Building Zero Trust: A Cloud-Native Perspective

Kathy Wang
CISO @ FullStory
Overview

- Introduction to Zero Trust Model
- Zero Trust @ FullStory
- Expanding on Zero Trust and Roadmap
- Lessons Learned
Intro to Zero Trust Model
Traditional Network Security Architecture
What is Zero Trust?
For every new connection, Zero Trust means...

...the device must be authenticated and authorized.

...the user must be authenticated and authorized.

...decisions are risk-based.
Zero Trust is...

...not a Product, It is a process.

...not new.

...not often implemented before a major breach.
Why Zero Trust Networks?
Why Zero Trust Networks?

- **Lateral movement is much harder.**
  
  Each service has to be authenticated - internal network is not permissive

- **Stolen credentials are less valuable.**
  
  Strong auth requirements increases cost of cred theft and MITM attacks

- **Known vulnerabilities that are easy to exploit will be rarer.**
  
  Increased ecosystem hygiene

- **Non-targeted attacks have less value.**
  
  Forces targeted attacks - higher cost to attacker
Zero Trust: Caveats
Zero Trust Caveats

ZTN is not all built at once.

This is NOT the totality of everything needed in Zero Trust.
Zero Trust @ FullStory
What did we have already?
What did we have already?

**Data Classification Policy**

**GCP Security Guidelines**

**Internal Acceptable Use Policy**

**HRIS System**

**Cloud-Native Workforce**

- Part of the company is remote
- No self-hosting

**Homogeneous Endpoints**

- macOS and a few Pixelbooks
- Linux in SaaS
Current Problem #1

Managing User Identity and Access
How do we verify endpoint integrity?
OSquery (e.g., Uptycs, Kolide)

Is the person accessing data appropriate to the role?
Org Chart DB (e.g., HRIS)

How we streamline onboarding/offboarding of Cloud services?
Centralized SSO (e.g., Okta, Duo, Google’s Cloud Identity)
Google Cloud Identity’s Secure LDAP tie-in with FullStory.com accounts

How do we minimize cred theft?
U2F devices (e.g., YubiKey)

How are we enforcing our data classification policy?
G Suite Enterprise (e.g., DLP solution)
Current Problem #2

Securing our Applications
Securing Applications and DevOps

Shift security to the left

Educate developers on secure coding

AppSec team develops consistent, repeatable process for internal reviews

Every commit is scanned for security vulnerabilities:

SAST, Dependency Scanning, Container Scanning+binauthz, DAST, etc.
Example: Binary Authorization

Ensure only trusted container images can be deployed

Remove human from deploy process

Sign and annotate images during CI phase
Example: Key Management

Make use of KMS services provided by public cloud provider (e.g., Google KMS, Amazon KMS)

Do NOT store keys in S3 buckets (this happens surprisingly often, and developers are not aware this is bad practice)

Automate scanning for the presence of keys in unsafe places (e.g., S3)

Keys are auto-rotated every 90 days
Ex: User and Entity Behavior Analytics

Security Teams have too much data to process

Scale the team by automating ‘needle in the haystack’

How?

- Google Cloud Identity/StackDriver logs
- git actions
- Proxy and WAF traffic anomalies
Current Problem #3

Securing our Infrastructure
How do we ensure systems are patched in a timely manner?
Vulnerability Management (e.g., Tenable)

Who owns what asset or resource?
Asset Database (e.g., Uptycs)

How do we quickly mitigate DDoS and other abuse activities?
Web Application FW (e.g., Fastly, Cloudflare)

How do we make it harder for attackers to move laterally?
Virtual Private Cloud (e.g., Google VPC)

How do we apply Google’s best security practices for FullStory.com?
Security Monitoring (e.g., Cloud Security Command Center)

How do we enforce our cloud security policies?
Cloud Policy Automation (e.g., Forseti Security)
Putting it all Together
Expanding on Zero Trust and Roadmap
Components of Zero Trust for FullStory

**FullStory.com**: Segment that processes/stores customer data, and is centrally-managed

**Endpoints**: Segment includes user/employee laptops and devices, and is individually-managed

**Backend infra**: Segment that does not store/process customer data
Zero Trust Roadmap

FullStory.com
1. Vulnerability management
2. Org chart DB
3. OSquery (FullStory.com)
4. Asset DB
5. Web application firewall
6. Google KMS

Endpoints
1. OSquery (endpoints)
2. Org DB
3. Asset DB
4. Vulnerability management
5. U2F devices
6. Device management
7. Risk-based detection

Backend Infra
1. Centralized SSO
2. Org DB
3. Asset DB
4. KMS
5. Vault audits
Lessons Learned
Lessons Learned

1. Implementing Zero Trust is always ongoing
2. Each roadmap can be built independently
3. Build root mechanisms first - order matters (e.g., central SSO)
4. UX matters
5. Serious automation will be needed
6. One size does not fit all (org requirements may differ)
7. Your mileage may vary (mature environments are more challenging)
Thank you!

kathy@fullstory.com