Identity
the Foundation of your
Zero Trust Architecture

Rob Wilson - SailPoint
Madhu Mahadevan - Okta
Traditional Security

- Protect the Perimeter
- Keep the bad people out
- Trust the people inside
Drastic Rise in Cyber Security Issues

73% of black hat hackers said traditional firewall and antivirus security is irrelevant or obsolete.

209,000 payment card numbers and expiration dates were stolen from Equifax.

Cybercrime is more profitable than the global illegal drug trade – $600 BILLION. vs $400 BILLION

Marriot International – 500 million users’ data stolen.

65% of companies have over 1,000 stale user accounts.

Russian hackers can infiltrate a computer network in 18 minutes.

32% of black hat hackers admit privileged accounts are their number one way to hack systems.
Data Breaches Have Become the New Normal

3 in 5 expect to be breached

$4.1M avg. loss due to a security breach
Any Industry Can be Impacted

Data Breaches by Industry — 2.6 billion data records lost or stolen

- Healthcare: 471 Incidents
- Government: 193 Incidents
- Other: 354 Incidents
- Retail: 219 Incidents
- Financial: 199 Incidents
- Technology: 199 Incidents
- Education: 130 Incidents

Breach Level Index: 2017 Annual Report
Credentials Are The Target

- 81% of data breaches involve stolen/weak credentials
- 91% of phishing attacks target credentials
- 73% of passwords are duplicates

Source: 2017 Verizon Data Breach Investigations Report
Source: 2016 Verizon Data Breach Investigations Report
64% Of data breaches are a result of insider negligence

74 days Average time to find and contain insider-related breach

Traditional security doesn’t solve the problem.

Source: Ponemon Research
DON'T PANIC
KEEP CALM
THE ANSWER IS 42
"TRUST BUT VERIFY"
What’s the Password

Password1234

It’s Rob, Let me in please

Password1234
Trust me, I know what i am doing.
- Universe
Never Trust
ALWAYS Verify
Zero Trust Architecture

- People-Centric perimeters
- Verifying access through context
- Data is the central point
- Access must be verified at any time
- Designed to reduce the risk of insider threats
A Zero Trust Access Story
Identity is the Foundation
Zero Trust Architecture and Identity

- Digital identities, at different levels of privilege, underpin all digital transactions.

- Digital identities are used to log in to the network, access data and applications, and enforce organizational policies.

- Digital identities contain the values leveraged by Zero Trust processes.
Zero Trust Architecture and Identity

• Zero Trust requires confidence in knowing who a person is, his/her role, and what he/she should be able to access.

• Strong Identity Governance and Access Management builds confidence in digital identities and their access to systems and data
Zero Trust and Identity Governance

1. Identity Lifecycle
2. Access Requests
3. Access Certification
4. Policy and Role Management
Homegrown commissioning tool

Arthur Dent
Sales rep

Access management

Identity governance

Salesforce

Oracle Peoplesoft
Zero Trust Architecture & Access Management

The right people have the right level of access to the right resources in the right context that is assessed continuously. Least Friction Possible
Zero Trust Architecture - Contextual Access

- **App Context**
  - Network Context
  - New IP
  - Threat Intelligence
  - New city/state/country
  - Impossible travel

- **User Context**
  - Device Context
  - New device
  - Managed device
  - New geo-location

- **Contextual Response**
  - Prompt for proper factor
  - Allow/deny access
Zero Trust Access Management Maturity Curve

Stage 0: Fragmented Identity
- Active Directory on-premises
- No cloud integration
- Passwords everywhere

Stage 1: Unified IAM
- Single sign-on across employees, contractors, partners
- Modern multi-factor authentication
- Unified policies across apps and servers

Stage 2: Contextual Access
- Context-based access policies
- Multiple factors deployed across user groups
- Automated deprovisioning for leavers
- Secure access to APIs

Stage 3: Adaptive Workforce
- Risk-based access policies
- Continuous and adaptive authentication and authorization
- Frictionless access
What Capabilities Reinforce Zero Trust?

- Identity Governance
- Access Management
  - Single Sign On - Step up Authentication & Federated Access
  - Multifactor Authentication with context based access management
- Principal of Least Privilege
  - Appropriate Business Role Access ≠ Least Privilege Access
Steps to Zero Trust Architecture

1. Establish strong identity governance
2. Establish authentication & access management
3. Ensure application security and data governance
4. Develop better network and cloud security
Zero Trust Architecture Best Practices

• Prioritize replacement of poorly authenticated legacy systems.
• Design based on how users and apps access sensitive information.
• Automate the management of accounts & entitlements.
• Verify trust upon access to any network resources using MFA.
• Extend identity controls to recognize and validate all devices.
• Educate and coach end users to be part of the solution.
STAY PARANOID AND TRUST NO ONE
Thank You

Rob Wilson CISSP
robin.wilson@sailpoint.ca
linkedin.com/in/roblwilson/

Madhu Mahadevan
mmahadevan@okta.com
linkedin.com/in/madhumahadvan/

Come see us at booth 606