Secure Access Discovery Guide

Guide

carahsoft

For more information, contact Carahsoft or our reseller partners:
CAmarketing@carahsoft.com | 703-871-8539

Discovery Guide

Symantec Secure Access Cloud | Zero Trust

Draft Copy

June 2020

BROADCOM®

Secure Access Cloud | Introduction

A brief introduction to Secure Access Cloud – Zero Trust Framework

INDEX

The Challenges

Protecting your organization's network and data can be a tough task especially when you're not using the most optimal tools or architecture. Some of the challenges organizations are facing

- Network complexity associated with legacy technologies, backhauling VPN traffic
- Operational expenses
- Operational complexity
- The traditional architecture - **castle wall and moat" model** is not sufficiently secure. Once a would be attacker gets in to your network, they can easily move around from device to device – **a hard exterior but soft gui interior**.
- Users have access to the whole network therefore if a device is compromised, the attacker can easily access the network.
- Wide attack surface
- No ability to monitor user's movements

How SAC can help

The Cloud Generation has forever changed the way employees access information and this transformation has created significant complexities for enterprises and has exposed the security vulnerabilities that exist in traditional network access technologies like VPNs.

Secure Access Cloud introduces zero trust principles to fully protect your resources

- Cloud Native
- Adhere to the zero trust principles
- Only extending users the access to specific applications, not to the entire network – accessible via SAC only.
- The whole network is more secure.
- Reduces the attack surface - Software Defined Perimeter Approach - preventing Lateral Movement
- Monitoring your user's actions

Technology Types

Zero Trust Framework

Zero Trust provides a model for designing networks and systems to address the modern threat landscape. It is based on the concept of least privilege, which calls for limiting access rights to users to the bare minimum that they need to accomplish their specific tasks.

SASE

SASE is the convergence of wide area networking, or WAN, and network security services like CASB, FWaaS and Zero Trust, into a single, cloud-delivered service model. According to Gartner, "SASE capabilities are delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions.

Add 2 different slides – zero trust and Sase Alignment

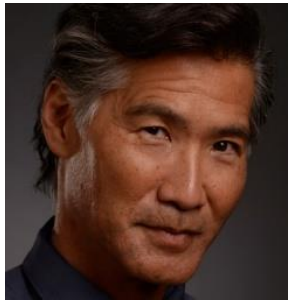
Key capability in sase and zero trust architecture

BROADCOM

Key Personas | IT Decision Maker

Grant

Chief Information Security Officer (CISO)



Alternative Titles:

Chief Security Officer (CSO), Chief Security Architect (CSA), Chief Risk Officer, Information Security Manager (ISM), VP Information Security

Overview

Reports to: Usually the CIO, but occasionally to other C-Level executives (CTO, CEO)

Buying role: Approves or significantly influences the vendor selection decision.

Buying center: IT, Security

Budget authority: Operates within CIO/CTO budget, approves individual allocations within that budget.

Personality

Background: Usually a highly technical background, but will be very business focused. Pragmatic and logical.

Likes: The Big Picture, staying up to date on the latest and greatest, risk/benefit analysis.

Dislikes: Risk, spending too much time in the weeds.

Preferences

Interaction Preferences

- Analyst and consultant inquiries
- Personal and customer references
- Industry conferences
- Will rely on his/her technical team

Content Preferences

- Analyst reports & third-party reports or validations
- Customer testimonials & case studies
- EBC briefings, especially further down the funnel.

Interaction and Content Dislikes

- Blogs, either thought leadership or vendor.
- Marketing fluff – brochures, videos, newsletters
- Trade shows & user conferences, Vendor webinars

Watering Holes

- Consultants: Deloitte, KPMG, PWC, DXC
- Conferences: RSA, Gartner IAM, Evanta CISO Summit, Secure World, Blackhat, Def Con, ISSA CISO Forum, industry specific
- Forums: RSA Board, Gartner Board, Forrester Security and Risk Leadership Council, LinkedIn CSO Forum, LinkedIn CISO Executive Network
- Analysts: Gartner, Forrester, KuppingerCole

Qualifying Questions

Discovery Stage

Explore Stage

Buy Stage

BROADCOM

Key Personas | IT Influencer

Marcus

Chief Security Architect

Alternative Titles:

Enterprise Architect, Information Security Architect, Information System Security Architect, Security Architect

Overview

Reports to: Usually CISO

Buying role: Evaluates solutions and makes product recommendations

Buying center: IT, Security

Budget authority: Operates within CIO/CTO budget, requests individual allocations within that budget.

Personality

Background: Technical background and maybe some business experience. Wants to do anything to make the system better.

Likes: Big Picture, but also a clear understanding of what is going on

Dislikes: Risk

Preferences

Interaction Preferences

- Analyst and consultant inquiries
- Industry conferences
- In person, straight-forward logical 1:1 conversations and demos; SMEs over sales
- Prefers email over phone; WebEx over conference call so he can see what you're talking about
- May turn to online communities to stay up-to-date with cybersecurity ideas

Content Preferences

- Analyst reports & third-party reports or validations
- Customer testimonials & case studies
- Websites, hands-on demos/trials
- Product documentation

Interaction and Content Dislikes

- Marketing fluff – brochures, videos, newsletters
- Basic overviews – prefers more technical explanations

Watering Holes

- Conferences: RSA, Gartner IAM, Secure World, BlackHat, Def Con, ISSA Chapter Meetings, industry specific
- Forums: Information Security Forum, Chief Architect Forum, The Open Group
- Analysts: Gartner, Forrester, KuppingerCole

Qualifying Questions

Discovery Stage

Explore Stage

Buy Stage

BROADCOM

Secure Access Cloud | Positioning

Elevator Pitch

Embrace Zero Trust strategy to ALL corporate resources and data
Comprehensive Zero Trust solution, combined with our market-leading security products, e.g., CASB, DLP
SAC offers a competitively differentiated zero-trust solution by securing access at the application layer through a simple, agentless deployment, giving customers a single, enterprise-grade solution that integrates easily with existing identity, and access management solutions.

Market Trends

• Digital transformation leading to rapid adoption of cloud-based datacenters, IaaS and PaaS and the adoption of software-defined management of the datacenter infrastructure.

• Increasing number of partners and contractors requiring limited or restricted access to corporate applications and data. Variety of device types in corporate environment has proliferated, including BYOD.

• Attackers leveraging network-level access for network-level exploits, MiTM attacks, lateral movement, etc.

• High infrastructure and operations costs of existing access solutions (VPN, DMZs).

Leading Questions

- What does your environment look like today, and where are your applications hosted? (On-prem, IaaS, etc.)
- Are you planning on moving corp apps to a hosted/cloud-based environment?
- How important is it for you to allow secure, native access for your employees to corporate resources from anywhere, anytime using any device?
- Do you have any corporate resources directly exposed to the internet today?

Value Proposition

In <15 words:
Secure Access Cloud is a software-as-a-service security platform that enables organizations to securely manage access to all their corporate resources from any device anywhere in the world.

In <75 words:
Secure Access Cloud enables organizations to adopt a multi-cloud approach while keeping operations and the security of access to corporate resources uniform and scalable. Without compromising on security, organizations can now allow their users, be they employees, contractors, business partners or customers, the flexibility to access corporate applications from any device and location worldwide."

Differentiators

Ease of Deployment
- Agentless access
- Deploys in minutes
- BYOD & 3rd party support
- Transparent to users
- Flexible integration (CI/CD,SIEM, SOC, etc.)
- Visibility

Enhanced Security
- Application level connectivity (Layer 7 only; no need for network access)
- Application specific access
- Eliminate Layer 3-6 network vulnerabilities
- Least-privileged access model based on user, device and application contexts
- Continuous enforcement of the defined contextual authorization policy
- Support for user-to-service and service-to-service access

Superior Visibility & Control
- Granular and adaptive access policies (e.g. user behaviour, data context)
- App Level Visibility and governance controls over user activities (e.g. file download)
- User actions audit trail

Proof Points

Analyst Quotes

“Gartner "Cool Vendors in Cloud Security," May 2018..”

Symantec was named a Leader in the Forrester Wave™: Zero Trust eXtended (ZTX)

Surveys

BROADCOM

Secure Access Cloud (ZT) | Prospecting

How to position and sell Symantec Secure Access Cloud

Goal	Challenges	Discovery	Positioning	Enablement
Increase product usage and customer retention	• Customer is worried about how they will impact their legacy systems and the historical deployment of peer-to-peer and distributed systems • How do they move from traditional architecture to zero trust architecture • Have not taken into account “least privilege” or PAM	• What does your current infrastructure look like now? • Are you securing access to privileged accounts today? • Do you have partners / contractors that have to access your network?	• If customer owns one or more other Symantec products, then position the PLA • If customer does not own any Symantec products, then position Secure Access Cloud or the Information Security PLA.	• Secure Access Cloud Customer Deck – add link

Assets	Awareness	Education	Validation	Adoption
Buyer & Customer Journey	• Demo Video – Secure Access Cloud • Whitepaper - 5 tips to make your cloud security roadmap flexible, agile, and user-friendly • Infographic – 5 tips to make your Coud Security Roadmap • Secure Access Service Edge (SASE) or Zero Trust? • The Good and Bad of 3 Common IP Whitelisting Scenarios • Digging Deeper into zero trust – Blog	• At-a-Glance *(internal/partners)* • Customer Deck • Data Sheet • Licensing Guide • A 5 step guide to go Zero Trust	• The Forrester WaveTM: Data Security Portfolio - Vendors, Q2 2019 • Market Guide for Zero Trust Network Access	

BROADCOM

Competitor Battlecards

BROADCOM

Secure Access Cloud (ZT) | Zscaler ZPA Battlecard

Corporate Overview

Key Statistics

World HQ: San Jose, California

Size: 1,480 employees

Revenues: $1 billion

Customers: Over 3,800

Key Dates

- Founded in 2008 by Jay Chaudry
- In April 2020, Zscaler agreed to purchase cloud security posture management startup Cloudneeti

Zero Trust Product Offerings

Zscaler provides a zero security solution called

- Zscaler Private Access (ZPA)

Sales Strategy

Embrace a zero trust networking strategy for your internal apps

- Position Zscaler Private Access (ZPA) as the Zero Trust access solution eliminating the need to segment networks, enabling user and application-centric security.
- Easy to install, providing a complete product for securing access.
- Integrates seamlessly with Zscaler Internet Access (ZIA) for access to the Internet and SaaS applications
- Secure your cloud transformation – get fast, secure and direct access to your apps without appliances
- Provide agentless connectivity for web applications

Objection Handling

Claim: Achieve a Zero Trust security model using ZPA
Zscaler supports only network level access policies, which does not prevent network level exploits and lateral movement. SAC provides brokered 'application level' access, never putting the user and their device inside the corporate network, removing the possibility of leveraging network level exploits and lateral movement.

Zscaler provides only network level auditing data (connection opened/closed, etc.) with no application level operation details. In addition, Zscaler does not provide any ability to restrict user's actions performed. SAC monitors all user's actions performed and blocks any unauthorized or anomalous user action in real-time.

Claim: A better access experience for the users
ZPA's UX is equivalent to any legacy VPN solution which requires using an endpoint agent to connect, define the authentication in the agent and troubleshoot any connectivity issues. With SAC's agentless solution, a user can easily be authenticated through their existing IdP or IAM solution and establish a connection to the corporate application using any native tool the user is using today.

Claim: Admins can easily set granular policies at the application level
ZPA claims that it allows for easy adjustment of policies or adding new rules. Setting up an access policy in ZPA requires manual integration with the IdP, complex SAML attribute mapping and does not provide the ability to define any activity policies to restrict the user's actions. In addition, ZPA policies are defined at the network level (IP:Port) ignoring software defined and dynamic cloud-based environments.

Claim: ZPA doesn't expose applications directly to the internet
Zscaler indeed doesn't expose applications directly to the internet. However, by providing direct connectivity between the user, the application server, and the network; network-based attacks are still a real threat when considering compromised computers or malicious users.

Secure Access Cloud (ZT) | Zscaler Battlecard

Zscaler Strengths

- **ZPA discovers IT apps**
- **Zscaler supports CIFS file sharing – meta file sharing and legacy fat client applications**
- **ZPA provides micro-segmentation:** Zscaler allows for micro-segmentation in the application server by deploying the Zscaler App connector directly on the application server.

Zscaler Weaknesses

- Web Portals (Limited)TCP Connection
- Network-level based connectivity – not application based
- No ability to restrict users' application activities
- No automation API's
- No service to service access scenarios

How to Position Against Zscaler

Simple, agentless deployment
Unlike Zscaler, which requires the deployment of an endpoint agent and a virtual appliance, SAC is agentless and does not require the deployment and maintenance of any appliances. Agents and appliances are invasive, offering a poor user experience, and only addressing corporate-issued devices. In today's modern enterprises, 3rd party access and BYOD have become the new norm and can't be ignored. SAC minimizes the time to deployment to bare minutes as no agents or appliances are required while providing a native user experience. In addition, SAC can easily integrated with the customer's environment (Identity provider, MFA, SIEM, etc.). Customers can also automate their entire remote access setup and configuration using SAC's management API.

Enhanced Security
SAC, the customer's datacenters are fully isolated from the internet and the end-users' devices (never putting the end-user and their device 'inside' the datacenter's network). This completely removes the ability of incoming internet threats as well as the possibility of network level exploitation and lateral movement originating from a compromised end-user device. In addition, SAC provides an out of the box 'least-privilege' access model by allowing the customers to enforce a per-application access policy based on the user (authentication method, location, etc.) and device (managed/unmanaged, compliance, etc.) context. SAC will continuously evaluate and enforce the defined access decision to prevent unauthorized or malicious access.

Detailed visibility and control of users' actions
Unlike ZPA which provides only network connection logs, SAC monitors and logs every user action performed at the application level. This allows customers to define the exact actions a specific user or group can perform, how often they can be performed, and respond in real-time in case of an unauthorized action or anomaly. The audit logs contain full details on the actions performed by the users to meet the organizational compliance and DFIR requirements.

BROADCOM

Secure Access Cloud (ZT) | Palo Alto Networks Battlecard

Corporate Overview

Key Statistics

Key Dates

Product Offerings

Sales Strategy

Objection Handling

BROADCOM

Secure Access Cloud (ZT) | Battlecard

How to Position Against Palo Alto

Palo Alto Strengths

Palo Alto Weaknesses

•

BROADCOM

Proof Points

BROADCOM

Secure Access Cloud | Proof Points

The Advantages and **Differentiators**

1 Ease of **Deployment**

- Agentless access
- Deploys in minutes
- BYOD & 3rd party support
- Transparent to users
- Flexible integration (CI/CD,SIEM, SOC, etc.)

2 Enhanced **Security**

- Application level connectivity (Layer 7 only; no need for network access)
- Application specific access
- Least-privileged access model based on user, device and application contexts

3 Superior Visibility and **Control**

- Granular and adaptive access policies (e.g. user behaviour, data context)
- App Level Visibility and governance controls over user activities (e.g. file download)
- User actions audit trail

4 Proven **Leadership**

Leadership in Industry Analyst reports

BROADCOM

Secure Access Cloud | Proof Points

Quick **Time to Value**

“Secure Access Cloud provides us with a practical access solution to all our applications while minimizing our risk exposure. Deploying Luminate's solution saved us at least 18 months and hundreds of man hours.

Guy Naor, CTO
NEX Optimization

BROADCOM

Symantec Secure Access Cloud | Proof Points

Proven **Leadership** | Analysts name Symantec PAM as Leader

Gartner names Symantec as a Strong Performer
in the Zero Trust Forrester Wave Report

Symantec has a powerful platform for big enterprise Zero Trust

The company's earlier acquisition of Luminate adds to its capabilities in the software-defined perimeter (SDP) space and in extending its solution in the network pillar of ZTX.

Forrester Wave Report, 2019

BROADCOM

Customer Stories

BROADCOM

Secure Access Cloud | Customer Stories

Click on logo to read the customer story

BROADCOM

Addressing Privileged Accounts at Scale with Symantec PAM

Customer Stories

Tracing its history back to 1690, Barclays Bank ranks in the Top 25 largest banks in the world. Barclays is also one of the Eurozone's largest financial institutions, with a market capitalization of over 37 billion dollars, 24 million customers, and over 4,750 branches.

BARCLAYS

The Business Challenge:

- Last year, Barclays needed to address Sarbanes Oxley, and went to CyberArk to manage their privileged accounts.
- This year, Barclays decided to expand this project to all non-personal accounts; however, when they performed scalability tests on CyberArk product, it failed. It could not handle the volume of accounts that Barclays needed to protect.

Symantec Delivers:

- Barclays is a large Broadcom customer and they recently signed a PLA with us in 2019.
- They decided to replace CyberArk with our PAM solution after they evaluated it and learned that they could use it for free under the PLA, saving themselves about $500K in maintenance annually.
- We are currently migrating the CyberArk accounts to PAM, and will have about 1.6 million accounts being protected by PAM when fully deployed.

Our superior performance and scalability factored significantly in Barclays' decision to replace CyberArk with Symantec Privileged Access Management. Additionally, the PLA eliminated the need for a new procurement action.

BROADCOM

Protecting App to App Communications with Symantec PAM

Customer Stories

Credit Suisse Group AG is a global wealth manager, investment bank and financial services company that was founded in 1856 in Switzerland. With about 47,000 employees and over CHF 1 Trillion is assets under management, it is one of the world's largest financial services companies.

CREDIT SUISSE

The Business Challenge:

- Provide ultimate security to one of the world's biggest financial services brands, who is known for its strict bank–client confidentiality and banking secrecy practices.
- Sought an enterprise solution to protect its privileged accounts and credentials, especially for those being used by applications.

Symantec Delivers:

- Application to Application Password Management (AAPM) capabilities that could easily scale to protect the massive Credit Suisse environment.
- Credit Suisse has deployed 65,000 A2A agents, which are protecting privileged communications and activities being performed by thousands of apps.
- Credit Suisse wants to expand this deployment to protect 1.2 million devices.

Our capabilities, scalabilities, performance and small footprint factored significantly in Credit Suisse's decision to select Symantec Privileged Access Management to protect their A2A Communications.

BROADCOM

Protecting Privileged Access at the Happiest Place on Earth

Customer Stories

With 12 theme parks, 52 resort hotels, and a top-rated cruise line, Disney is one of the world's leading providers of family travel and leisure experiences. Through the work of approximately 150,000 cast members, the magic of Disney comes to life for families and fans every day around the world.

The Business Challenge:

- Provide ultimate security to one of the world's most visible brands and create their parks-as-a-platform concept.
- Leverage same security platform on the Disney Cruise Lines, which has a particularly challenging environment as devices will have limited connectivity, infrastructure space is limited, and employees routinely use shared accounts.

Symantec Delivers:

- Protection for all privileged access functions, session recording and credential rotation of Windows Local & domain accounts as well as UNIX/Linux passwords & SSH keys within the Disney parks and cruise ships.
- API's that enabled Disney to build a custom and branded portal for their admins to use.

Our capabilities, performance and small footprint factored significantly in Disney's decision to select Symantec Privileged Access Management.

BROADCOM

Protecting Navy Federal Members is Symantec's Mission

Customer Stories

Navy Federal Credit Union (or Navy Federal) is the largest credit union in the United States with over $110.2 billion USD in assets, and 8.85 million members. Navy Federal was originally incorporated 1933 and only open to Navy employees, but has steadily opened its membership over the years.

NAVY FEDERAL Credit Union

The Business Challenge:

Navy Federal purchased CyberArk in 2013, but 3 things disrupted their progress:

- CyberArk required manual entry for Unix devices; they had hundreds of Unix devices
- The ongoing pricing to maintain the system was "out of control".
- Internal Audit told IT that they had to find a PAM solution that could properly support their entire enterprise.

Symantec Delivers:

Symantec PAM was the only solution that Navy Federal POC'ed because it offered:

- Lowest total cost of ownership with much smaller footprint than any of our competitors.
- Linux-based appliance model was preferred over the CyberArk Microsoft-based server model
- Symantec PAM

Navy Federal Credit Union selected the Symantec Privileged Access Management to Replace CyberArk to Reduce Operating Costs and Ease the Management of their Privileged Accounts.

BROADCOM

Securing at the speed of business with Symantec PAM

Customer Stories

United Parcel Service (UPS) is a global package delivery and supply chain management company, whose divisions include its cargo airline, freight-based trucking operation, and its delivery drone airline. UPS employees over 480,000 people and services over 200 countries.

The Business Challenge:

- UPS relies on digital services to give their customers unprecedented control of their deliveries and business logistics.
- Management of privileged identities was a top priority to help them pass audits.
- Additionally, UPS needed a solution that could span their distributed and mainframe environments.

Symantec Delivers:

- A solution to better control & monitor Privileged Users for better security and for Audit & Regulatory purposes.
- The ability to eliminate hard-coded usernames and passwords from mainframe scripts and jobs
- One of the easiest and quickest solutions to deploy and one that can scale to cover the 400,000 devices that UPS wants to protect.

Our ease of use, ease of implementation, scalability, and small footprint factored significantly in UPS's decision to select Symantec Privileged Access Management over CyberArk for their enterprise PAM solution.

BROADCOM

Thank You


BROADCOM®
connecting everything®

Thank you for downloading this Symantec solutions brief! Carahsoft is the reseller for Symantec Fed and Sled solutions available via Navy BPA, DIR-TSO, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Symantec's solutions, please check out the following resources and information:

For additional resources:
carah.io/Symantec-resources

For upcoming events:
carah.io/Symantec-webinars

For additional BlackBerry solutions:
carah.io/Symantec-remote-solutions

For additional FED and SLED solutions:
carah.io/Symantec-solutions

To set up a meeting:
symantecteam@Carahsoft.com
703-871-8539

To purchase, check out the contract vehicles available for procurement:
carah.io/Symantec-contracts