ZERO TRUST
DATA PROTECTION

Bob Gilbert, VP & Chief Evangelist, Netskope
Circa 1983 – My first cyber security experience

Ran a Bulletin Board System (BBS) that hosted software

Developed a whitelist terminal program (assembly + Pascal) to keep out the hackers that wiped out my site

Commodore 64, 1200bps modem, 5.25in floppy storage
Charlie Ciso

We’ve implemented zero trust.

I don’t believe you.

Exactly.
Zero trust is the ability to continuously assess the context of various conditions to enable adaptive risk-based decision making.
What is a Zero Trust concept?

Zero Trust is an Architectural principle with one main purpose:

**Removal of Implicit Trust**
Zero Trust is:

- A business enabler
- A marriage of process & technology
- A reduction of complexity strategy
- Data and context centric
- Contextual and dynamic in nature
Zero Trust is not:

- A quick win
- A packaged product
- Only for identity or network tech
- An idea where all trust is removed
- A one-off or IT only centric project
- A Next-Gen perimeter
SASE (Secure Access Service Edge)

The delivery mechanism for Zero Trust
Digital Transformation Forcing a Tech Shift

Yesterday

Today

SaaS use has increased
2400+ cloud apps used by average enterprise

Data is everywhere
90% of all data has been created within the past 2 years

Remote users will continue to work from anywhere
82% of company leaders plan to allow remote work some of the time
Digital Transformation and remote workers are driving major changes in network traffic leaving you blind to the network traffic

Network Traffic

- Digital transformation is shifting network load to internet
- Remote workers change the pattern of network traffic
- Controls need to follow the data
APPLICATIONS

EXTERNAL APPS (SAAS & WEB)

EXTERNAL APPS (SAAS & WEB)

INTERNAL APPS (DATA CENTER / IAAS)

WORK FROM ANYWHERE, BYOD, THIRD PARTY

HQ AND BRANCH

USERS
How do we *rationalize* this?
**Security Transformation**

**Requirements**
- Data protection
- Threat protection
- Visibility / Risk
- Compliance
- Zero trust
- Context

**Technology**
- CASB
- SWG
- EDR
- DLP
- AI/ML
- UEBA

**Network Transformation**

**Requirements**
- App performance
- 99.999%
- Resilience
- TCO
- User experience

**Technology**
- ZTNA
- SD-WAN
- SWG
- FW
- Intelligent Routing

---

**EXTERNAL APPS**
(SAAS + WEB)

**APPLICATIONS**

**INTERNAL APPS**
(DATA CENTER / IAAS)

**DATA**

**SECURE**

**ACCESS**

**WORK FROM ANYWHERE, BYOD, THIRD PARTY**

**HQ AND BRANCH**
APPLICATIONS

EXTERNAL APPS (SAAS + WEB)

INTERNAL APPS (DATA CENTER / IAAS)

WORK FROM ANYWHERE, BYOD, THIRD PARTY

HQ AND BRANCH

?
Applications

External Apps (SAAS + WEB)
- Single Agent, Single Console
- Single Pass

Internal Apps (DATA CENTER / IAAS)
- Highly Performant, Peered Security Cloud Network

Work From Anywhere, BYOD, Third Party

HQ and Branch Office Locations

SASE
- Single Agent, Single Console
- Single Pass
- Highly Performant, Peered Security Cloud Network

Users
Starting on a Zero Trust Journey
### What to Consider Before Implementing Zero Trust:

<table>
<thead>
<tr>
<th>You must architect with your business in mind first</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand your technology stack, process, and capability gaps</td>
</tr>
<tr>
<td>Understand your threats and risk</td>
</tr>
<tr>
<td>Understand your end user requirements (transparency, ease of use, availability, etc.)</td>
</tr>
</tbody>
</table>
A Path to Implement Zero Trust Principles:

- Understand your information assets by both sensitivity and criticality
- Understand the user population that requires access
- Identify applications that you want to expose first - start with low risk applications and determine what will give the biggest value return
- Understand and start grouping key business user populations and core application combinations
A Path to Implement Zero Trust Principles:

Begin defining business rules for access - Starting with coarse grained controls first using hierarchy of information asset ratings

Define differentiated controls for high risk users – overlaying these additional controls as you work through the user population

Implement controls into the form of policies that can be applied within the relevant technology platform(s)

Revoke access to previous VPN/RAS services when users have been fully on-boarded
Zero Trust Data Protection Architecture

Continuous evaluation throughout the session

More telemetry – More CONTEXT

Inline Inspection

Next transaction

Inline Policy Enforcement

Risk Engine

Permit
Deny
Restrict

Risk based adaptive policy for authorization

Data
Identity
Application
Endpoint
Behavior
Network

24
<table>
<thead>
<tr>
<th>Trust</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Activity</td>
<td>Non-Sensitive Data (Read Only)</td>
<td>Non-Sensitive Data (Read &amp; Write)</td>
<td>Limited Sensitive Data (Read)</td>
<td>Sensitive Data (Read &amp; Write)</td>
<td>Sensitive Data (Read &amp; Write &amp; Store on Device)</td>
</tr>
<tr>
<td>Identity</td>
<td>Limited Access Validation</td>
<td>Multifactor Authentication</td>
<td>Multifactor Authentication</td>
<td>Time Based Multifactor Authentication</td>
<td>Event Based Multifactor Authentication</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Unmanaged Device</td>
<td>Unmanaged Device</td>
<td>Unmanaged Device</td>
<td>Unmanaged Device</td>
<td>Managed Device</td>
</tr>
<tr>
<td>Application</td>
<td>Unsanctioned App</td>
<td>Unsanctioned App</td>
<td>Sanctioned App</td>
<td>Sanctioned App</td>
<td>Sanctioned App</td>
</tr>
<tr>
<td>Example</td>
<td>Social Media</td>
<td>Google Drive, Box, Office365</td>
<td>Confidential Reports</td>
<td>Email</td>
<td>HR Data, Board Materials, Large Database</td>
</tr>
</tbody>
</table>
Benefits of Zero Trust

Zero trust *drastically* decreases an organization’s risk posture

- **Prevention of lateral movement**
- **Predefined application/resource access governance**
- **Provide conditional/least privileged access only**
- **Gain massive visibility and control within your ecosystem**
- **Enables the ability for risk-based decision making at scale**
5-step Zero-Trust Implementation Strategy

**Discover**
Understand your unique organizational needs – assets, users, apps

- 1. Understand your assets by criticality and sensitivity
- 2. Understand the user population access needs

**Protect**
Implement technology and policies to enable continuous risk assessment

- 3. Identify priority applications – risk or consumption driven
- 4. Understand and start grouping key user populations and core application combinations
- 5. Start with coarse grained controls first and refine over time
- 6. Implement these into enforceable policies that can be applied
- 7. Add differentiated controls to the user population
- 8. Revoke access to previous VPN/RAS services when users have been on-boarded into above
- 9. Report exposure to data owners
- 10. Identify broken business processes
- 11. Report on cloud security program and measure risk buy-down improvements
- 12. Continually look for changes to profile or new high-risk issues – continuous policy refinement

**Govern**
Govern services and data through continuous assessment

- 1. Understand your assets by criticality and sensitivity
- 2. Understand the user population access needs
- 3. Identify priority applications – risk or consumption driven
- 4. Understand and start grouping key user populations and core application combinations
- 5. Start with coarse grained controls first and refine over time
- 6. Implement these into enforceable policies that can be applied
- 7. Add differentiated controls to the user population
- 8. Revoke access to previous VPN/RAS services when users have been on-boarded into above
- 9. Report exposure to data owners
- 10. Identify broken business processes
- 11. Report on cloud security program and measure risk buy-down improvements
- 12. Continually look for changes to profile or new high-risk issues – continuous policy refinement

**Prioritize**
Prioritize findings and align with business requirements

**Educate**
Safely enable services across the enterprise

Deliverables
1. Understand your assets by criticality and sensitivity
2. Understand the user population access needs
3. Identify priority applications – risk or consumption driven
4. Understand and start grouping key user populations and core application combinations
5. Start with coarse grained controls first and refine over time
6. Implement these into enforceable policies that can be applied
7. Add differentiated controls to the user population
8. Revoke access to previous VPN/RAS services when users have been on-boarded into above
9. Report exposure to data owners
10. Identify broken business processes
11. Report on cloud security program and measure risk buy-down improvements
12. Continually look for changes to profile or new high-risk issues – continuous policy refinement
Zero Trust Maturity

STAGE 0 – Initial
1. No device info & visibility
2. No consolidated identity store
3. No real-time threat updates
4. No knowledge of app risk
5. No data classification
6. Passwords used for authentication

STAGE 1 – Telemetry
1. Device visibility
2. Consolidated identity store
3. Real-time threat updates
4. Fixed policy authorization at session initiation
5. SIEM in place but not linked to processes
6. Simple multi-factor authentication for most critical applications

STAGE 2 - Reactive
1. Understanding of the application risk
2. Step-up authorization & multi-factor authentication or higher risk sessions
3. End user risk groupings
4. Data classification
5. Some telemetry used to force reauthorization updates such as time
6. Telemetry gathered and sent to central repository
7. Capabilities for security direct to internet and private applications

STAGE 3 - Optimized
1. User Behavior Monitoring
2. Telemetry from multiple sources are used for risk decision making in real time
3. Continuous evaluation of telemetry resulting in adaptive policy
4. Seamless access for end-users
Our Next “New Normal” in Cyber Security

Traditional
- Single factor authentication
- On-premise devices
- Private network
- VPN
- MSPs

Hybrid
- MFA
- Managed devices
- Private and public cloud
- Virtualization

Zero-Trust
- Zero trust
- Contextual authentication
- User Behavior Analytics

Secure Access Service Edge
- Software defined perimeter
- Pure policy-based security
- Entity Behavior Analytics

Bound to Fail

Current & Future Architecture

How are you transitioning back and what is your new normal?
Live Demo of 10 Common Zero Trust Scenarios
Bob in marketing needs browser access to internal LMS app

Frank, a sysadmin, needs SSH access to internal LMS app

Zero Trust access to Internal App Hosted in AWS

Concern: Bad actors gain access and move laterally
**Scenario 1:** A member of the marketing team, Bob needs browser access to his company’s internal Learning Management System that is hosted in AWS

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>Port/Protocol</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser access to LMS app</td>
<td><a href="mailto:bob@bobsbank.net">bob@bobsbank.net</a> is in the marketing group</td>
<td>Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled</td>
<td>Access to port 80,443</td>
<td>Bob is granted browser access to the internal LMS app</td>
</tr>
</tbody>
</table>

**Old way:** Make app publicly accessible or provide VPN access, enabling Bob to move laterally
**Scenario 2:** A member of the Sysadmin team, Frank needs SSH access to his company’s internal Learning Management System that is hosted in AWS

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>Port/Protocol</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH access to LMS app</td>
<td><a href="mailto:frank@bobsbank.net">frank@bobsbank.net</a> is in the sysadmin group</td>
<td>Frank is using a managed laptop with encryption and CrowdStrike endpoint enabled</td>
<td>SSH, requiring access to port 22</td>
<td>Frank is granted SSH access to the internal LMS app</td>
</tr>
</tbody>
</table>

*Old way:* Make app publicly accessible or provide VPN access, enabling Frank to move laterally
Finance team needs access to social media so they can follow companies.

Marketing team needs full access to social media so they can post, retweet, and comment as part of social campaigns.

Concern: FINRA compliance

Zero Trust data protection when using social media.
### Scenario 3: Social media is blocked company-wide because of FINRA compliance, but Finance team needs view-only access to get their job done

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity (<a href="mailto:adele@bobsbank.net">adele@bobsbank.net</a> is a member of the finance group)</th>
<th>Device (Adele is using a managed laptop with encryption and CrowdStrike endpoint enabled)</th>
<th>App (App: Twitter, Cat: Social, App Risk: Low)</th>
<th>Activity (Login View)</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adele in finance is attempting to view social media posts</td>
<td>Adele is granted view access to social media apps</td>
<td></td>
<td></td>
<td></td>
<td>Adele is granted view access to social media apps</td>
</tr>
<tr>
<td>Post to Twitter</td>
<td>Post</td>
<td>Post</td>
<td>Post</td>
<td>Post</td>
<td>Adele is blocked from posting to Twitter</td>
</tr>
</tbody>
</table>

**Old way:** Block social media outright or face risk of FINRA violation
**Scenario 4:** Social media is blocked company-wide because of FINRA compliance, but Marketing team needs full access to get their job done.

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Data</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob in Marketing is attempting to post to Twitter</td>
<td><a href="mailto:bob@bobsbank.net">bob@bobsbank.net</a> is a member of the marketing group</td>
<td>Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled</td>
<td>App: Twitter</td>
<td>Activity: Post</td>
<td>Data: Opinion about NCAA bracket</td>
<td>Bob is granted access to social media apps and can post to Twitter</td>
</tr>
<tr>
<td>Bob in Marketing is attempting to post sensitive data to Twitter</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>Data: stock recommendation</td>
<td>...</td>
</tr>
</tbody>
</table>

*Old way: Block social media outright or face risk of FINRA violation*
Zero Trust data protection when using risky cloud apps

**Concern:** Data loss and malware

Bob in marketing wants access to a popular cloud storage app so he can quickly upload and share data.
**Scenario 5:** Bob wants to access a popular cloud storage app so he can quickly upload and share data.

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
</table>
| Bob in Marketing is attempting to access Zippyshare | bob@bobsbank.net is a member of the marketing group | Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled | App: Zippyshare  
Cat: Cloud Storage  
App Risk: High | Login | Bob is blocked from accessing Zippyshare and is redirected to OneDrive install page |

**Old way:** Blunt force blocking of cloud apps
Zero Trust data protection for risky users

Concern: Data loss/theft

Adele’s contract with the company is ending and she wants to download data from the company OneDrive
**Scenario 6:** Adele’s contract with the company is ending and she wants to download data from the company OneDrive

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
</table>
| Adele, a contractor, is attempting to download and share data in OneDrive | adele@bobsbank.net is a contractor | Adele is using a managed laptop with encryption and CrowdStrike endpoint enabled | App: O365 OneDrive  
Cat: Cloud Storage  
App Risk: Low | Download | Adele is blocked from downloading data from OneDrive |

*Old way: Coarse-grained access controls*
Zero Trust data protection for unintentional or unapproved data movement between cloud apps

Concern: Data loss

Bob wants to download data from the corporate Office 365 OneDrive account and upload it to his personal instance of O365 OneDrive.
**Scenario 7:** Bob wants to download data from the corporate Office 365 OneDrive account and upload it to his personal instance of O365 OneDrive

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Data</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob in marketing is attempting to download data from OneDrive</td>
<td><a href="mailto:bob@bobsbank.net">bob@bobsbank.net</a> is a member of the marketing group</td>
<td>Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled</td>
<td><strong>App:</strong> O365 OneDrive</td>
<td><strong>Instance:</strong> Corporate</td>
<td><strong>Cat:</strong> Cloud Storage</td>
<td>Low</td>
</tr>
<tr>
<td>Bob in marketing is attempting to upload confidential data to OneDrive</td>
<td>***</td>
<td>***</td>
<td><strong>App:</strong> O365 OneDrive</td>
<td><strong>Instance:</strong> Personal</td>
<td><strong>Cat:</strong> Cloud Storage</td>
<td><strong>App Risk:</strong> Low</td>
</tr>
</tbody>
</table>

*Old way:* Block Office 365 instances!
Zero Trust data protection when sharing, posting, creating, editing data in cloud apps

Bob wants to share his credit card info in Slack and in the company’s O365 OneDrive account so his team can use it to buy marketing schwag

Concern: Data loss
**Scenario 8:** Bob wants to share his credit card info in Slack and in the company’s O365 OneDrive account so his team can use it to buy marketing schwag

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Data</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob in marketing is attempting to post credit card data to a public Slack channel</td>
<td><a href="mailto:bob@bobsbank.net">bob@bobsbank.net</a> is a member of the marketing group</td>
<td>Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled</td>
<td>App: Slack&lt;br&gt;Instance: Public&lt;br&gt;Cat: Collaboration&lt;br&gt;App Risk: Low</td>
<td>Post</td>
<td>PCI</td>
<td>Bob's Post activity in Slack is blocked</td>
</tr>
<tr>
<td>Bob in marketing is attempting to edit content in OneDrive and paste in credit card data</td>
<td>⬤ ⬤ ⬤</td>
<td>⬤ ⬤</td>
<td>App: O365 OneDrive&lt;br&gt;Instance: Corporate&lt;br&gt;Cat: Cloud Storage&lt;br&gt;App Risk: Low</td>
<td>Edit</td>
<td>PCI</td>
<td>Bob's edit activity in O365 OneDrive is blocked</td>
</tr>
</tbody>
</table>

*Old way: Block Slack*
Adele, a contractor, wants to download data from the company's Box account to her personal laptop.

**Concern:** Data loss via device not managed by IT and malware coming from unmanaged device.

**Zero Trust data protection for unmanaged devices**
# Scenario 9: Sensitive data downloaded from the corporate Box account to a device not managed by IT

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Data</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adele is a contractor and is attempting to download the latest presentation from Box to her personal device</td>
<td>Adele is a contractor</td>
<td>Adele is using a device not managed by IT</td>
<td>App: Box</td>
<td>Download</td>
<td>benign pptx</td>
<td>Adele's download of the benign data is allowed</td>
</tr>
<tr>
<td>Adele is a contractor and is attempting to download confidential data from Box to her personal device</td>
<td>✔️</td>
<td>✔️</td>
<td>❓</td>
<td>✔️</td>
<td>❓</td>
<td>❓</td>
</tr>
</tbody>
</table>

*Old way: Block unmanaged devices*
Bob wants to email a list of corporate credit card numbers to his friend.

**Concern:** Data loss via email

**Zero Trust data protection for email**
**Scenario 10:** Sensitive data sent via email to a recipient outside of the company

<table>
<thead>
<tr>
<th>Access Requested</th>
<th>Identity</th>
<th>Device</th>
<th>App</th>
<th>Activity</th>
<th>Data</th>
<th>Contextual Response (Allow/Deny Access)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob in marketing is attempting to send an email containing credit cards data, to his friend’s Gmail address</td>
<td>? From user is Bob in marketing</td>
<td>✔ Bob is using a managed laptop with encryption and CrowdStrike endpoint enabled</td>
<td>✔ App: Gmail Cat: Email App Risk: Low</td>
<td>✔ Send</td>
<td>? PCI</td>
<td>Bob’s email containing PCI data is blocked</td>
</tr>
</tbody>
</table>

**Old way:** Enable DLP and block sensitive data without user context
Key Takeaways

Zero trust is the ability to continuously assess the context of various conditions to enable adaptive risk-based decision making.

1. **Zero Trust Model**
   - The Zero Trust Model is changing to a continuum of trust levels to support a user from any location, to any device, using any application and contextual sharing of information.

2. **Zero Trust Data Protection**
   - Zero trust is more than granting secure access. It is about using context to continuously verify trust when activities are being performed. Data protection is the #1 goal.

3. **SASE is a Requirement for Successful Zero Trust**
   - SASE enables you to move the control and zero trust decision point wherever the user and data goes as they access websites, cloud apps, and internal apps.
Thank You!

Connect with me:

https://www.linkedin.com/in/bobegilbert
@bobegilbert
bob@netskope.com

Must-read zero trust white paper:

https://resources.netskope.com/cloud-security-solution-white-papers/zero-trust-leading-practice
Authors: Vladimir Klasnja
David Fairman