Navigating Toward Zero Trust - How To Pick A Platform

Colin Chisholm
Senior Manager, Security Architecture
Agenda

• Define Zero Trust and SASE.
• Review of Zebra Technologies and Current State.
• Discuss Zebra Technologies' Objectives and Goals.
• Walk through the major steps of two proof of concepts.
• Lessons Learned and Insights.

• This is a presentation on process and approach.
• NO vendor information.
Cat-veats

• All vendors have been replaced with randomly generated cat names
  https://thestoryshack.com/tools/cat-name-generator/

Herbie  Milo  Toffee
Nickels  Oliver  Dash
What is Zero Trust?

- **Zero trust** is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication—*not assumed trust*.

- A **zero trust** architecture follows the maxim "*never trust, always verify.*"

- Data, workflows, services, and such are protected by **software-defined micro-segmentation**.

What is SASE?

- Secure Access Software Edge (SASE) is a **framework** of multiple technologies to achieve the design goals of **Zero Trust**.

- **Essential Elements:**
  1. Software-defined wide area network (SD-WAN)
  2. Secure web gateway (SWG)
  3. Cloud access security broker (CASP)
  4. Firewall as a service (FWaaS)
  5. Zero trust network access (ZTNA)
  6. Centralized management

You likely have some, or many, of these components already in-place.

What is SASE (Secure Access Service Edge)? [https://www.zscaler.com/resources/security-terms-glossary/what-is-sase](https://www.zscaler.com/resources/security-terms-glossary/what-is-sase)

[https://accelerate-technologies.com/solutions/sase/](https://accelerate-technologies.com/solutions/sase/)
About Zebra Technologies
Fact Sheet

Zebra Technologies is an innovator at the edge of the enterprise with solutions and partners that enable businesses to gain a performance edge. Zebra’s products, software, services, analytics and solutions are used to intelligently connect people, assets and data to help our customers in a number of industries make business-critical decisions. These industries include:

- Retail and E-commerce
- Manufacturing
- Transportation and Logistics
- Banking
- Healthcare
- Public Sector
- Hospitality

With a rich history of innovation, Zebra is recognized as an industry leader in the following segments:

- #1 Enterprise Mobile Computing*
- #1 Barcode Scanning*
- #1 Specialty Printing*
- #1 RFID Reader & RFID Printing*
- A Leader in Workforce Management**
- A leader in Magic Quadrant for Indoor Location Services – Global***

Quick Facts

- Headquarters: Lincolnshire, Illinois, USA
- Stock Symbol: ZBRA (NASDAQ)
- Index listings: S&P 500, Information Technology and ESG Indices
- ROBO Global Robotics and Automation
- Fortune 1000 Ranking:
  - #596 in 2020
  - #607 in 2019
  - #628 in 2018

Products & Solutions

- Specialty Printing and Supplies
- Barcode Scanning
- Mobile Computing and Rugged Tablets
- RFID and Real-Time Location Systems (RTLS)
- Intelligent Workforce Management and Execution Solutions
- Data Services and Prescriptive Analytics
- Support, Managed and Professional Services
- Intelligent Automation Systems
Extensive Reach
Scalable to meet any enterprise demands

$5.6 billion global sales
128 offices across 55 countries
~5,300 patents US and INTL patents issued and pending
9,800 employees worldwide
10,000+ channel partners in over 180 countries
~10% of sales R&D*
  * $567 million

2021 data
A Commitment to Innovation

1969
- Founded as Data Specialties by Ed Kaplan and Gary Cless

1979
- First handheld laser barcode scanner

1991
- First laser-scannable 2D barcode

2004
- First rugged RFID handheld and first enterprise digital assistant (EDA)

2014
- Acquisition of Motorola Solutions’ Enterprise Business
- Becomes the official on-field player-tracking provider of the NFL

2015–2016
- Introduced Zebra DNA that embeds intelligence into mobile computers, printers and scanners; only migration path to modern OS for legacy Windows™ applications
- First all-touch Android™ inventory solution
- First Android-powered enterprise wearable computer

2017–2018
- Zebra Savanna™ First data intelligence platform

2019
- Acquisition of Cortexica, Profitect and Temptime

2020
- Acquisition of Reflexis Systems

2021
- Development of retail workforce software
- Introduced SmartSight™ intelligent automation system for retail
- Acquisition of Fetch Robotics, Adaptive Vision, and Antuit.ai
- Launched machine vision, fixed industrial scanning

Hardware-centric

Solution evolution

Solution and software-centric
Zero Trust / SASE Related History and Current State

<table>
<thead>
<tr>
<th>On-Prem</th>
<th>SaaS</th>
<th>SaaS</th>
<th>On-Prem</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Prem</td>
<td>Agent-to-the-cloud</td>
<td>Agent-to-the cloud</td>
<td>Agent and On-Prem VPN</td>
</tr>
<tr>
<td>URL Filtering (.pac files)</td>
<td>Secure Web Gateway (SWG)</td>
<td>Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG)</td>
<td></td>
</tr>
</tbody>
</table>

- **Herbie**: ~2015 - 2017
- **Nickels**: 2017 - 2018
- **Milo**: 2018 - Present
- **Oliver**: ~2005 - Present
Step 1

Obtain an Executive Sponsor
Step 2

Assemble a team of stakeholders

https://www.marvel.com/movies
Step 3

Define Objectives
Zebra’s Zero Trust / SASE Objectives

Reduce the attack surface
  • Remove internet-facing assets from the public.

Reduce risk to the corporate network
  • Remove direct VPN access from workstations, cloud-gapping malware from internal network.

Reduce risk for remote users
  • Encrypt all user traffic (no split-tunnel).

Reduce risk of data loss
  • Data Protection policies and SSL/TLS termination.

Improve user experience
  • “Always-On” replacement for legacy VPN.
Zebra’s Zero Trust / SASE Objectives

Ease integration of acquisitions prior to site standardization
  • Provide access to Zebra assets from new M&As.

Reduce risk of malware
  • SSL/TLS decryption to detect malware in-flight.

Reduce risk related to device non-conformance
  • Posture assessment for managed workstations prior to internal access (e.g. VPN replacement).

Improve ability to pursue micro-segmentation
  • Combine authorization data in IGA tool with control layer in SASE to limit access to pre-authorized users.
Step 4

Define Use Cases
Zebra Use Case Approach

• Project Team developed 70+ use cases.
• Use Cases were vendor-agnostic and aspirational.
• Did not incorporate budget or schedule.
• Limited use of specific technologies (except for integrations).
• Use cases followed the defined Objectives.
• Business and Technical considerations helped shape or define some use cases
• Many mergers and acquisitions = M&A Use Cases
Zebra Use Case Categories

• Cloud Access Security Broker (CASB)
• Firewall-as-a-Service (FWaaS)
• Integrations
• Mergers and Acquisitions (M&As)
• Secure Web Gateway (SWG)
• Software Defined Perimeter
• Software-Defined Wide Area Network (SD-WAN)
• Zero Trust Network Access (ZTNA)
• Other
Zebra Use Case Objectives

Adblocking & Tracking
API, SaaS, and IaaS
Application ID
Automate Security Health
Monitoring
Block Categories
Block URL/Domain
Certificate-Pinned Exceptions
Cloud App Classification
Cloud Application Definitions
Cloud Security Posture Management (CSPM)
Cloud/Internet Firewalls
Decrypt Data (e.g. SSL Termination)
Dedicated Proxy IP
DLP
DLP - Integration with MIP
Fail-over
"First Packet" and QoS

"First Packet" and Security Policy
Forward Proxy and Reverse Proxy
FWaaS Integration
Geofencing Policies
Integration with PAM
Integration with Threat Intelligence
Integration with EDR
Integration with SIEM
Integration with SSO
Integration with Email Security
Integration with IGA
Integration with Security Operations
Integration with SOAR Platform
Integration with Vulnerability Management
Integration with Threat Intelligence
Integration with Ticketing
International POPs
IoT security and visibility
Malware

Micro-Segmentation
Multiple OS Test
NGFW Parity
Financial Cloud Integration
Orchestration
Out-of-Box Rules
Peering Relationships with Major Providers
Posture Checks
Private Cloud Networks
Sandbox
SASE Integration with SD-WAN
SD-WAN Validation
Secure Connection Location
Software firewall forensics
Source-to-Destination Analysis
Transition Network Replacement
URL Filtering
User ID
VPN Replacement
Step 5

3rd Party Research and/or Guidance
Research the Market

- With Objectives, Goals, and Use Cases in-hand, research the market.
- Who are the vendors in the marketplace?
- Do they offer capabilities in-line with your Objectives, Goals, and Use Cases?
- Research their product pages.
- Conduct meetings with their sales teams.
- Independent research from technology and research organizations.
- Community discussion sites.
- Collaborate with your peers and colleagues.
- Attend security presentations (like this one!)
Step 5

Define Key Implementation Goals
Zebra Zero Trust Key Goals

- Replace **Oliver** (legacy VPN) with an “always-on” alternative.
- Replace **Milo** (CASB, SWG, and CSPM)
- Device posture inspection for access to internal resources.
- Full port/protocol encapsulation and inspection.
- SSL Inspection + Data Protection rules.
- Restrict access to internet hosted applications from unmanaged devices (IP Source Anchoring).
- M&A Integrations.
Step 6

Define the Impact on End-Users
Step 7

Conduct the POC
Proof of Concept Process (2021)

**September-October 2021**
- RFPs and discussions with four vendors (September-October).
- **Toffee** and **Dash** were short-listed as final candidates.
- A 70-item use case list was leveraged across nine (9) categories and three (3) levels of criticality.

**November 2021**
- Toffee POC

**December 2021**
- Dash POC

**January 2022**
- Final decision

Use Cases  
Design  
Implementation  
Testing  
Scoring
Step 8

Scoring the POC (Quantitative)
# Zero Trust SASE Objectives & Use Case Scoring

<table>
<thead>
<tr>
<th>Board Objective</th>
<th>Toffee High Priority (39 Use Cases)</th>
<th>Dash High Priority (39 Use Cases)</th>
<th>Toffee Medium Priority (26 Use Cases)</th>
<th>Dash Medium Priority (26 Use Cases)</th>
<th>Toffee Low Priority (17 Use Cases)</th>
<th>Dash Low Priority (17 Use Cases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the attack surface (2 use cases)</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Reduce risk to the corporate network (26 use cases)</td>
<td>14</td>
<td>10</td>
<td>12</td>
<td>7</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>Reduce risk for remote users (4 use cases)</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>9</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Reduce risk of data loss (6 use cases)</td>
<td>9</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Improve user experience (11 use cases)</td>
<td>11</td>
<td>26</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Ease M&amp;A Integrations (1 use case)</td>
<td>1</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Reduce risk of malware (4 use cases)</td>
<td>n/a</td>
<td>n/a</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Reduce risk related to device non-conformance (4 use cases)</td>
<td>10</td>
<td>9</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Improve ability to pursue micro-segmentation (11 use cases)</td>
<td>9</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total Scores</strong></td>
<td>63</td>
<td>68</td>
<td>30</td>
<td>25</td>
<td>20</td>
<td>30</td>
</tr>
</tbody>
</table>

**Scoring Legend per Use Case**

- 3 = Pass
- 2 = Pass (but not ideal)
- 1 = Fail
- 0 = Not Tested
## Zero Trust SASE Objectives & Use Case Scoring

<table>
<thead>
<tr>
<th>Board Objective</th>
<th>Toffee High Priority (39 Use Cases)</th>
<th>Dash High Priority (39 Use Cases)</th>
<th>Toffee Medium Priority (26 Use Cases)</th>
<th>Dash Medium Priority (26 Use Cases)</th>
<th>Toffee Low Priority (17 Use Cases)</th>
<th>Dash Low Priority (17 Use Cases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce the attack surface (2 use cases)</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Reduce risk to the corporate network (26 use cases)</td>
<td>14</td>
<td>10</td>
<td>12</td>
<td>7</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>Reduce risk for remote users (4 use cases)</td>
<td>9</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Reduce risk of data loss (6 use cases)</td>
<td>3</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Improve user experience (11 use cases)</td>
<td>11</td>
<td>26</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Ease M&amp;A Integrations (1 use case)</td>
<td>1</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Reduce risk of malware (4 use cases)</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Reduce risk related to device non-conformance (4 use cases)</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Improve ability to pursue micro-segmentation (11 use cases)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total Scores</strong></td>
<td>63</td>
<td>68</td>
<td>30</td>
<td>25</td>
<td>20</td>
<td>30</td>
</tr>
</tbody>
</table>

### Scoring Legend

- **3 = Pass**
- **2 = Pass (but not ideal)**
- **1 = Fail**
- **0 = Not Tested**

**Active engagement from stakeholders on this scoring is crucial**

**POC should be long enough to test all use cases, especially Medium and Low Priority**

**Scoring should be a wider range for more nuance and fidelity**
Step 9
Scoring the POC (Qualitative)
## SASE Solution – Tangible and Intangible Comparison

<table>
<thead>
<tr>
<th>Objective</th>
<th>Toffee</th>
<th>Dash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posture Checking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Tool Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Tool Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M&amp;A Flexibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Layer Firewalling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated Public IPs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CASB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSPM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>China Connectivity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Experience Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Decryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend**
- Meets All Needs
- Meets Some Needs
- Meets No Needs
Step 10
Retrofit Missed Use Cases
Step 11

Lessons Learned
Lessons Learned & Guidance

• More Time = Better POC.
• Objectives, Goals, and Use Cases are your roadmap.
• Network Performance – Test with a cross-section of your users.
• It’s a marathon, not a sprint. You’re not going to implement everything at once. Plan for a crawl > walk > run evolution.
• Objectives, Goals, and Use Cases are your roadmap.
• Stakeholder engagement is essential.
• Integrations - Be aware of current and future integration capabilities (e.g. SD-WAN).
• Request conversations with the vendor’s customers.
• User experience should be top-of-mind.
• Legal Approval for any monitoring capabilities (e.g. SSL Decryption).
• Deal Making – Vendor Professional Services and Training Credits.
Final Decision and Key Benefits – Dash!

**Strengths**

**Network**
- Superior network performance against **Oliver** (legacy VPN) for both internal and cloud resources.
- IP overlap flexibility
- China deployment architecture
- Flexible architecture for supporting cloud-based connectivity

**Security**
- No-effort SSL Termination and Analysis.
- Strong integration with EDR, SIEM, and Threat Intelligence tools (and others)
- Equivalent CASB and Security Web Gateway performance as **Milo**.
- Strong out-of-box reporting and templates.

**Challenges**

**Network**
- Complex network and security policy design requires additional administrative overhead.
- Geolocation based policies require complex configurations.
- Some geolocation functionality is dependent on IAM functionality.
- Does not offer true application based (layer 7) firewalling
- Does not supply dedicated public IPs for SWG.

**Security**
- Posture checking functionality is limited.
- Inline malware analysis not available for VPN replacement.
- Data Protection capabilities are limited compared to existing solution (**Milo**).
Questions