WHITE PAPER

SD-WAN For Financial Services

a Hewlett Packard
Enterprise company

In a recent survey[1] from the Enterprise Strategy Group on technology spending intentions, 55% of respondents in the financial services sector stated that they will increase their IT budget for 2021. In a post-COVID world, IT departments of financial services are indeed facing new challenges, with the acceleration of digitization to offer an improved customer experience and beat the competition, but also due to the increase of cybersecurity risks.

This white paper explores how an advanced SD-WAN platform coupled with network security features can address the challenges of financial services though five common use cases. By adopting an SD-WAN platform, financial institutions can simplify and secure their network infrastructure, enabling them to accelerate their digital transformation efforts and lay the foundation for a SASE architecture (Secure Access Service Edge).

CHALLENGES FACED BY FINANCIAL SERVICES

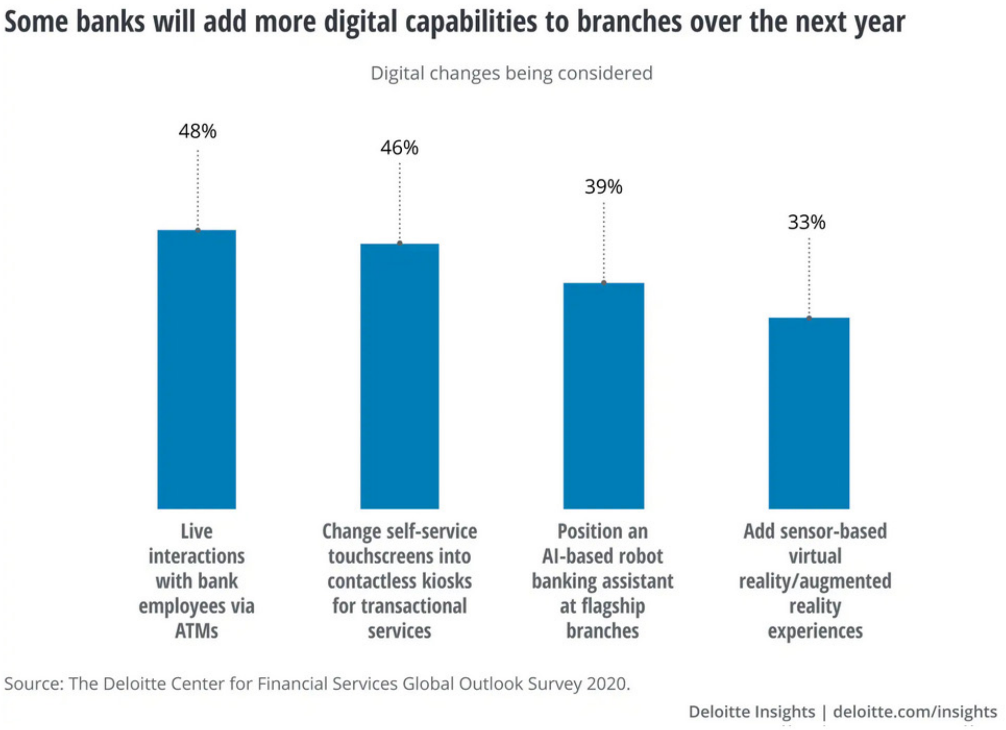
Digitization

One of the key challenges for financial services organizations is to implement new digital services and improve customer experience. With the growing number of fintech startups proposing a simplified user experience, but also with the virtualization of exchanges due to the COVID crisis, traditional banks have been engaged in reshaping their services to provide a unified experience to remain competitive.

A Deloitte study[2] conducted in April 2021 indeed mentions that *"Fintech investment increased from $12.7 billion in the first quarter of 2020 to $23.4 billion for the same period in 2021, an increase of 84%. This figure represents the most investment of any quarter over the last 3 years."*

Additionally, as digital services grow, retail banks will be focusing on providing more complex operations, while simpler transactions will be performed online. According to a McKinsey study from June 2020[3]: *"Branches' focus will evolve to assisting customers' complex needs. Branches will increasingly feature self-service (including intelligent ATMs and in-branch kiosks)."*

In another study from Deloitte[4] on banking and capital markets outlook in 2021, *"Nearly one-half of respondents indicate their institutions are considering live interactions with bank staff via ATMs, and installing self-service, contactless touchscreens. In addition, banks could incorporate artificial intelligence (AI)-based banking assistants and sensor-based augmented reality and virtual reality experiences."*



Source: The Deloitte Center for Financial Services Global Outlook Survey 2020.

[1] Source: 2021 Technology Spending Intentions Survey by Enterprise Strategy Group

[2] Source: Venture Scanner data; Deloitte Center for Financial Services analysis, April 2021

[3] Source: Reshaping retail banking for the next normal, McKinsey, June 2021

[4] Source: 2021 banking and capital markets outlook, Deloitte, December 2020

This evolution mainly relies on the cloud, and especially on the public cloud. In that context, corporate data centers are no longer at the center of all business application traffic. This implies providing a secure network connection to all customers with maximum uptime.

Additionally, as the number of remote workers also increases and brick-and-mortar locations decrease, financial services organizations are witnessing a virtualization of their workforce and therefore must also provide reliable and secure connectivity to their employees.

Network infrastructure

Banks often rely on a legacy MPLS network to connect branches to the headquarters. According to Deloitte[5] in its 2018 Banking Industry Outlook, *"The potential for cyber risk has been increasing with greater interconnectedness in the banking ecosystem, rapid adoption of new technologies, and* ***continued reliance on legacy infrastructure designed for a different age."***

In fact, many banks have had to face multiple mergers and acquisitions which increased the complexity of the network. Also, business-critical applications including CRM software, office applications and customer-facing applications are shifting to the cloud. This creates bottlenecks when cloud traffic is backhauled to the corporate data center for security reasons. Very often, branches have difficulty maintaining consistent high-quality video and voice over IP services, or simply they are unable to load customer information on their screens, as they can't reliably connect to the main data center. Many banks have difficulties expanding their locations, opening up new branches or connecting to remote ATMs as it can take as much as four months to provision a new MPLS circuit. They may also not have sufficient bandwidth to accommodate disaster recovery plans and backups in remote sites.

Additionally, banks often have limited IT budgets that prevent them from investing in new expensive MPLS lines or modernizing their network infrastructure to improve application quality of service.

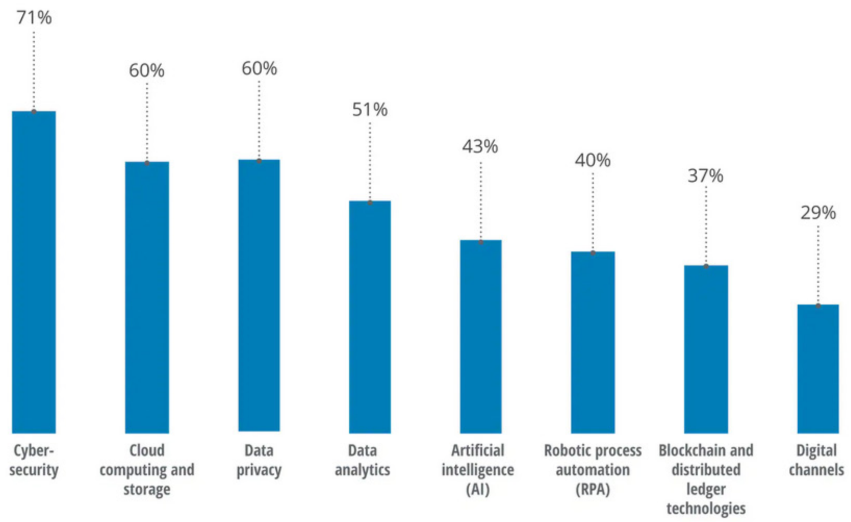
Cybersecurity threats

Due to the sensitivity of their data, financial services organizations are a main target for cybercrime and data breaches. Cyberattacks range from stealing money, to stealing personal identifying information including social security numbers, leaks of credit card numbers, DDoS attacks, ransomware and more.

As the volume of transactions continues to increase, cyberattacks have become a major concern for banks, and during the COVID-19 pandemic, financial institutions experienced a spike of digital attacks. According to a Deloitte study[6] on banking and capital markets outlook, most respondents said they will increase spending on cybersecurity technology in 2021.

Banks plan to increase spending on various technologies over the next year

Finance respondents whose organizations plan to increase spending



Source: The Deloitte Center for Financial Services Global Outlook Survey 2020.

Deloitte Insights | deloitte.com/insights

[5] Source: 2018 Banking industry outlook, Deloitte, 2018

[6] Source: 2021 banking and capital markets outlook, Deloitte, December 2020

The interconnectivity of banks is another factor of risk. In a 2020 report[7] by the Federal Reserve Bank of New York on cybersecurity risks and the US financial system, a cyberattack on one of the most active banks could affect 38% of the network.

To prevent – or at least minimize – cyber risk, it is essential that banks secure their transactions and their network connections.

Regulatory Compliance

Financial services are one of the most regulated industries. Most regulations are in place to protect the consumer from potential fraud and to bring transparency to financial services' operations. Many regulations deal with data security and require establishing secure network connections, for example, between branch locations and the data center to protect customer data. Other requirements such as PCI Data Security Standard (PCI DSS) establish security standards for protecting credit cardholder data, especially when vulnerabilities exist anywhere in the transaction process including point-of-sale devices, servers and web sites.

Financial services organizations are required to demonstrate compliance while dealing with limited resources to enforce regulations, as well as potential data security issues and other threats.

SD-WAN USE CASES SPECIFIC TO FINANCIAL INSTITUTIONS

Many of the challenges mentioned above will be addressed as part of an overall enterprise effort. Based on a few use cases, let's take a look at how adopting an advanced SD-WAN platform can help financial services better tackle these challenges.

Use case #1: Simplify network infrastructure while reducing costs

Many banks continue to subscribe to legacy MPLS services that often provide limited bandwidth, especially at branch sites. Additionally, as the number of cloud-hosted applications have increased proportionally over the years, financial organizations, still using traditional router-based WAN architectures, must backhaul cloud-destined traffic to the main data center for security reasons. This results in added delay (latency) and leaves remote branches in a difficult situation to handle business operations efficiently as more business-critical applications rely on the cloud.

The Aruba EdgeConnect SD-WAN edge platform can actively use broadband internet and 4/5G LTE services that are less expensive than private line services.

The Aruba EdgeConnect SD-WAN edge platform simplifies the WAN infrastructure and supports a number of advanced performance features to overcome the lack of reliability of internet and LTE connections. Features include:

Path Conditioning: Internet and wireless links often suffer from packet loss and jitter and are more prone to outages. With the Aruba EdgeConnect **Forward Error Correction (FEC)** feature, lost packets are automatically reconstructed. This is accomplished by periodically sending parity packets, using a technique similar to RAID disk drive arrays, to rebuild dropped data packets without having to retransmit them. Depending on the application quality of service requirements, the FEC ratio can be specified in the EdgeConnect Business Intent Overlay (BIO) configuration. For example, for applications that demand very high quality and availability such as real-time voice or video, a 1:1 ratio can be used; for less demanding applications, an adaptive FEC algorithm may be specified that automatically adjusts the error correction packet ratio based on the current rate of packet loss at any given time. In addition, when load-balancing traffic between multiple WAN transport services using tunnel bonding, **Packet Order Correction (POC)** re-orders any packets that arrive out of sequence at their destination.

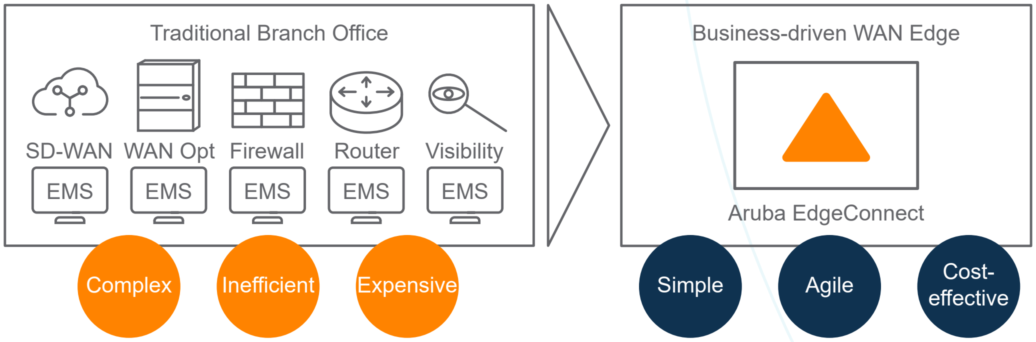


Figure 3. Aruba EdgeConnect enables financial institutions to move from a complex architecture to a simple, cost-effective network infrastructure

[7] Source: Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis, Federal Reserve Bank of New York, January 2020

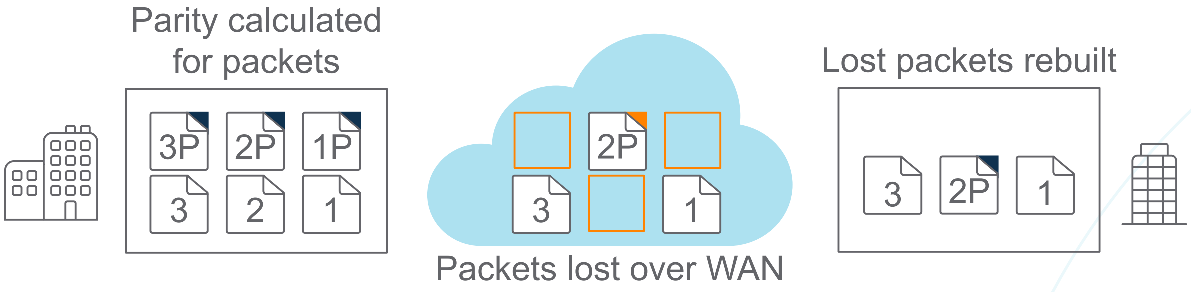
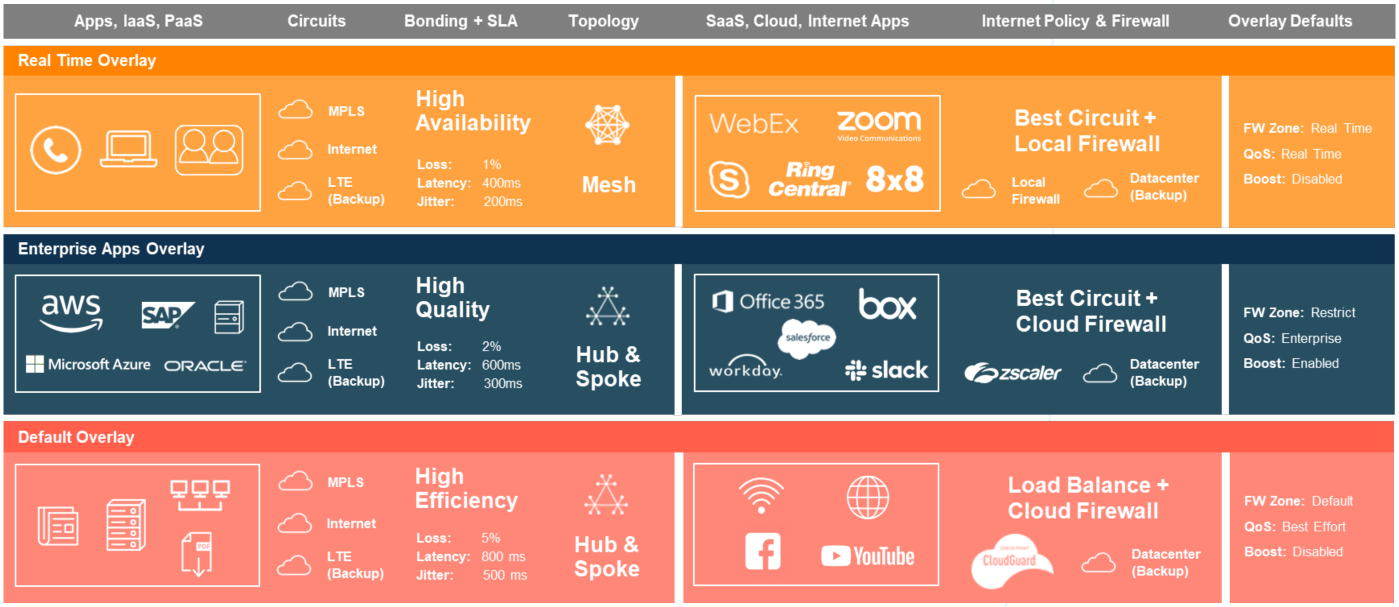


Figure 4. Forward Error Correction: packets lost in transmit across the WAN are automatically rebuilt

Tunnel Bonding and Dynamic Path Control: The Aruba EdgeConnect tunnel bonding feature combines multiple WAN transport services to create a single, higher bandwidth logical link. Link bonding policies optimize the connection speed depending on the type of traffic and business needs. For example, WAN connections from two different service providers can be bonded to increase the speed of delivery. In another example, an MPLS service, an internet broadband link and a 5G/LTE connection can be bonded together.

Business Intent Overlays are used to configure the policies that control how EdgeConnect automatically and seamlessly steers application traffic. Link bonding policies include “high availability” for applications such as video over IP which requires the highest levels of performance and availability. Because data packets traverse one link and error correction packets traverse the other link, failover is instantaneous in the event of a transport outage. The “high throughput” link bonding policy distributes traffic across multiple paths such that the aggregate bandwidth is used, providing higher bandwidth and performance than possible on any single link. Other link bonding policies provide additional flexibility, and network managers can also define custom policies.



Apps, IaaS, PaaS	Circuits	Bonding + SLA	Topology	SaaS, Cloud, Internet Apps	Internet Policy & Firewall	Overlay Defaults
Real Time Overlay						
☎	MPLS Internet LTE (Backup)	High Availability Loss: 1% Latency: 400ms Jitter: 200ms	Mesh	WebEx zoom Video Communications Ring Central 8x8	Best Circuit + Local Firewall Local Firewall Datacenter (Backup)	FW Zone: Real Time QoS: Real Time Boost: Disabled
Enterprise Apps Overlay						
aws SAP Microsoft Azure ORACLE	MPLS Internet LTE (Backup)	High Quality Loss: 2% Latency: 600ms Jitter: 300ms	Hub & Spoke	Office 365 box salesforce workday. slack	Best Circuit + Cloud Firewall zscaler Datacenter (Backup)	FW Zone: Restrict QoS: Enterprise Boost: Enabled
Default Overlay						
PDF	MPLS Internet LTE (Backup)	High Efficiency Loss: 5% Latency: 800 ms Jitter: 500 ms	Hub & Spoke	YouTube	Load Balance + Cloud Firewall CloudGuard Datacenter (Backup)	FW Zone: Default QoS: Best Effort Boost: Disabled

Figure 5. Business intent overlays enable financial institutions to create virtual networks based on the needs of the business

Local internet breakout: To avoid backhauling all the traffic to the corporate data center, Aruba EdgeConnect SD-WAN can automatically steer internet-bound traffic directly to its destination or to a cloud-delivered security service. The EdgeConnect First-packet iQ™ feature identifies and classifies applications based on the first packet, enabling automatic traffic steering to the internet or to the data center according to business and security requirements. With this feature, financial services organizations can build security policies that:

- Backhaul data center-hosted application traffic to a headquarters or hub location,
- Send trusted cloud application traffic, such as Microsoft 365 or UCaaS traffic, directly to the internet,
- Send all other internet-bound traffic, including Salesforce, Facebook, YouTube, and web browsing traffic to a cloud-delivered security solution such as Zscaler for security inspection before it is handed off to the SaaS provider

Aruba EdgeConnect also monitors the performance of all links by continuously measuring the throughput, packet loss, latency, jitter, and mean opinion score (MOS) in real-time. Through intelligent internet breakout and using statistical learning based on loss, latency, jitter, and MOS, it dynamically determines and automatically chooses the best performing internet link (if more than one has been provisioned) to send the traffic.

In summary, local Internet breakout reduces the MPLS bandwidth circuit requirements by limiting the number of applications to backhaul, reducing cost and improving security.

Use Case #2: Quickly spin up new branches and open new ATMs

As they grow, retail banks open new branches to reach more customers and increase competitiveness. Also, banks are adding a new generation of ATMs in branches, that deliver advanced digital capabilities such as live interactions and AI, requiring more network bandwidth. However, it can take 60 to 120 days or more to deploy a new MPLS service at a new location, while broadband internet services can usually be provisioned within a few days. Aruba EdgeConnect SD-WAN advanced features deliver private line-like performance over the broadband internet. As discussed in the previous use case, EdgeConnect uses **path conditioning, dynamic path control and local internet breakout** to speed up and secure the traffic over the public internet and 4/5G LTE connections.

Additionally, Aruba EdgeConnect **zero-touch provisioning (ZTP)** greatly simplifies connecting and deploying a new site. An office manager with limited or no IT experience can simply install the EdgeConnect SD-WAN appliance in the remote site. The new appliance will self-register if it has been authenticated prior to being admitted onto the SD-WAN fabric. Once authenticated, the new appliance automatically receives its configuration from Aruba Orchestrator with no human intervention required at the location. Centralized Orchestration also ensures that QOS and security policies are seamlessly enforced in the new branch.

Instead of taking months to deploy new sites, it just takes a couple of weeks with an EdgeConnect SD-WAN while reducing costs and improving network efficiency.

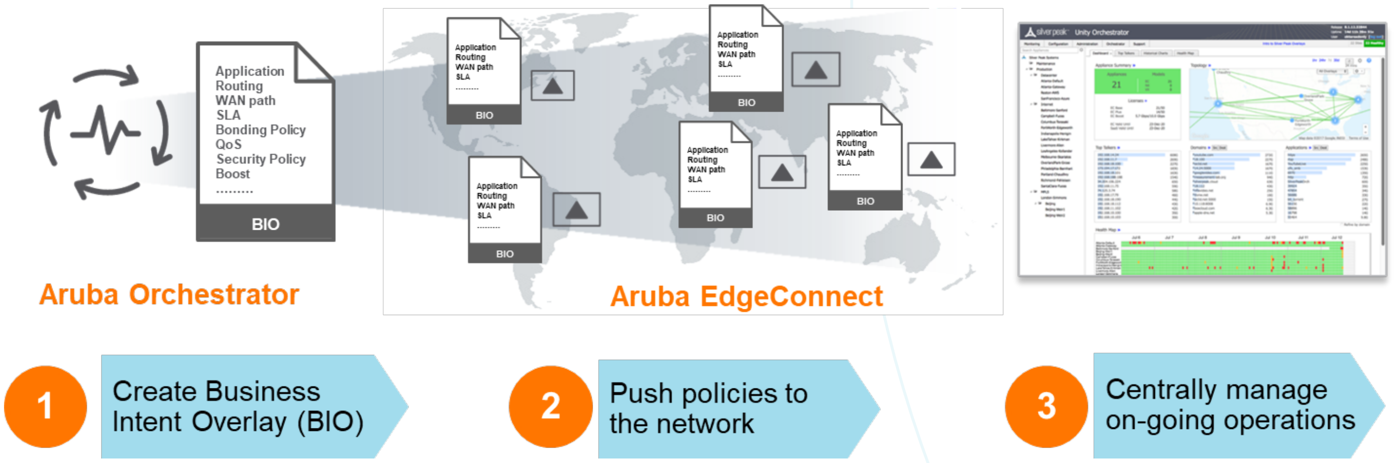

Application
Routing
WAN path
SLA
Bonding Policy
QoS
Security Policy
Boost
BIO
Aruba Orchestrator
Application Routing WAN path SLA
BIO
Aruba EdgeConnect
silver peak Unity Orchestrator
1
Create Business Intent Overlay (BIO)
2
Push policies to the network
3
Centrally manage on-going operations

Figure 6. Simplify and accelerate deployments with a top-down model and business-driven policies

Use Case #3: Accelerate backups and improve disaster recovery plans

Most enterprise disaster recovery planning includes data to be backed up in one or more remote locations that could be hundreds of miles away from the main location. As the distance between remote sites and backup locations increases, latency increases, resulting in a slower data transfer. With data sets now measured in terabytes, the transmission of data for backup purposes can take several hours or can fail when WAN transport services become impaired.

Aruba Boost **WAN Optimization** significantly accelerates the transmission of data by applying TCP protocol acceleration as well as data deduplication and compression:

TCP Protocol acceleration: delays are caused in latent environments by window scaling and acknowledgment procedures. Aruba Boost TCP Acceleration overcomes these delays with four key components:

- **Window scaling:** Aruba Boost increases by a factor of 250 the transmitting window size, which corresponds to the amount of data that can be sent before an acknowledgement is sent back. By doing so, it significantly increases the maximum possible transfer rate.
- **Selective acknowledgement:** It supports selective acknowledgement (SACK) by retransmitting only the necessary packets instead of retransmitting data that was already sent in a lossy network environment.
- **Round Trip Time measurement:** It reduces the round-trip time (RTT) measurement by using the actual latency instead of the fixed-length acknowledgement timer that is normally used in case of lost packets.
- **High Speed TCP:** It modifies the congestion mechanism by optimizing the congestion window size, that regulates the times at which the segments are sent into the network. It may indeed take a very long time for the congestion window to recover in a standard TCP congestion control technique. With High-Speed TCP, window congestion size is increased by a larger amount and decreased by a smaller amount.

Data deduplication and compression: due to the amount of data to be sent from the branch office to the backup site combined with other application traffic, network congestion can occur. To minimize the amount of data to be transmitted, Aruba Boost employs sophisticated data deduplication and data compression algorithms. Duplicate data is removed and replaced with a fingerprint and a pointer so that only the necessary data is transmitted across the WAN. The original data is stored in a disk cache so that data is reconstructed with the duplicate data at the destination. Data compression leverages an LZ (Lempel-Ziv) compression algorithm to reduce the amount of data transmitted. Data compression is applied both for the payload and the IP header.

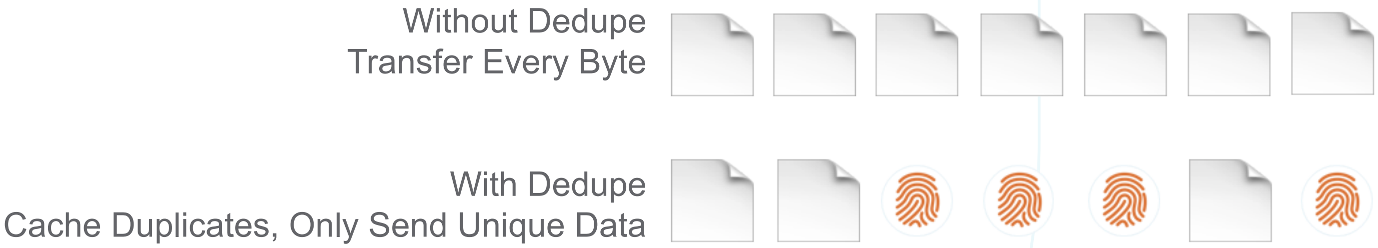


Figure 7. Data reduction: Eliminate overhead of redundant packets traversing the WAN

By applying Aruba Boost WAN optimization, financial services organizations increase WAN throughput from their main locations to the remote backup sites. They significantly shrink backup time and accelerate recovery. They also increase replication capacity by sending more data to the recovery site while reducing bandwidth used.

Use Case #4: Secure access and protect customer data

The security perimeter of financial institutions is dissolving. As the pace of digitization of financial services has accelerated, more transactions are now being carried out in the cloud. In fact, fewer financial applications now reside in the corporate data centers, while more traffic is heading to the public cloud.

Financial institutions must protect customer data when using cloud applications to meet compliance requirements. They also must provide secure access from anywhere to their customers as well as their employees, as remote working is the new norm.

Backhauling cloud application traffic to the main data center for security inspection is no longer a viable solution, as it provides a poor customer experience.

Aruba EdgeConnect is the foundation for a robust SASE architecture that lets financial institutions choose from the best-of-breed cloud security components to complement their best-of-breed WAN edge.

A Secure Access Service Edge (SASE), as defined by Gartner[8], focuses on users and provides security and access services close to the users, instead of securing a limited perimeter. SASE combines advanced WAN edge network functions including SD-WAN with core network security features such as ZTNA, CASB, SWG, FWaaS, and more hosted in the cloud rather than physical appliances.

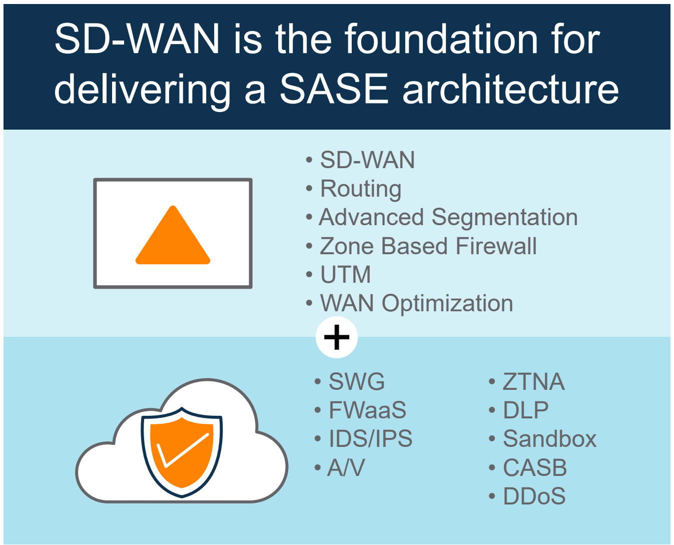


Figure 8. SD-WAN combined with network security delivers a SASE architecture that enables organizations to fully embrace digital transformation.

By successfully implementing SASE, financial services can move from a heavy branch to a thin branch model.

It is indeed common to find many discrete network and security appliances in branches, including routers, firewalls, VPNs, and WAN optimization controllers. Besides equipment sprawl, the local staff rarely has the skills and time to operate and maintain them. By moving to a thin branch model and adopting a SASE architecture, branches can simplify their network infrastructure and increase security.

Aruba EdgeConnect SD-WAN reduces equipment sprawl by centrally managing and automatically deploying network controls, but also it includes advanced security features such as a zone-based firewall and automates the orchestration to third party cloud security providers. Aruba security capabilities rely on three pillars:

- Unified branch security
- Zero trust segmentation
- Automated orchestration with third-party cloud providers

Unified branch security

With centralized orchestration, security policies are automatically pushed to branches with zero-touch provisioning. New branch offices are set up quickly and easily, and security policy changes can be automatically distributed to hundreds or thousands of branches in minutes while minimizing errors.

Aruba EdgeConnect embeds an app-user aware firewall, providing stateful capabilities that controls incoming traffic and blocks packets that do not belong to a valid session. The built-in firewall also uses deep packet inspection that checks both data packet headers and the packet payload. It is therefore capable of blocking malicious content included in websites and applications. It also provides web-content and URL filtering to block any unsafe and inappropriate content.

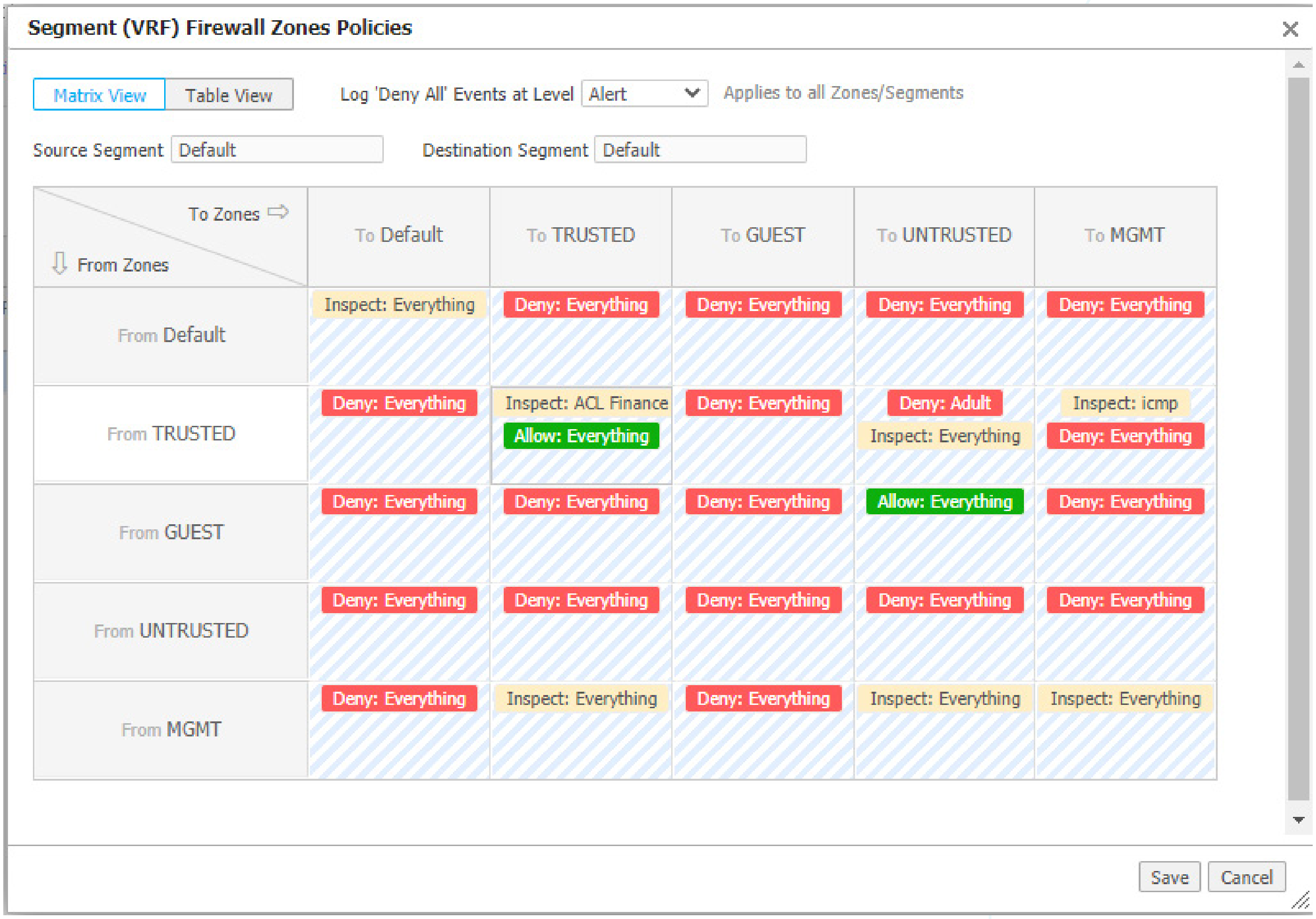
The integration of Aruba Threat Defense with the Aruba EdgeConnect firewall adds intrusion detection and prevention capabilities (IDS/IPS) to monitor, flag and drop traffic in case of a security threat.

[8] Gartner, The Future of Network Security Is in the Cloud; 30 August 2019; Lawrence Orans, Joe Skorupa, Neil MacDonald

Zero trust segmentation

Aruba SD-WAN advanced zero trust security features ensures that users and devices can only communicate with destinations consistent with their role based on identity, role and security posture.

Segmentation improves security and protects customer data by splitting the network into subnetworks, limiting the spread of cyberattacks and malware. It also helps reduce congestion and improve operations. For example, the customer network can be separated from the bank operational network, or control systems such as HVAC, can be separated from financial transaction applications.



Segment (VRF) Firewall Zones Policies

Log 'Deny All' Events at Level: Alert — Applies to all Zones/Segments

Source Segment: Default   Destination Segment: Default

To Zones ⇨ ⇩ From Zones	To Default	To TRUSTED	To GUEST	To UNTRUSTED	To MGMT
From Default	Inspect: Everything	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything
From TRUSTED	Deny: Everything	Inspect: ACL Finance Allow: Everything	Deny: Everything	Deny: Adult Inspect: Everything	Inspect: icmp Deny: Everything
From GUEST	Deny: Everything	Deny: Everything	Deny: Everything	Allow: Everything	Deny: Everything
From UNTRUSTED	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything	Deny: Everything
From MGMT	Deny: Everything	Inspect: Everything	Deny: Everything	Inspect: Everything	Inspect: Everything

Figure 9. Segment and isolate application traffic with micro-segmentation

Segmentation is achieved with an end-to-end zone-based firewall in Aruba EdgeConnect. Business intent overlays and WAN interfaces are assigned to zones. Network managers can then allow or deny traffic between zones. For example, a zone for customers can be defined, and another one for the bank's accounting systems. A rule can then be set to deny access from the customer zone to the accounting zone.

The integration of Aruba ClearPass Policy Manager with Aruba EdgeConnect adds identity knowledge of users, devices and roles with authentication capabilities such as RADIUS, TACACS+, and OAuth2 to manage network access and enable a dynamic segmentation, anywhere on the network – wired or wireless infrastructure. Through role-based access policies, users and devices are automatically assigned the proper access control policy and dynamically segmented from other users and devices.

Automated orchestration with best-of-breed third-party cloud security providers

Financial institutions can choose best-of-breed security services to integrate with Aruba EdgeConnect thanks to the First-packet iQ™ application classification feature. Aruba EdgeConnect identifies applications on the first packet and sends the cloud application traffic to a third-party cloud-delivered security service that provides best-in-class security functions such as CASB, SWG and ZTNA, while traffic from suspicious applications is sent to the data center for further inspection. The orchestration and integration with cloud security vendors are fully automated enabling financial institutions to quickly deploy multiple security partners.

It is also possible to deploy a virtual instance of EdgeConnect in any or all of the four public cloud providers including AWS, Microsoft Azure, Google Cloud and Oracle Cloud Infrastructure. This "bookended" solution provides advanced security and predictable application performance.

The automated security orchestration ensures that no data breach happens, no malware is downloaded, and no command-and-control servers are connected.

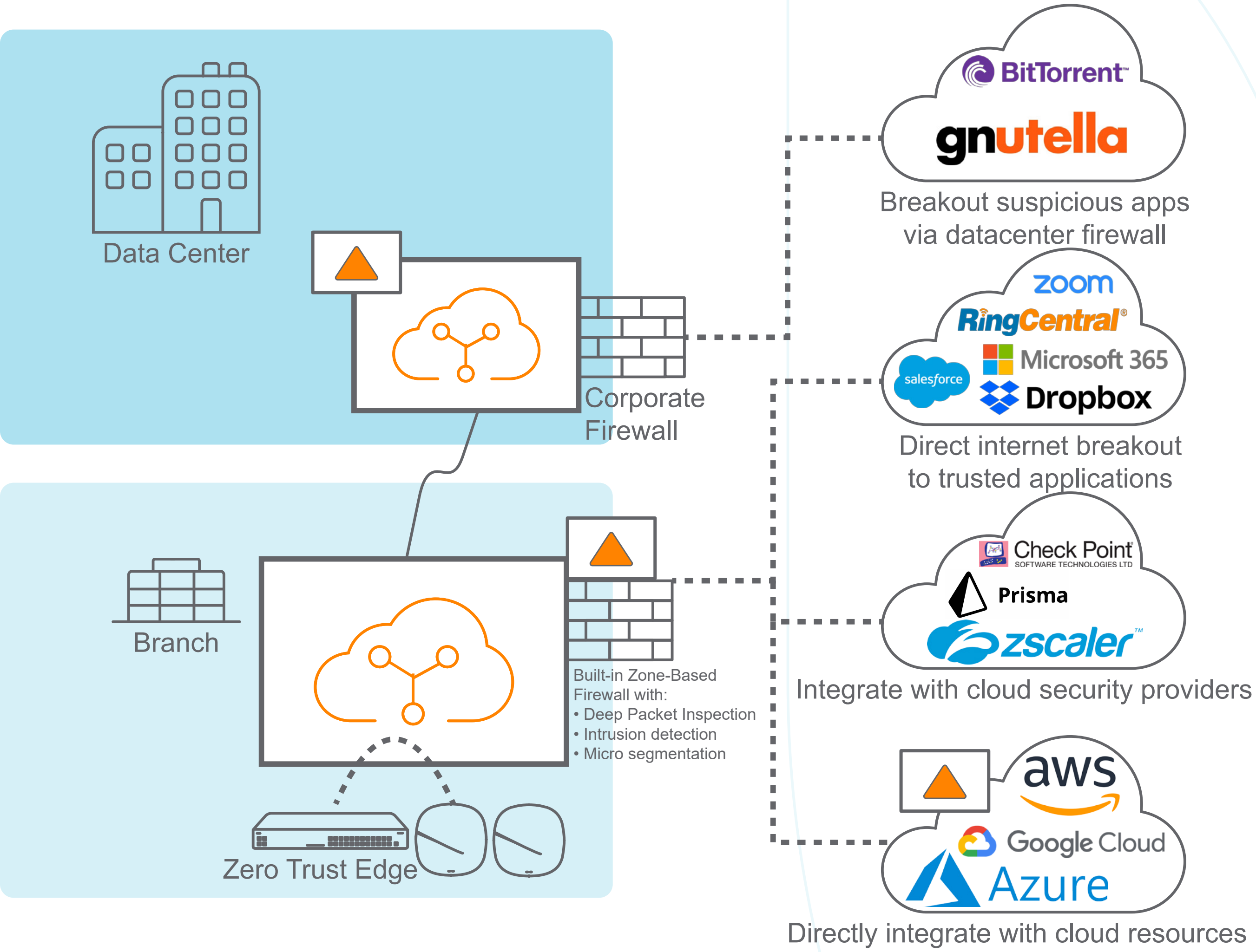

Data Center
Corporate Firewall
Branch
Built-in Zone-Based Firewall with:
• Deep Packet Inspection
• Intrusion detection
• Micro segmentation
Zero Trust Edge
BitTorrent
gnutella
Breakout suspicious apps via datacenter firewall
zoom
RingCentral
salesforce
Microsoft 365
Dropbox
Direct internet breakout to trusted applications
Check Point SOFTWARE TECHNOLOGIES LTD
Prisma
zscaler
Integrate with cloud security providers
aws
Google Cloud
Azure
Directly integrate with cloud resources

Figure 10. Automate security orchestration based on application type and threat

Use case #5: Meet PCI DSS compliance mandates

According to a 2020 Nilson report[9], fraud losses of card transactions from merchants, as well as acquirers of card transactions from ATMs reached $28.65 billion in 2019, up 2.9% from $27.85 billion in 2018.

Fines for non-compliance can vary from $5,000 to $100,000 per month until the merchant or the financial service achieves compliance.

PCI DSS (Payment Card Industry Data Security Standard) specifies twelve requirements around cardholder data to reduce credit card fraud. Any organization that processes cardholder data is required to comply. The Aruba EdgeConnect SD-WAN platform assists organizations in meeting compliance for nine of the twelve requirements while the three remaining are not applicable.

#	REQUIREMENT	ARUBA COMPLIANCE
1	Installing and maintaining a firewall configuration to protect cardholder data.	Protection of device and control planes; secure configuration and change management
2	Changing vendor-supplied defaults for system passwords and other security parameters.	Password policies including default password warning
3	Protecting stored cardholder data.	Boost WAN optimization network memory function may store packet contents on a flash drive or disk in which case it is encrypted using AES-128
4	Encrypting transmission of cardholder data over open, public networks.	Data and management interface encrypted using AES-256
5	Protecting all systems against malware and performing regular updates of anti-virus software.	Direct selected network traffic to anti-malware and sandboxing products from Aruba security partners using automation, orchestration, and drag-and-drop service chaining
6	Developing and maintaining secure systems and applications.	Vulnerability assessments with each new release Issue patch updates as required
7	Restricting access to cardholder data to only authorized personnel	N/A
8	Identifying and authenticating access to system components.	Multiple unique logins for different user roles with appropriate privilege levels; Optionally support authentication with RADIUS or TACACS+; Enforce the use of multi-factor authentication for all non-console administrative access and remote access to the cardholder data environment
9	Restricting physical access to cardholder data.	Provisions for backup and disaster recovery; EdgeConnect configuration and snapshots may be stored offsite.
10	Tracking and monitoring all access to cardholder data and network resources.	Full audit logs of user logins and all change management actions
11	Testing security systems and processes regularly.	N/A
12	Maintaining an information security policy for all personnel.	N/A

[9] Nilson report, December 2020, issue 1187, https://nilsonreport.com/publication_newsletter_archive_issue.php?issue=1187

CONCLUSION

In the post-COVID world, with the digitization of financial services occurring at an increasing pace, the virtualization of the workforce, and increase in cybersecurity risks, financial institutions must now rely on secure, trustworthy, and dependable network connections.

Due to limited budgets and other priorities, the network infrastructure of financial institutions has oftentimes been neglected. Many institutions struggle with complex, aging MPLS networks, as well as outdated VPN connections that are no longer adapted to the cloud and the post-COVID world.

Backhauling cloud application traffic to the corporate data center is no longer a viable solution to secure the increasing number of cloud-hosted financial applications. With the cloud, banks must move away from a data center centric approach, as the hub of all network traffic. Instead, they must embrace a flexible approach that relies on a thin branch model that is easy to deploy, using SD-WAN as the foundational element, backed by highly efficient security solutions hosted in the cloud. This approach is called SASE – Secure Access Service Edge – that combines advanced SD-WAN functions with comprehensive security services delivered in the cloud.

The Aruba EdgeConnect SD-WAN enables a robust SASE architecture and a simpler thin branch WAN edge model. It enables financial institutions to simplify their network infrastructure and reduce costs by combining MPLS, 5G and internet broadband lines in the same logical link. Aruba EdgeConnect improves application performance, it is centrally orchestrated and easy to deploy. It includes advanced security capabilities with data encryption, zone-based firewall and zero-trust segmentation. Coupled with the best-of-breed cloud network security providers, it provides the foundation for a strong and reliable SASE architecture, that allows financial services to fully embrace digital transformation while mitigating cybersecurity risks.

Additionally, Aruba EdgeConnect SD-WAN seamlessly integrates with all of the four cloud services providers – AWS, Microsoft Azure, Google Cloud, Oracle, as well as API integration with Microsoft 365 – increasing security and application performance.

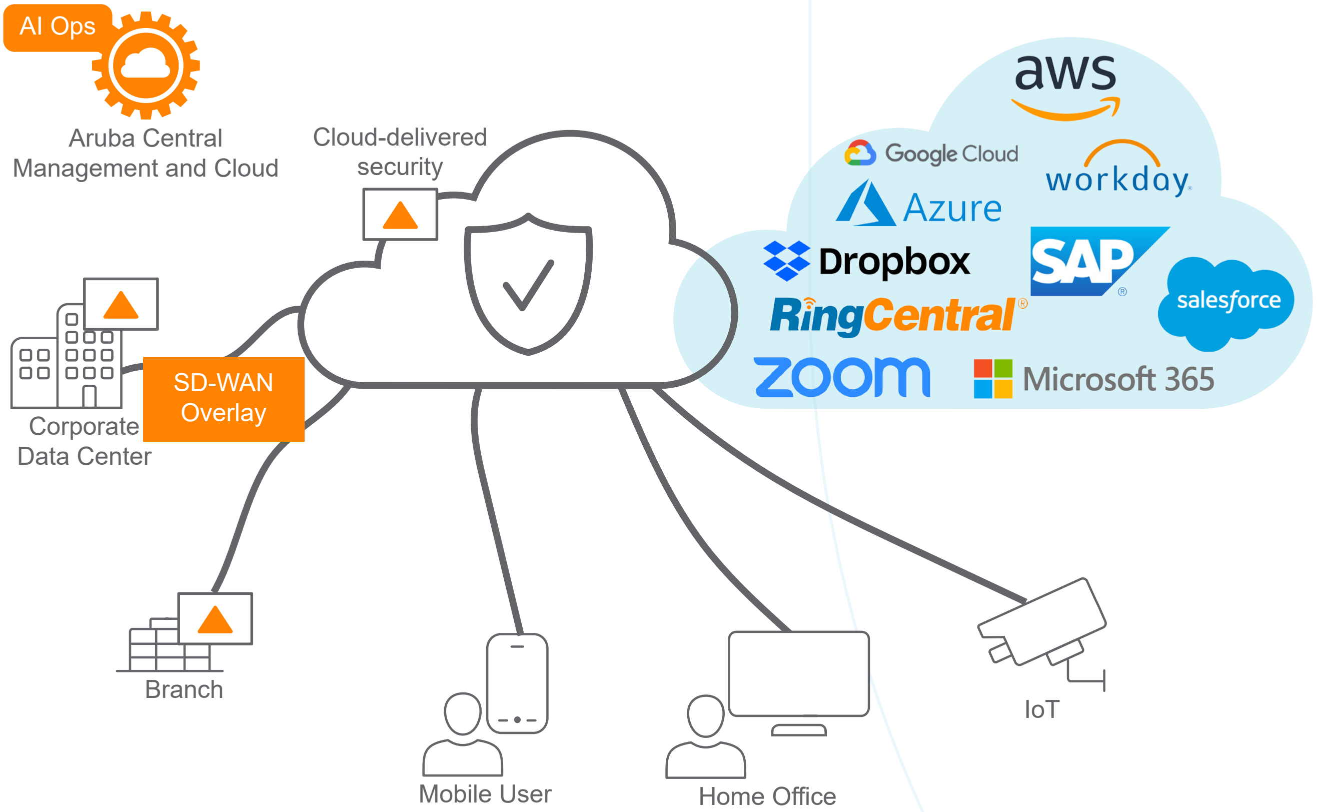


Figure 11. Aruba EdgeConnect is the foundation for a robust SASE architecture that enables financial institutions to choose from the best-of-breed security components

Aruba EdgeConnect is a key element of the Aruba Edge Services Platform (ESP) that provides a unified approach to centrally manage all network aspects including wireless, LAN and WAN connectivity with a common zero trust and SASE security framework spanning the entire portfolio. Aruba advanced AIOPS capabilities automatically and continuously monitor the network, applications and security policy enforcement, enabling automated remediation to impairments or potential threats.

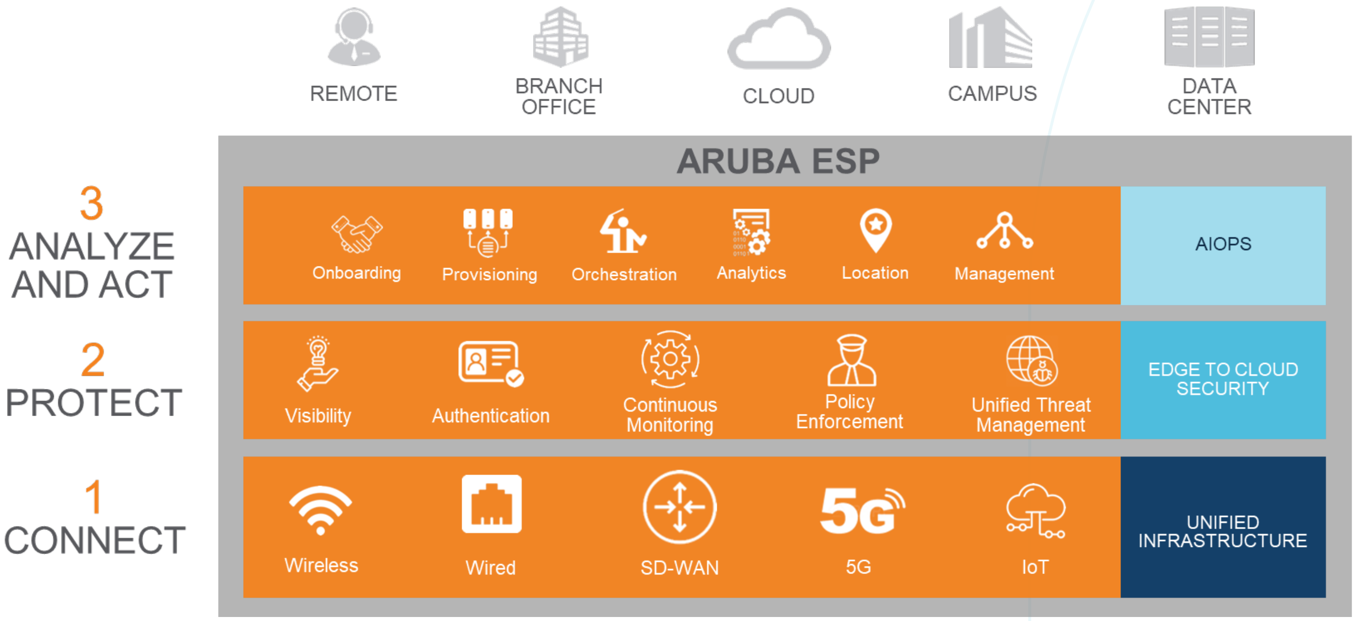


Figure 12.. The three layers of Aruba Edge Services Platform

aruba
a Hewlett Packard Enterprise company

WP_SD-WANforFinancialServices_RVK_120321

Contact us at www.arubanetworks.com/contact