BUILDING A ZERO TRUST PROGRAM ON A SOLID PLATFORM

• CSTS 2019 Bonn | 13th-14th March 2019

• Ingo Kruckewitt, Symantec
Agenda

1. Introduction to Zero Trust
2. Extended Ecosystem Model
3. Where to Start
4. Platform vs. Fragmentation
5. Symantec Platform Alignment
6. Q&A
Introduction

Zero Trust Security

• Popularized by Forrester nearly a decade ago
  o Challenged existing perimeter-based security strategies
  o Promoted a concept of “Default Deny”; allowing only Least Privileged Access
  o Network-centric

• Zero Trust has grown in its scope and definition
  o Evolved beyond network
  o Addresses new threats and compliance requirements
  o Becoming a practical framework capable of guiding security practitioners across all IT areas
Introduction

Forrester Zero Trust eXtended (ZTX) Ecosystem Model

Forrester states the model’s goal is to:

• Strengthen data security
• Limit the risks associated with excessive user privileges and access
• Improve security detection and response with analytics and automation
Forrester ZTX Model
Zero Trust eXtended (ZTX) Ecosystem Model

Requires an organization to rethink security approach

6 key interrelated areas to consider
Data

Key Zero Trust Capabilities to Consider

- Visibility of data on all channels and repositories; SaaS, IaaS, network, data center, endpoints, mobile
- Protection with encryption, classification, and integrations with communication control points; endpoint, email, cloud, and web
- Visibility by building a perimeter around the data with identity, and user behavior

Securely managing corporate and customer data, classifying and categorizing it correctly, and ensuring sensitive information is encrypted at rest and in transit are key pieces of a Zero Trust approach.
Networks

The Zero Trust network starts with enforcing limited access to the resources that exist in it. The network must be segmented, with sensitive resources being isolated and strictly controlled.

**Key Zero Trust Capabilities to Consider**

- Least-privileged granular access controls, such as Software Defined Perimeters (Zero Trust Access)
- Ability to segment networks, isolating key resources, and apply controls limiting access to segments
- Watch encrypted network traffic “blind spots” – ensure full visibility on encrypted traffic
Workloads

All of the Zero Trust controls you have in-place securing on-premises apps and resources need to be in place for cloud workloads as well, especially those running in public clouds.

Key Zero Trust Capabilities to Consider
• Centralized policies for security, visibility, and compliance across major IaaS platforms
• Control access to, and communications between, sensitive apps, workloads, and containers
• Enforce malware protection, perform vulnerability assessments and compliance checks, and enforce data protection controls
Every Zero Trust strategy must take devices into account, and Security teams must be able to isolate, secure, and control every device on the network at all times.

Key Zero Trust Capabilities to Consider
• Protect endpoint against advanced threats
• Verify device integrity and securely connect devices to sensitive applications and data
• Apply controls to monitor behavior and ongoing device health checks
People’s interaction with the Internet impacts any organization’s Zero Trust strategy. Users must be continually authenticated, and acceptable use policies and access privileges must be strictly enforced.

Key Zero Trust Capabilities to Consider

- Application-specific access, with multi-factor authentication
- Context-aware access – considers posture changes
- Tools enforcing acceptable web/app use policies; isolation of risky web sessions; inspection of encrypted traffic
- Same for email
Analytics (Visibility) and Automation

The ability to capture and analyze network and device traffic to look for threats and malicious activity is key. Technologies that provide automated policy-based actions across multiple technologies improve security outcomes.

Key Zero Trust Capabilities to Consider
- Incorporate User Behavior Analytics across data and threat protection products
- Correlate information from all existing infrastructure for analytics and IR
- Apply technology for automated policies that increase overall security posture and reduce human error
OK, I’m In...
Where Do I Start?
ZT Starts with a Well Defined Strategy/Mission

Strategy Links to Capabilities, Technologies, and Features

- Define ZT Strategy
- Prioritize Capabilities
- Identify Specific Technologies
- Highlight Any Specific Feature Requirements

Broad – “We are committed to moving to a ZT architecture”

Narrow (Access) – “We want to enforce limited application access based on identity”
Narrow (Data) – “All sensitive data uploaded to SaaS Apps will be encrypted”
Example - Zero Trust

Uploading Content to a SaaS Application

1. Connect to Cloud Proxy
2. Authenticate the connection
3. Validate user access to cloud application
4. Inspect document upload for sensitive material
5. Encrypt document due to sensitivity
6. Document uploaded into cloud app
7. Content is classified and tagged inside of cloud app
8. Email sent to user confirming document receipt
9. Threat inspection performed on email content
10. Full packet capture forensics
11. Endpoint activity telemetry

COMPLICATIONS OF CLOUD ADOPTION
Secure Access Cloud

Zero Trust Application Access in the Cloud Generation

Securely connect any user from any device

To any corporate application

In the cloud / On-premises
Without provisioning VPN, DMZ
Without managing endpoint agents

Zero Trust Access - trust is continuously verified; access is limited
How It Works
Zero Trust Based Application Access

Secure Access Cloud

- DEPLOY CONNECTORS & CONNECT TO SECURE ACCESS CLOUD
- AUTHENTICATE USER
- VALIDATE DEVICE HEALTH
- POINT-TO-POINT ACCESS
- MONITOR & LOG ACTIVITIES
- CONTEXTUAL PREVENTION
- APPLICATION LAYER

Agentless

EMPLOYEE
AFFILIATE
CHAIN PARTNER
CONTRACTOR
B2B PARTNER
B2C CUSTOMER

DEPLOYS IN MINUTES
Secure Access Cloud Benefits

**SIMPLE**
- Increased speed to market
- Accelerated cloud adoption
- Seamless user experience
- Agentless

**SECURE**
- No lateral movement
- Continuous user action governance
- Reduced network attack surface

**COST EFFECTIVE**
- No additional infrastructure
- User based pricing
- No hidden costs
Platform vs Fragmentated Approach

Benefits of a ZTX Platform

- Integrations Deliver Improved Security Outcomes
- Reduction of Operational Complexity
- Better Visibility & Audit/Compliance
- Simplifies Automation and Orchestration
- Streamlines Sourcing & Vendor Management
Symantec Integrated Cyber Defense

Simplified Security Model Enabling Zero Trust Security Outcomes
Integrated Cyber Defense and Zero Trust

**DATA**
- Data Loss Prevention
- Data Encryption, Tagging, and Analytics
- Device Encryption

**WORKLOADS**
- Cloud Workload Protection
- Storage Protection
- Cloud Security Gateways (CASB)
- Compliance Automation
- WAF/Reverse Proxy

**NETWORK**
- Software Defined Perimeter
- Cloud Proxy & SD-WAN/Firewall
- Data Center Security
- Proxy, Reverse Proxy, & WAF
- Encrypted Traffic Management

**DEVICES**
- Endpoint Protection and Management
- IoT Security
- Data Center Security

**WORKFORCE / PEOPLE**
- Multi-Factor Authentication
- Web & Email Gateways
- Web Browser Isolation
- Content Analysis and Sandboxing
- Cloud Security Gateway (CASB)

**AUTOMATION & ANALYTICS**
- Data-Driven Analytics/Reporting
- Ueba
- Full-Packet Capture Forensics
- Endpoint, Network, Cloud, Email Reporting & Threat Analytics
<table>
<thead>
<tr>
<th>Partners Inquiries</th>
<th>Technology Partners</th>
<th>Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000+</td>
<td>116</td>
<td>200+</td>
</tr>
</tbody>
</table>

**Symantec TIP Program**

**Symantec TIP Program: ELITE**
- Amazon Web Services
- Bay Dynamics
- Box
- IBM
- Microsoft
- Splunk
- ServiceNow

**Symantec TIP Program: PREMIER**
- Cisco
- cyberO:SERVER
- Demisto
- Dropbox
- FireEye
- ForeScout
- Fortinet
- Gemalto
- Google
- Hitachi
- Lastline
- Oracle
- Radware

**Symantec TIP Program: ACCESS**
- A10
- Aashio
- Accellion
- Aella Data
- AGARI
- AGAT
- Allure
- Anomali
- Area 1
- Aryaka
- Attivo
- Aviatrix
- Aviary
- ATLAS
- Boldon James
- Cellebrite
- Ciscar
- Citrix
- Cylance
- Cyberoam
- Cybrary
- Dell EMC
- Docker
- Dradient
- Echoworx
- Egger
- ESET
- Enjin
- F5
- Fastly
- Fronius
- Gauss
- HPE
- Hewlett Packard Enterprise
- Ixia
- JASK
- Jamf
- McAfee
- Meta Networks
- Micro Focus
- N3
- Naver
- Napatech
- NetApp
- NetScout
- NetDialog
- Nuance
- Okta
- OpenText
- Opsware
- PatienceKeeper
- Pulse Secure
- Qualys
- Red Hat
- Reversing Labs
- RSA
- Safety
- Salesforce
- Security
- ServiceNow
- SfN
- Sequrionix
- Siemens
- Simplify
- Silver Peak
- Sophos
- SWIMLANE
- Symantec
- Symphony
- Thales
- Thycotic
- TiMUS
- Tufin
- Valarmail
- Varnish
- VERA
- Veritas
- VERSA
- VMware
- WhiteHat Security
- Zerofix
Symantec Named a Leader in the Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

“Symantec is a juggernaut, given its breadth of security solutions. The company has extensive endpoint, network security, and threat identification capabilities”

- The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

FORRESTER

Source: November 2018, The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester’s call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.
Data Detection and Protection in The Cloud

Data protection must be consistent across all channels

- **Endpoint**
- **Storage**
- **Network**

Cloud

- **SaaS/IaaS**
  (AWS, Box, OneDrive, SFDC...)

- **Web**
  (LinkedIn, Facebook, Twitter...)

- **Email**
  (O365, Gmail)

DATA DETECTION AND PROTECTION

- **Cloud Access Security Broker**
- **Secure Access Cloud**
- **Web Gateways**
- **Email Security**

Detection in the cloud  All control points  Single pane of glass  Mobile & BYOD
THANK YOU

- CSTS 2019 Bonn | 13th - 14th March 2019
- Ingo Kruckewitt, Symantec