child company
- Inherited vulnerabilities**  
Acquiring parent company is exposed to legacy assets from the child company

**Sensitive timeline**  
M&A timelines are aggressive and there is very little time to stand up new infrastructure
- Over access commitment**  
Expanding application scope for insider threat and foreign nationals to inspect












We provide outcomes that can help your business to adapt efficiently

Integrating in weeks versus months leveraging ZTNA

Expedites go-to-market value with today’s modern workplace

Deloitte and Palo Alto Networks’ joint offerings and capabilities

ADVISE. IMPLEMENT. OPERATE.

	 <b>ZTNA</b>	 <b>SWG</b> Secure Web Gateway	 <b>CASB</b> Cloud Access Security Broker	 <b>SD-WAN</b> Software Define Wide Area Network	 <b>Managed SASE</b>
<b>Description</b>	Establish and accelerate secure remote access to applications, data, and services through a distinct blend of industry cyber technology platforms and professional services	Enhance web content inspection, enforcing security and compliance, while mitigating malicious websites and application security threats/exposure	Monitor and evaluate Software as a Service (SaaS) application consumptions, enforce Data loss prevention (DLP) policies, threat prevention, data protection, and governance	Securely connect users to applications, leveraging a variety of transportation services, establish connectivity and protection to users	
<b>Palo Alto Networks product alignment</b>	 	 			
<b>Outcome</b>	The expanded adoption of Zero Trust principles and SASE capabilities can help enhance overall security posture.	Established artifacts to fast-track onboarding, promote time to value, reduce cost, and promote high-performing, security enhancements	Removing complexity and Increased agility and productivity for a remote workforce, partners, and contractors	Experienced security professionals providing converged network and Security as a service to help meet your compliance requirements	

We’re well-positioned to help you achieve your objectives

Outcome-driven

In the face of growing complexity, we make finding a cyber & strategic risk provider easy.

Our breadth and depth allows us to provide the outcomes (and value) you seek in a trusted advisor, a technology-savvy pioneer, a visionary integrator, and a dependable operator.

We connect the dots, so you don’t have to – helping you to improve security, trust, and resilience.

Quality-oriented

We bring together a powerful combination of accelerators to expedite the onboarding process, domain experience, leading alliances, and industry knowledge. Our focus on quality means we consistently work to help you realize your vision.

Value-focused

We act as a leader in times of crisis, a teammate to help you navigate change, and a force to have your back when you are on the front lines.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

All product names mentioned in this presentation are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest to clients under the rules and regulations of public accounting.

Full acquisition

The client acquired another healthcare organization and needed to efficiently onboard 50,000 global users without standing up new infrastructure-, apply security controls for specific apps and layer data loss prevention and internet security for secure access and roll out SASE to the parent organization of 130,000 users.

How SASE addresses challenges

We helped the client remove the burden of standing up infrastructure by leveraging SASE capabilities via the cloud, leveraging one platform for ZTNA and SWG, onboard US users in weeks and phase out the global workforce from Europe, China, and Russia-, and implementing guardrails leveraging leading security practices.

Joint venture

SASE can help with joint ventures by providing a more secure connection between the two partners in the venture, allowing for more effective communication and collaboration-, as well as more secure access to data and applications enabling employees to access the resources they need.

SASE can also help protect the joint venture from potential cyber threats and attacks providing visibility into the activities of users and devices connected to the network.

Divestiture

SASE can help facilitate divestitures by providing a streamlined and efficient process for decommissioning and migrating applications, services, and data from one environment to another.

It can also automate processes of decommissioning and migrating applications, and services, providing an audit trail of activities for compliance and maintaining traceability throughout the divestiture process and data to decrease time and effort.

Acquisition of a carveout

The client a spinoff from the parent company, required new and secure infrastructure globally for 3,000 remote workforces. The client had three months to become independent from the parent company. The client served ~30,000 customers globally, ranging from small business owners to enterprise treasurers, educational institutions, and law firms, and needed the workforce to onboard efficiently and securely.

How SASE addresses challenges

We helped the client implement and deploy-SASE infrastructure and integrate existing technologies, Identity, Logging, SD-WAN, Cloud Service Providers-, and Datacenter access to applications and services. We also helped the client expedite the onboarding of SASE capabilities via agents and identity integration for remote access.

How we help our clients with an effective transformation

- Provide secure internet access with enhanced protection capabilities not just to employees but also to external personnel like agents and contingent workforce

Avoid backhauling traffic to the corporate network to enforce security controls and to monitor, detect, and take appropriate actions against advanced threats like ransomware attacks

Use a single product with a wide range of security capabilities and provides a unified management interface and a single pane of glass for traffic visibility

Protect sensitive data from unauthorized access and data loss as it is being accessed remotely via managed and unmanaged devices

Secure remote access to internal and SaaS applications regardless of the physical location of the user or the client device while keeping them invisible to unauthorized users.

Start the conversation



**Jane Chung**  
Managing Director | Deloitte Cyber  
Deloitte & Touche LLP  
[jchung@deloitte.com](mailto:jchung@deloitte.com)



**Cary Hickerson**  
Sales Executive | Deloitte Cyber  
Deloitte Services LP  
[Chickerson@deloitte.com](mailto:Chickerson@deloitte.com)



**Gary Moreau**  
Solutions Engineer | Deloitte Cyber  
Deloitte Services LP  
[Gmoreau@deloitte.com](mailto:Gmoreau@deloitte.com)



**Lindsey Sherman**  
Alliance Lead | Deloitte Cyber  
Deloitte Services LP  
[Lisherman@deloitte.com](mailto:Lisherman@deloitte.com)