The road to BeyondCorp is paved with good intentions

Maya Kaczorowski & Eric Chiang
NorthSec 2022

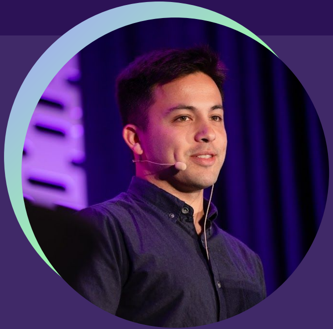
Who are we?

Maya Kaczorowski

@MayaKaczorowski

Product Manager

tailscale



Eric Chiang

@erchiang

Security Engineer

Google

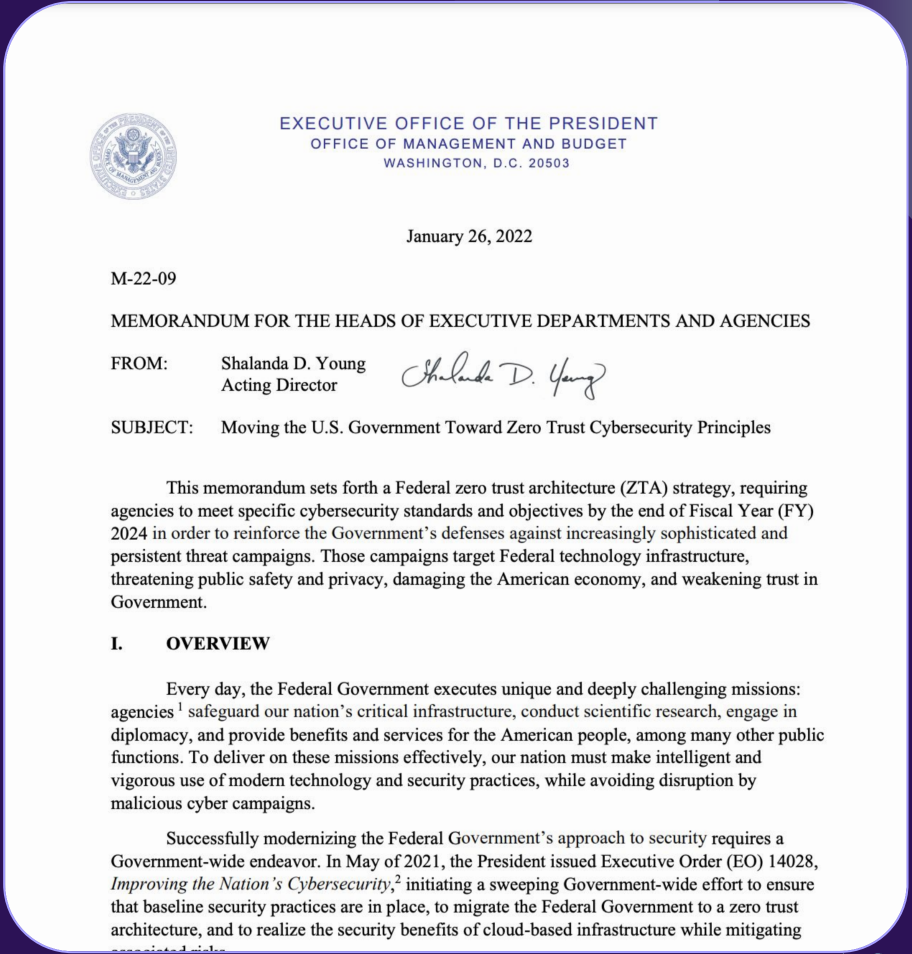
Agenda

- Zero Trust & BeyondCorp
- Components of BeyondCorp
- The road to BeyondCorp…
- … and the issues you’ll hit along the way

Zero Trust

M-22-09

Requires US Federal agencies to develop and implement a zero trust architecture by the end of 2024



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director
Shalanda D. Young

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating

https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Zero Trust Architecture

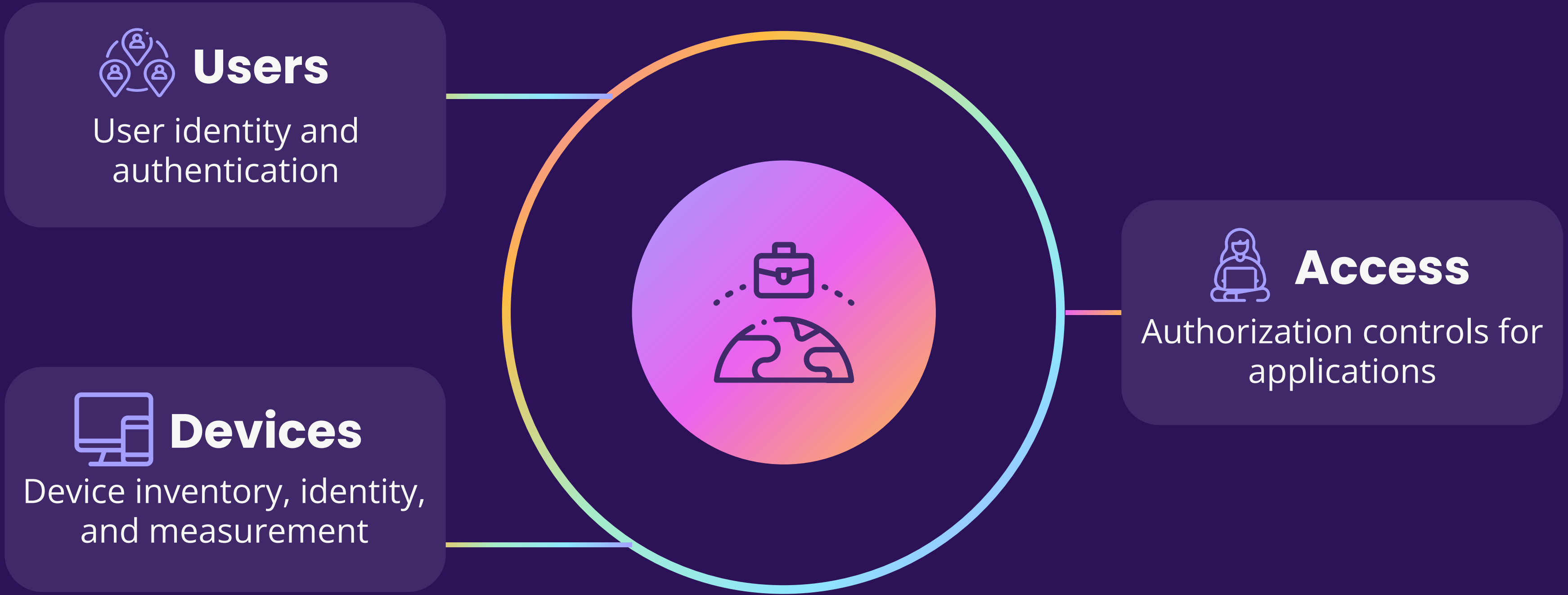
- Access by an individual to an application is not determined solely by your network
- ~~VPNs are bad~~ You're not trusted just because you're "on the network"

VS

BeyondCorp

- *Google's specific implementation*
- Original introduction of zero trust concepts in whitepapers from 2014+

3 components of BeyondCorp



Users

User identity and authentication

Devices

Device inventory, identity, and measurement

Access

Authorization controls for applications

Users

Employees and their credentials

Devices

The client devices that can access corporate infrastructure

Access

How services make authorization decisions based on user + device combination

The road to BeyondCorp

	01 Inventory	02 Management	03 “Zero Trust”	04 The long tail
	You can **enumerate** users and devices	You can **measure** most and enforce some security controls	You can **enforce** access based on device characteristics	You can dynamically **enforce risk-based** access to applications
	VPN + SSO	*VPN + SSO + MDM + MFA/security keys*	*“Zero trust” solution*	*Not for sale*
Users	Single sign-on	Security keys	Time-bound credentials	Credentials for third-party SaaS apps
Devices	Device inventory	Device inventory from an MDM	Strong device identity	All network devices included
	Manual device approval	Unique device credentials	Hardware-backed device credentials	Attested device state
Access	Network-based authorization (VPN)	Per-service authorization (proxies)	Tiered access	Real-time risk analysis

@MayaKaczorowski @erchiang

Level 01

Inventory

You can enumerate users & devices

Level 01
Inventory

You can enumerate users and devices

Users	Single sign-on
Devices	Device inventory
	Manual device approval
Access	Network-based authorization (VPN)

- Inventory of users
  - Typically SSO
  - Tied to your HRIS
- Likely no enforcement
  - SSO
  - Password manager
- Employees and contractors likely managed the same way

Level 01 Inventory

You can enumerate users and devices

Users	Single sign-on
Devices	Device inventory Manual device approval
Access	Network-based authorization (VPN)

- Potentially a lot of complexity
  - Do you support BYOD?
  - What OS do you support?
  - Do you support phones?
- Manual device inventory
  - (Corporate) Device inventory, e.g., spreadsheet
  - Likely no formal device identification
- Manual device approval, if any

Level 01 Inventory

You can enumerate users and devices

Users	Single sign-on
Devices	Device inventory
	Manual device approval
Access	Network-based authorization (VPN)

- Everyone can access everything
  - If you’re on the network, you’re trusted (like a traditional VPN)
- VPN is typically the access control point for applications
- No access control point for SaaS applications or cloud providers
  - Don’t necessarily know what these are
- Typical implementation: VPN + SSO

Level 02

Management

You can measure most and enforce some security controls

Level 02
Management

You can measure most and enforce some security controls

Users	Security keys
Devices	Device inventory from an MDM Unique device credentials
Access	Per-service authorization (proxies)

- Security keys, security keys, security keys
  - Exception processes where you need them
  - *“Google: Security Keys Neutralized Employee Phishing”* - KrebsOnSecurity
- User properties (groups, AD)

Level 02 Management

You can measure most and enforce some security controls

Users	Security keys
Devices	Device inventory from an MDM Unique device credentials
Access	Per-service authorization (proxies)

- Management of devices
  - Mobile device management
  - Potentially very simple
- Measurement of devices
  - What's your patch level?
  - Example: osquery
- Per-device credentials

Level 02 Management

You can measure most and enforce some security controls

Users	Security keys
Devices	Device inventory from an MDM Unique device credentials
Access	Per-service authorization (proxies)

- Different apps allow different user and device combinations
  - L7 proxies are a great way to centralize controls
  - Strategies for non-browser traffic (e.g. SSH or command line tools)
- Be able to consume device credentials
  - E.g. mTLS client certificates

@MayaKaczorowski @erchiang

Level 03

Zero Trust®®

You can enforce access based on device characteristics

Level 03 “Zero Trust”

You can enforce access based on device characteristics

Users	Time-bound credentials
Devices	Strong device identity
	Hardware-backed device credentials
Access	Tiered access

- Understanding of second order credentials
  - Initial auth is strong, but often exchanged for weak ones
  - Credentials should be time-bound
  - “The bearer token problem”
- Credential binding

@MayaKaczorowski @erchiang

nsec

Level 03 “Zero Trust”

You can enforce access based on device characteristics

Users	Time-bound credentials
Devices	Strong device identity Hardware-backed device credentials
Access	Tiered access

- Active management
  - Force patching
  - Security-specific config, e.g., device firewall
- Hardware based-device identity
  - Trusted Platform Module
  - Secure Enclave
  - StrongBox
- Hardware storage of device credentials

@MayaKaczorowski @erchiang

nsec

Level 03
“Zero Trust”

You can enforce access based on device characteristics

Users	Time-bound credentials
Devices	Strong device identity
	Hardware-backed device credentials
Access	Tiered access

- “Tiered access”
- Access based on device state
  - Personal vs. corporate
  - Patch level
  - Security-relevant config (e.g. jailbroken)
- If devices lose trust (e.g. don’t patch) they lose access
  - Most important access “tier” is for the device that just lost access

@MayaKaczorowski @erchiang

nsec

Level 04

The long tail

You can dynamically enforce risk-based access to applications

Zero Trust is not reality

Things that are hard at the long tail

SaaS apps

Connecting to a network you don't control

Risk-based access

Making decisions instantly

Device state

Getting trusted info onto the device

Network devices

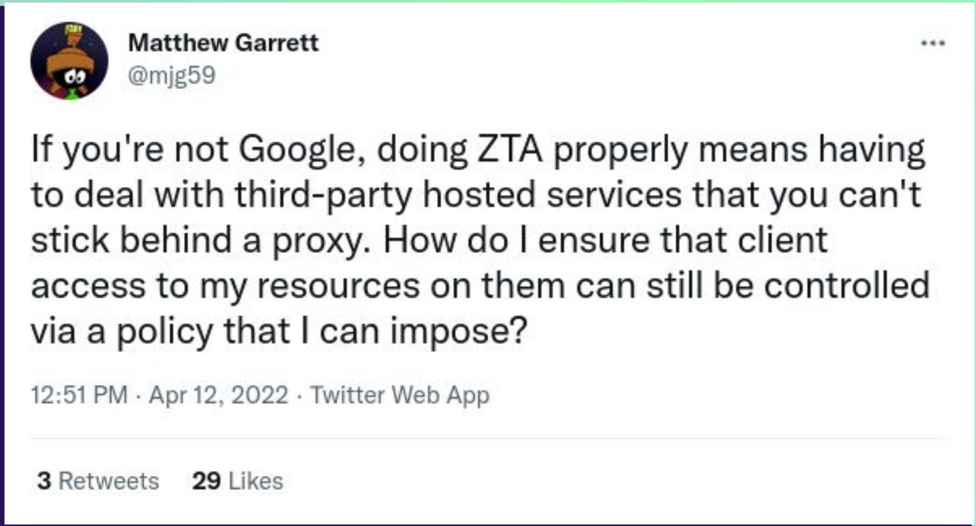
Dealing with legacy equipment

@MayaKaczorowski @erchiang

nsec

The long tail: SaaS apps

- Apps that you can't put behind a proxy are hard to access control
- SSO often the only place where you can make an access decision
    - You have to be the OAuth/SAML/OIDC provider

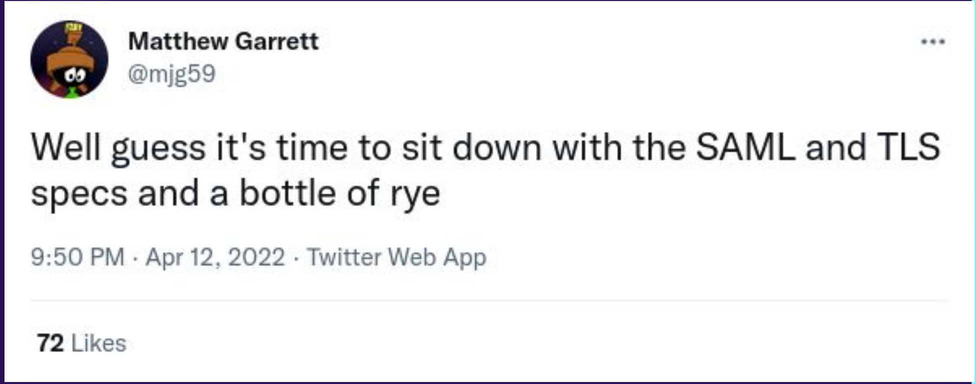


Matthew Garrett
@mjg59

If you're not Google, doing ZTA properly means having to deal with third-party hosted services that you can't stick behind a proxy. How do I ensure that client access to my resources on them can still be controlled via a policy that I can impose?

12:51 PM · Apr 12, 2022 · Twitter Web App

3 Retweets 29 Likes



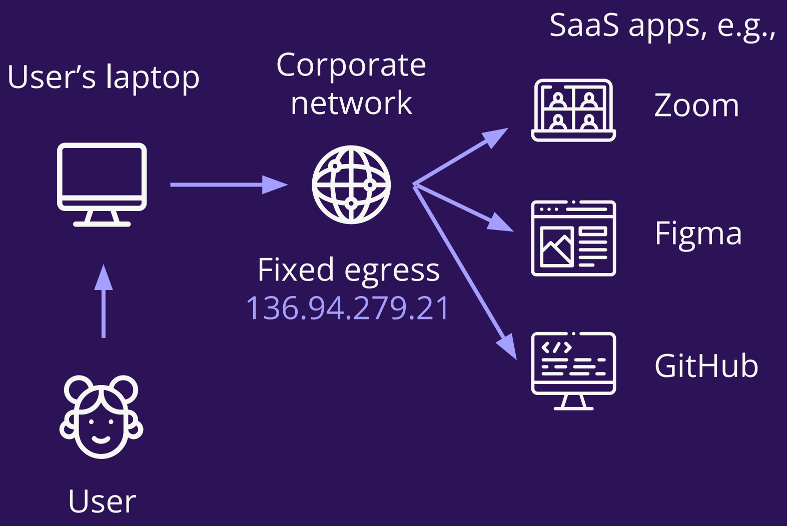
Matthew Garrett
@mjg59

Well guess it's time to sit down with the SAML and TLS specs and a bottle of rye

9:50 PM · Apr 12, 2022 · Twitter Web App

72 Likes

The long tail: SaaS apps & IP trust

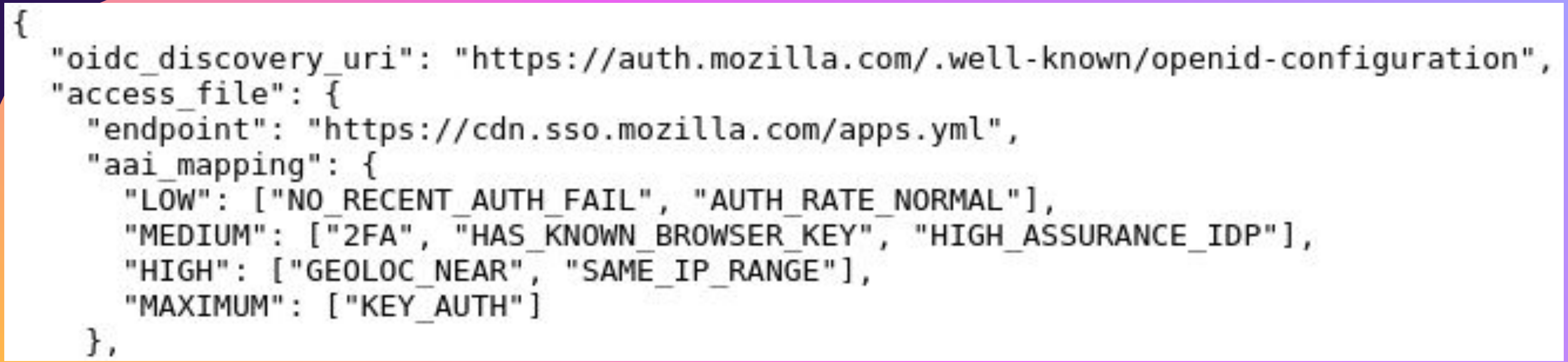


- Workaround for SaaS apps is to peer them to your network, so that you use fixed IPs to access a hosted application
- Cloud providers have a lot of IPs

@MayaKaczorowski @erchiang

nsec

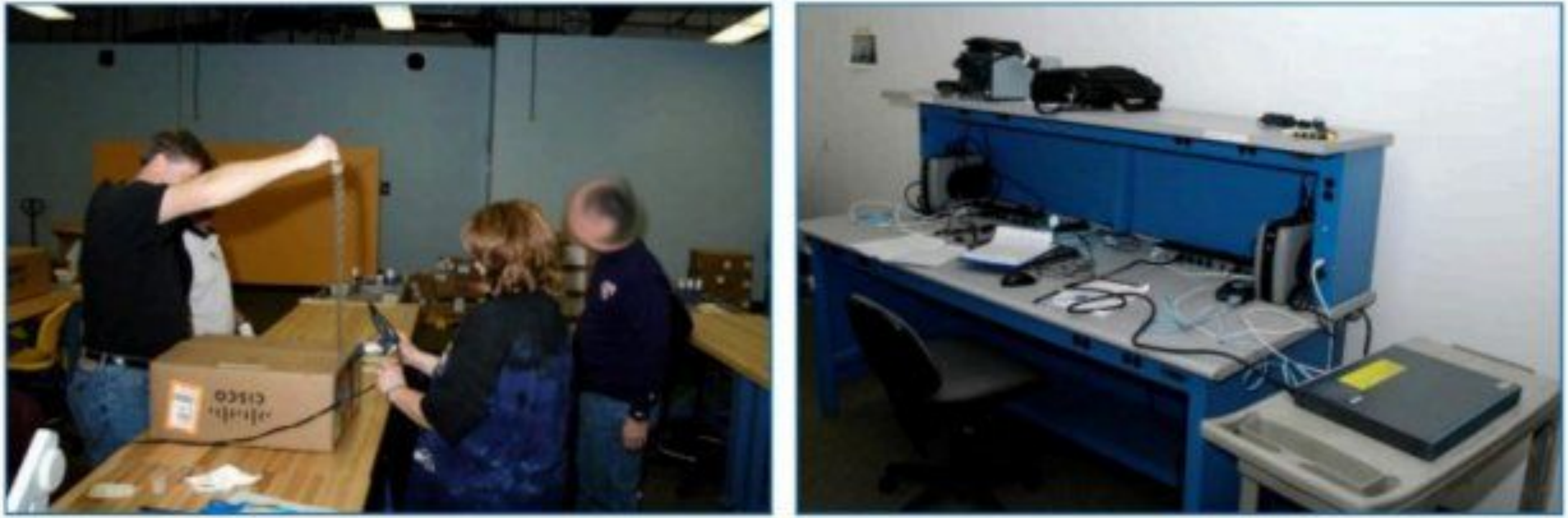
The long tail: Risk-based access



```
{
  "oidc_discovery_uri": "https://auth.mozilla.com/.well-known/openid-configuration",
  "access_file": {
    "endpoint": "https://cdn.sso.mozilla.com/apps.yml",
    "aai_mapping": {
      "LOW": ["NO_RECENT_AUTH_FAIL", "AUTH_RATE_NORMAL"],
      "MEDIUM": ["2FA", "HAS_KNOWN_BROWSER_KEY", "HIGH_ASSURANCE_IDP"],
      "HIGH": ["GEOLOC_NEAR", "SAME_IP_RANGE"],
      "MAXIMUM": ["KEY_AUTH"]
    },
```

https://github.com/mozilla-iam/mozilla-iam

The long tail: Device state



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

The long tail: Network devices

- Devices like printers don’t have device controls like MDM or secure boot
- More of an issue in brownfield vs. greenfield deployments

Level 04
The long tail

You can dynamically enforce risk-based access to application

Users	Credentials for third-party SaaS apps
Devices	All network devices included Attested device state
Access	Real-time risk analysis

- Few partial solutions today
  - Host it on prem behind a proxy
  - Be (insert large company here)
  - Enforce at SSO
- Ideally: SaaS has some understanding of device credentials
  - (See: Google's Context-Aware-Access)

Level 04
The long tail

You can dynamically enforce risk-based access to application

Users	Credentials for third-party SaaS apps
Devices	All network devices included Attested device state
Access	Real-time risk analysis

- All devices in the corporate network
  - Printers
- Device attestation
  - Root of trust that you trust!

Level 04
The long tail

You can dynamically enforce risk-based access to application

Users	Credentials for third-party SaaS apps
Devices	All network devices included Attested device state
Access	Real-time risk analysis

- Includes all known information about the user, the device, and the application at the time
  - More than rules
- Real-time
  - Without user getting frustrated

@MayaKaczorowski @erchiang

nsec

The road to BeyondCorp

	01 Inventory	02 Management	03 “Zero Trust”	04 The long tail
	You can **enumerate** users and devices	You can **measure** most and enforce some security controls	You can **enforce** access based on device characteristics	You can dynamically **enforce risk-based** access to applications
	VPN + SSO	*VPN + SSO + MDM + MFA/security keys*	*“Zero trust” solution*	*Not for sale*
Users	Single sign-on	Security keys	Time-bound credentials	Credentials for third-party SaaS apps
Devices	Device inventory	Device inventory from an MDM	Strong device identity	All network devices included
	Manual device approval	Unique device credentials	Hardware-backed device credentials	Attested device state
Access	Network-based authorization (VPN)	Per-service authorization (proxies)	Tiered access	Real-time risk analysis

@MayaKaczorowski @erchiang

nsec

BeyondCorp is never “done”

Focus on users, devices, and access, and the rest will follow

Thanks!

Questions?

sli.do #northsec

Get a copy of these slides: bit.ly/3PwXgIn