merlin
User Journey Map

Zero Trust framework supporting citizen and enterprise users securely accessing cloud and internal resources

Leveraging multiple tools, zero trust is achieved by requiring identity verification for every person and device trying to access network resources, regardless of whether they are sitting within or outside of the network perimeter.

okta · netskope · CYBERARK · FORESCOUT · wickr · SWIMLANE · SEPIO SYSTEMS · DARKTRACE

1a - Citizen using personal device logs into a citizen-facing cloud app. Her device has been unknowingly compromised by a rogue mouse.

2 - Citizen user is authenticated with Google MFA, while enterprise user requires 140-2 validated MFA using Okta Verify.

3a - With Okta and Netskope integration, user is routed through an inline Cloud Access Security Broker (CASB) - which provides security policies for session.

4a - Users are presented with the Okta App Catalog with authorized apps. Citizen opens Salesforce, Admin user opens Box.

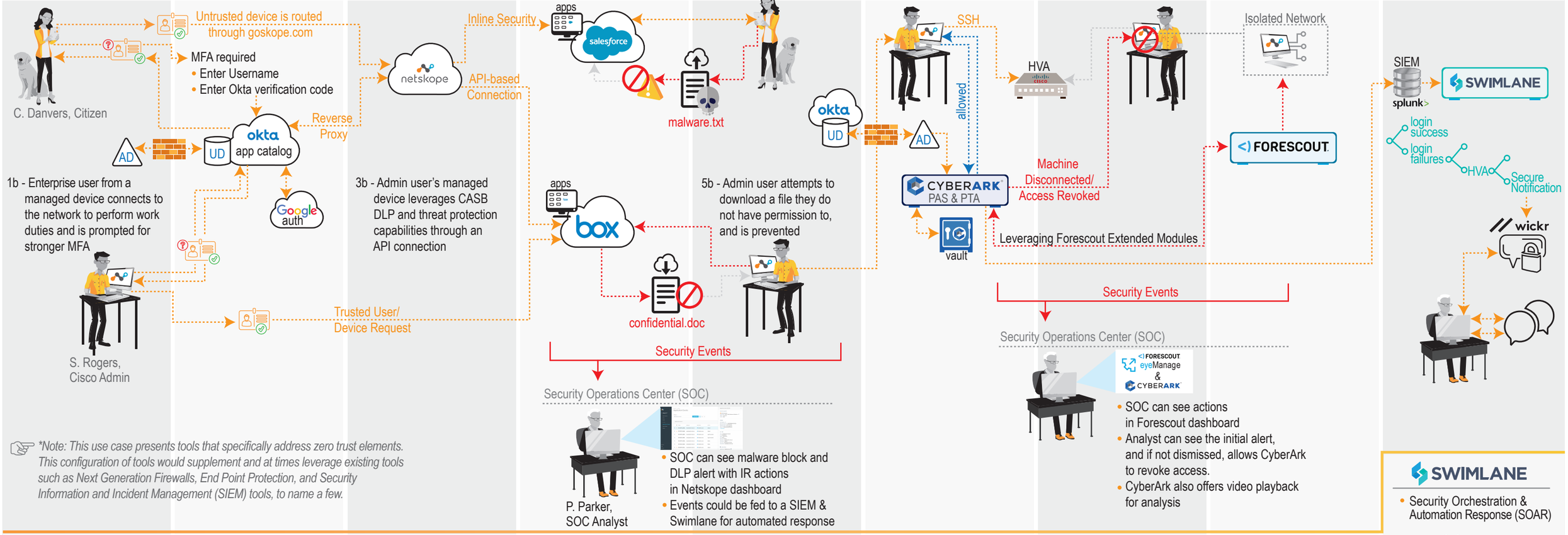
5a - Citizen unknowingly attempts to upload a file infected with malware, and is prevented from doing so by Netskope.

6 - Admin user SSH's into an internal High Value Asset (HVA) Cisco switch for routine admin, & sessions are recorded and assessed for risky behavior.

7 - After user performs a high risk action (or a series of risky actions) - a risk threshold is breached, and the SOC gets an alert. When not dismissed by the SOC, access is revoked.

8 - Due to the PTA policy violation, Forescout is instructed to move user's device to an isolated network.

9 - Threat events meet the criteria to kick off an automated response playbook, and initiate secure notifications to key stakeholders. Threat event also informs ML engine.



**Note: This use case presents tools that specifically address zero trust elements. This configuration of tools would supplement and at times leverage existing tools such as Next Generation Firewalls, End Point Protection, and Security Information and Incident Management (SIEM) tools, to name a few.*

SEPIO SYSTEMS
- Rogue Device Mitigation

okta
- Authentication & Access
- MFA & Adaptive MFA
- App Catalog/App Access
- Universal Directory (Centralized Identities)

netskope
- CASB - Cloud Security
- Threat Protection
- Data Loss Prevention (DLP)

CYBERARK
- Privileged Access Management
- Just in Time Access
- Granular Access Control

FORESCOUT
- Network Access Control
- Asset Visibility
- Orchestration Enabler

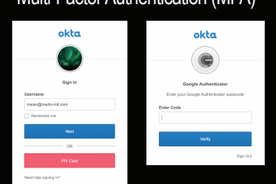
SWIMLANE
- Security Orchestration & Automation Response (SOAR)

wickr
- Secure Communication

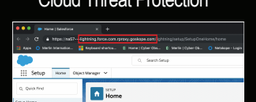
DARKTRACE
- ML and AI - Self Learning
- Autonomous Threat Response

Abbreviated Storyboard

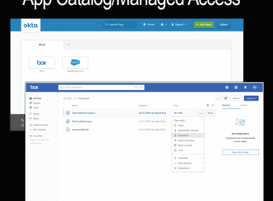
Multi-Factor Authentication (MFA)



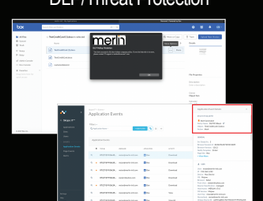
Cloud Threat Protection



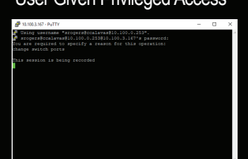
App Catalog/Managed Access



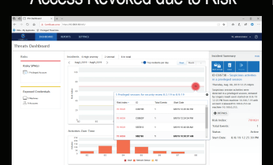
DLP/Threat Protection



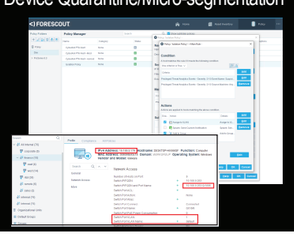
User Given Privileged Access



Access Revoked due to Risk



Device Quarantine/Micro-segmentation



Automated Response Orchestration