Solution overview

Securing and modernizing networks in manufacturing with unified SASE

Digital transformation initiatives targeting improved efficiency, productivity, reliability, safety, and physical security depend on access to data from Operation Technology (OT) and Industrial Internet of Things (IIoT) devices, as well as contextual information like location and identity from Information Technology (IT) networks. Additionally, the convergence of IT and OT provides enhanced data analytics and better decision-making processes, but it also introduces significant challenges, especially concerning security.

Connecting and protecting disparate devices and applications is no mean feat. Today's distributed enterprises have facilities, remote sites, and people spread far and wide. Applications workloads and real-time data may be processed locally on the factory floor, at a remote data center, in a private cloud, and/or at a cloud service provider. To ensure productivity, these enterprises need a flexible network architecture that can adapt to changing needs with simplified management and an easy way to integrate new locations and devices into the network.

Security has become crucial in manufacturing to protect production, sensitive data, intellectual property, and IoT against cyber threats, but also to demonstrate adherence to industry standards and regulations such as IEC 62443, GDPR and ISO 27000. And securing communications across such a distributed enterprise has become challenging with cloud expansion, the rise of the remote worker and the need for pervasive, always-on connectivity. In this scenario, the traditional network perimeter is not as defined as it used to be, demanding a different or an extra set of controls to the manufacturing defense-in-depth architecture.

Based on these above challenges, let's look at how adopting an advanced SASE (Secure Access Service Edge) solution can help industrial and manufacturing customers tackle these challenges.

HPE Aruba Networking unified SASE for manufacturing facilities

SASE is a transformative framework that combines network security functions with WAN capabilities to support the dynamic, cloud-driven needs of modern manufacturers. The two key components of HPE Aruba Networking's unified SASE are HPE Aruba Networking EdgeConnect SD-WAN and HPE Aruba Networking SSE (Security Service Edge). Together, these components create a holistic approach to security and networking, aligning with the decentralized and mobile nature of today's smart manufacturing organizations. Additionally, a unified approach allows simpler adoption and faster deployment, decreasing payback time.

HPE Aruba Networking's EdgeConnect SD-WAN solutions are engineered to deliver secure, high-availability access to OT, IT, and IIoT traffic over virtually any combination of links, including MPLS, internet, 4G/5G and satcom, improving application performance and providing flexibility to accommodate these dynamic environments and easily onboard new locations. EdgeConnect SD-WAN also supports multi-cloud networking by intelligently steering traffic to the cloud, eliminating the need to backhaul traffic to the data center and optimizing cloud-based traffic. It integrates a next-generation firewall to provide advanced security capabilities in manufacturing sites such as IDS/IPS, DDoS defense and role-based segmentation, going beyond the typical definition of SASE to incorporate IoT security.

HPE Aruba Networking SSE provides key cloud-delivered security capabilities including ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker). ZTNA enables users and authorized third parties to access resources, such as hybrid workers and contractors which must perform remote maintenance. Employees are protected against web-based threats that can make their way into the OT environment with SWG, and sensitive data hosted in SaaS applications is securely monitored to prevent data exfiltration (including product recipes, product design documentation, PII data) with CASB.

The adoption of unified SASE from HPE Aruba Networking offers tangible benefits such as a common Zero Trust foundation that network and security teams can use to drive compliance, unified security, threat defense, data protection, improved application performance, centralized management, and ease of deployment.

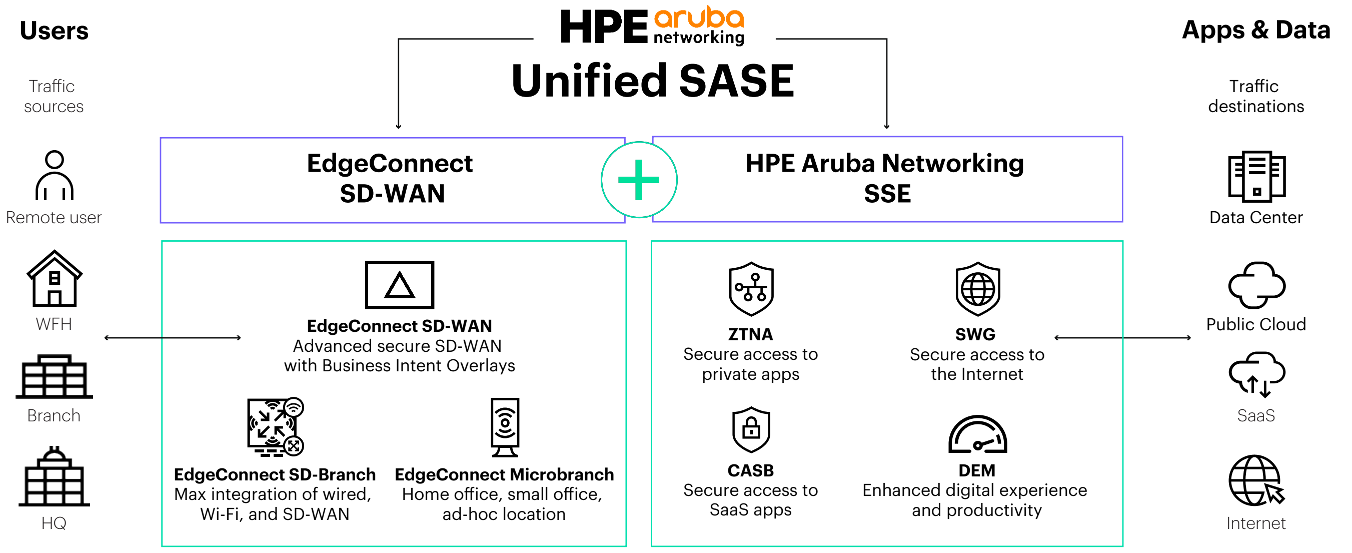
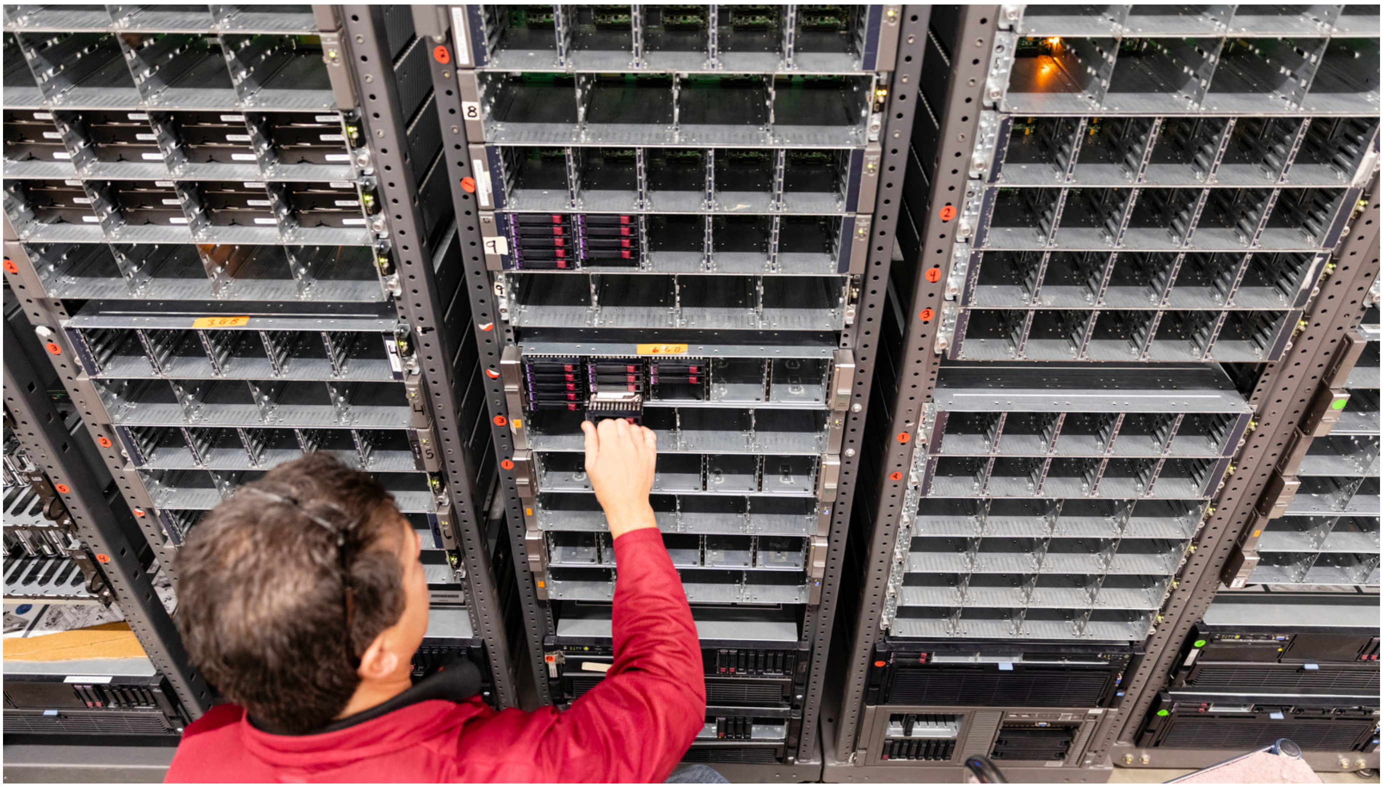

Users
Traffic sources
Remote user
WFH
Branch
HQ
HPE aruba networking
Unified SASE
EdgeConnect SD-WAN
HPE Aruba Networking SSE
EdgeConnect SD-WAN
Advanced secure SD-WAN with Business Intent Overlays
EdgeConnect SD-Branch
Max integration of wired, Wi-Fi, and SD-WAN
EdgeConnect Microbranch
Home office, small office, ad-hoc location
ZTNA
Secure access to private apps
SWG
Secure access to the Internet
CASB
Secure access to SaaS apps
DEM
Enhanced digital experience and productivity
Apps & Data
Traffic destinations
Data Center
Public Cloud
SaaS
Internet

Figure 1. Implement unified SASE in manufacturing with HPE Aruba Networking



Advanced security

As manufacturing organizations are moving to a cloud-centric architecture, where many applications in the Purdue model's layers 3 to 5 reside in the cloud and the demand for hybrid work environment increases, security must evolve in parallel to prevent disruptions in services and production. HPE Aruba Networking SSE integrates multiple security functionalities such as ZTNA, SWG and CASB to ensure a consistent security posture.

— **ZTNA (Zero Trust Network Access)** is based on the principle to "never trust, always verify", so that a subject connecting to the network is not trusted by default. It enables manufacturing enterprises to replace legacy VPN solutions that can be prone to known vulnerabilities. In addition to that, VPNs often do not deliver the experience that manufacturers require to perform time-sensitive operations. With ZTNA, user access is limited to only specific applications or microsegments that have been approved for the user, enforcing least-privilege access. With ZTNA, remote workers can connect from anywhere. Third-party users can also be easily onboarded in the network with agentless ZTNA.

— **SWG (Secure Web Gateway)** sits between a user and a website to secure and protect against malicious threats. It performs several security inspections including URL filtering, malicious code detection and web access control, and provides policies that can limit access to adult sites, gambling, dangerous sites, among others. Manufacturing has been severely affected by ransomware in the past few years and SWG plays a key role in mitigating this risk.

— **CASB (Cloud Access Security Broker)** ensures sensitive data hosted in SaaS applications like ERP and CRM remains protected. It identifies and detects sensitive data in cloud applications and uncovers shadow IT. It monitors user activities in cloud services, identifies potential security risks and policy violations to prevent data loss, while controlling uploads and downloads of SaaS applications.

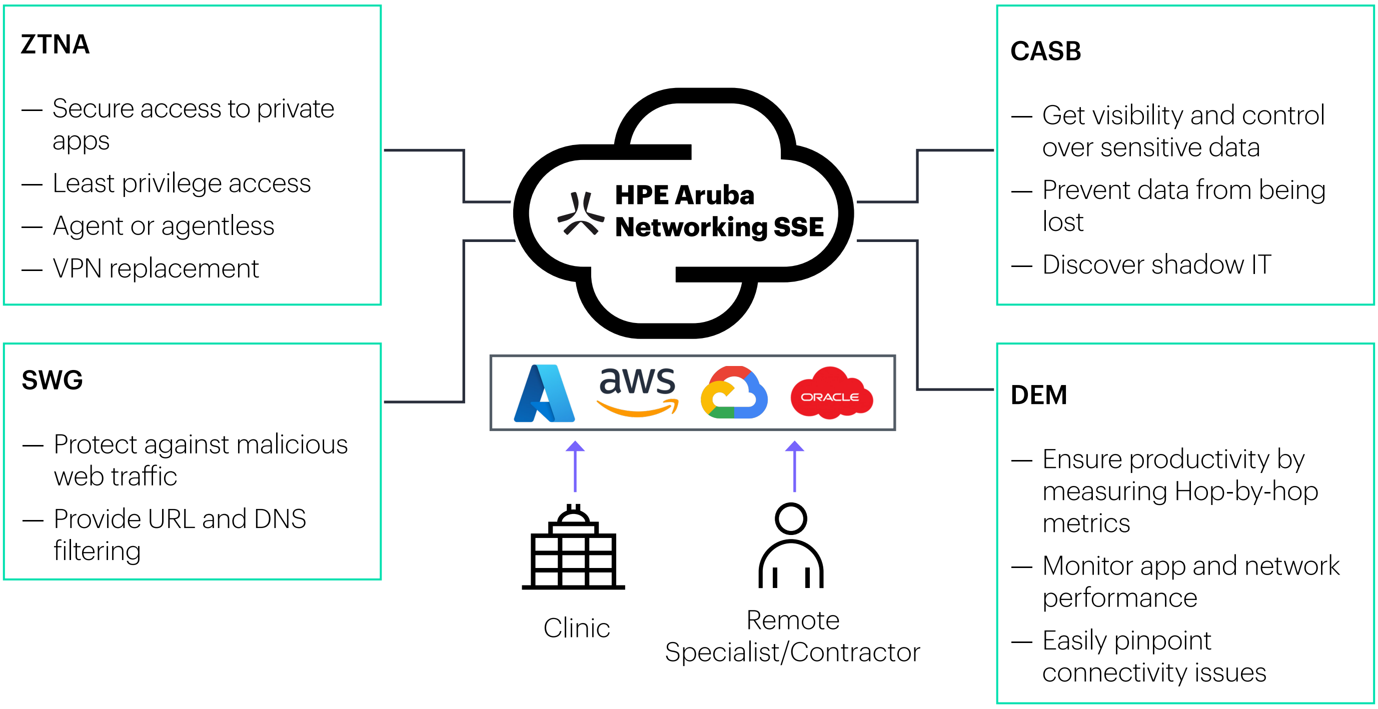

ZTNA
— Secure access to private apps
— Least privilege access
— Agent or agentless
— VPN replacement
SWG
— Protect against malicious web traffic
— Provide URL and DNS filtering
HPE Aruba Networking SSE
aws
ORACLE
Clinic
Remote Specialist/Contractor
CASB
— Get visibility and control over sensitive data
— Prevent data from being lost
— Discover shadow IT
DEM
— Ensure productivity by measuring Hop-by-hop metrics
— Monitor app and network performance
— Easily pinpoint connectivity issues

Figure 2. Secure access in manufacturing with HPE Aruba Networking SSE

To improve security in manufacturing sites, EdgeConnect SD-WAN's embedded, next-generation firewall extends Zero Trust segmentation from edge to cloud, protecting IT, OT, and IIoT devices, applications, and users. Segmentation is the number one control to orchestrate IT and OT traffic in a very heterogeneous manufacturing environment with assets from various vintages, including legacy proprietary protocols. By segmenting the network based on role and identity, users and devices can only connect to their target destinations and applications consistent with policy settings.

When traffic is sent over the Internet, EdgeConnect First-packet iQ™ identifies and classifies applications on the first packet transmitted. This secure Internet breakout feature automates traffic steering to the correct destination based on defined security policies. For example, trusted cloud application traffic such as UCaaS (video conferencing) can be sent directly to the Internet. Other Internet-bound traffic—ERP, CRM, Data Warehousing and Historians—might be redirected to HPE Aruba Networking SSE, or other third-party SSE solution. Untrusted applications can be backhauled to the enterprise data center for further security inspection.

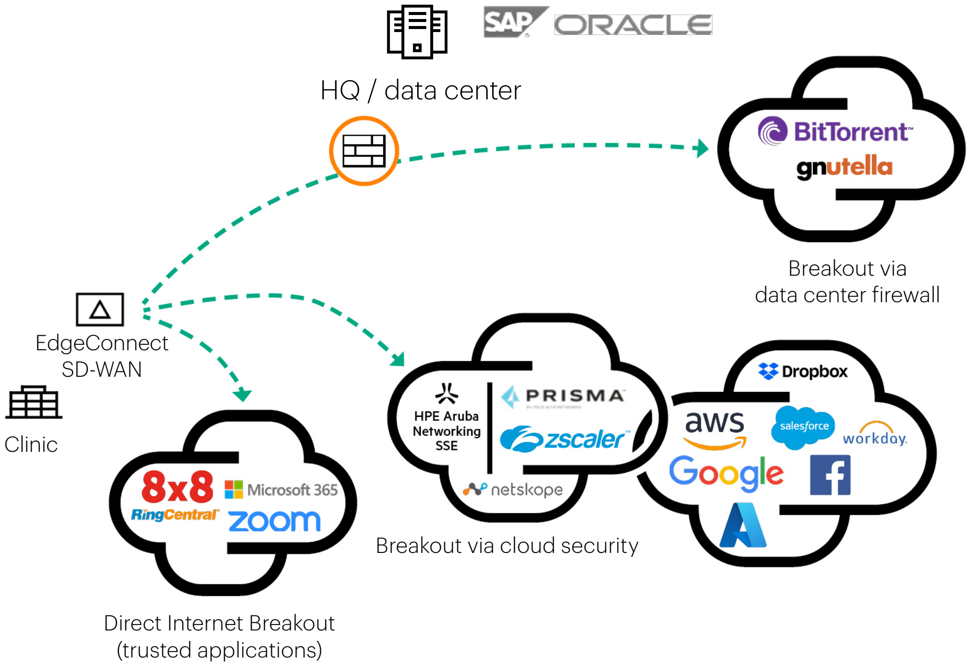


Figure 3. Securely breakout internet traffic based on first packet identification with EdgeConnect SD-WAN

Enhanced network experience

EdgeConnect SD-WAN tunnel bonding combines multiple WAN transport services—including MPLS, Internet broadband, satcom, and 5G—to create a single, higher-bandwidth logical link. Tunnel bonding enables low-cost Internet broadband, where its use is permitted, to deliver equal or better performance as expensive and complex MPLS. The challenge with Internet and cellular links is that they are more prone to packet loss, jitter, and outages which in a normal scenario could impact services that require a more deterministic performance in the manufacturing technology stack, such as video transmission or real-time process monitoring.

EdgeConnect SD-WAN Forward Error Correction (FEC) feature automatically reconstructs lost packets, while Packet Order Correction (POC) re-orders any packets that arrive out of sequence at their destination when load-balancing traffic across multiple WAN transport services. Slow links are addressed by the WAN Optimization option which applies TCP protocol acceleration, data deduplication, and compression to speed traffic flow. AppExpress optimizes user experience over multi-cloud networking for business-critical applications by exploiting SD-WAN path diversity and automatically selecting the best path for each application. Digital Experience Monitoring (DEM), part of HPE Aruba Networking SSE, ensures user productivity by measuring metrics, and monitoring app, device, and network performance over the internet.

Simple deployments

The unified SASE solution from HPE Aruba Networking is easy to deploy and accelerates SASE adoption. The platform offers centralized management to monitor and control the entire network infrastructure. This simplifies policy enforcement, monitoring, and troubleshooting. Centralized management includes remote set-up and diagnostics, eliminating the need for local specialized IT staff. This is particularly relevant in the current scenario of skill shortage in manufacturing where many sites don't have a dedicated (or just a limited) IT staff.

HPE Aruba Networking SSE is a unified platform where ZTNA, SWG and CASB share a single codebase. All policies are managed from a single user interface, making access control incredibly simple for IT admins. EdgeConnect SD-WAN integrates in one gateway a WAN optimizer, router, and firewall, eliminating the need for three separate appliances.

Summary

The unified SASE solution from HPE Aruba Networking enables manufacturing enterprises to fortify their cybersecurity defenses, optimize operations, and adapt to the evolving demands of the digital era. It delivers secure, high-availability access to OT, IT, and IIoT traffic over virtually any WAN pathway and enables secure remote access. New sites and devices can be easily integrated without compromising security or performance. Additionally, centralized management facilitates operations, increases visibility, and enables IT administrators to centrally orchestrate network and security policies. With this solution, manufacturing enterprises can improve adherence to standards and regulatory mandates.

Table 1. Key features and benefits

Enforce Zero Trust access, improve security and compliance	
Security Service Edge (SSE)	HPE Aruba Networking SSE provides key security components including ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker).
Support for remote work	Enable secure access to manufacturing applications and data from remote locations. Replace slow and unsecure legacy VPN with ZTNA.
Micro-segment IT, OT, and IIoT devices	Segment traffic based on role and identity into subnetworks, limiting the spread of cyberattacks and malware in manufacturing sites and reducing the attack surface.
Advanced firewall	EdgeConnect SD-WAN next-generation firewall features deep packet inspection, intrusion detection and prevention (IDS/IPS) and DDoS defense to control incoming traffic, and monitor, flag and drop threatening traffic, enabling manufacturing sites to replace legacy firewalls.

Provide an advanced connectivity experience	
Higher performance and cost reduction	EdgeConnect SD-WAN simultaneously bonds MPLS, Internet, satcom or cellular links for higher performance and lower operating costs. Additionally, by consolidating network and security functions, SASE potentially reduces infrastructure costs.
Network optimization	Overcome the latency effects of WAN by compressing and deduplicating data with WAN optimization. Mitigate the effects of Internet and wireless links that often suffer from packet loss and jitter with Forward Error Correction (FEC).
AppExpress	Optimize user experience by exploiting SD-WAN path diversity and automatically selecting the best path for each application across the web.
Multi-cloud networking	Provide end-to-end connectivity with public clouds and private clouds without the need to backhauling traffic to a data center.
Digital Experience Monitoring (DEM)	Give enhanced, in-line visibility and analysis into the interactions, experience, and performance of devices, applications, and networks.

Easily deploy new locations and monitor network activity	
Faster deployments	Centralized management and remote diagnostics speed deployments without specialized IT personnel. Seamlessly integrate new locations and remote sites without compromising security or performance.
Full visibility	Advanced dashboards provide an aggregated view of network health and security based on configured thresholds and alerts.
Policy enforcement	HPE Aruba Networking SSE provides a single policy engine to configure ZTNA, SWG and CASB policies in a single interface. EdgeConnect SD-WAN centrally orchestrates security and networking policies facilitating the deployment and management of the solution.

Additional resources

Designing Hyperaware Industrial Facilities

HPE Aruba Networking ESP in Industrial & Manufacturing

HPE Aruba Networking Unified SASE platform

HPE Aruba Networking Manufacturing

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The Google Logo is a registered trademark of Google LLC. All third-party marks are property of their respective owners.

a00119879ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com