CISCO Live!

ALL IN

#CiscoLive

Agenda

Industry

Challenges

Approach

Key Takeaways

Slido Question:

What is your biggest security challenge at the moment?

Evolving threat landscape

A new approach to security is needed
to address identity, application, and network threats

Targeting Identity

81%

of breaches involved
compromised
credentials

Targeting Apps

54%

of web app
vulnerabilities have
a public exploit
available

Targeting Devices

300%

increase in malware
variants targeting
IoT devices

Evolving threat landscape

99%

of vulnerabilities
exploited known
by security team
>1 year

Let's see the results from Slido!

Challenges Faced

Technology

Technical debt: complexity and lack of scalability

Heavy reliance on home-grown tools

Redundant solutions

Lack of standardization across '000s of applications

Resources

Fragmented security teams

Lack of accountability model within leadership team

Delivering multiple things without focus on priorities

IP risk due to geographical presence of teams
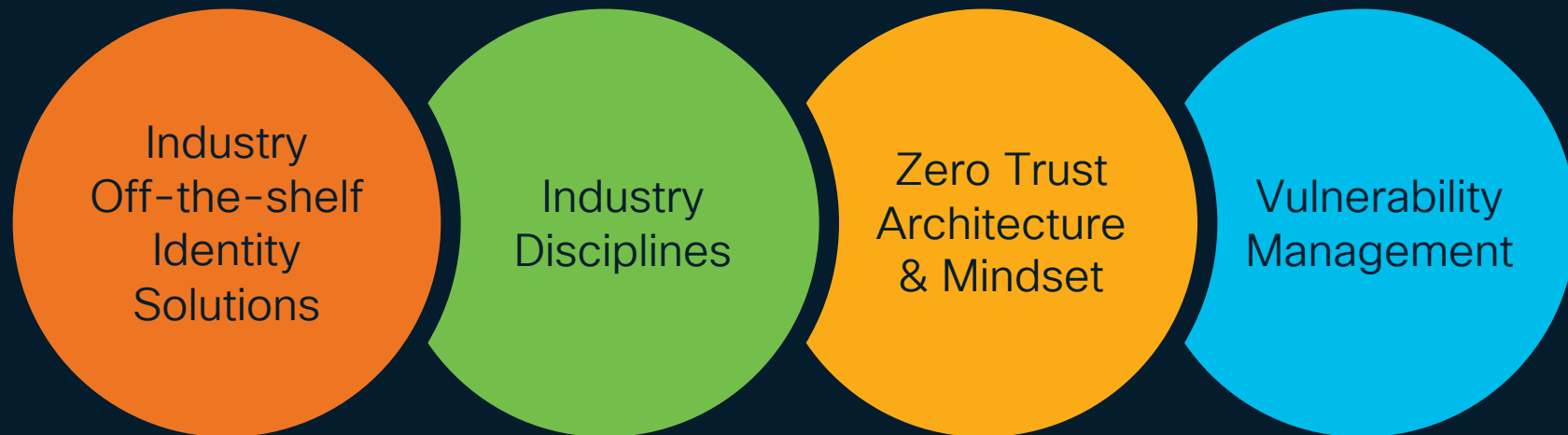
User Experience

Authentication

Frequent password resets

Inconsistent experience when accessing apps (VPN, no VPN)

VPN

Approach

Industry Off-the-shelf Identity Solutions

Industry Disciplines

Zero Trust Architecture & Mindset

Vulnerability Management

Industry Off-the-shelf Identity Solutions

New Internal & External Identity Provider

Align "Cloud First" and "Buy vs Build" principles

Address "Strengthen the Core" gaps

"Co-development" and "showcasing Cisco technology at scale"

Identity Governance

Opportunity to reduce Total Cost of Ownership(TCO)

Adopt industry standards

Drive adoption of our services by Engineering Business Units(BUs)

Privileged Identity Management

Address proliferation of tools across different teams

Eliminate reliance on homegrown code in favor of standard integrations

Full cycle solution to managing privileged accounts

Industry Disciplines

External Directory Services	Internal Directory Services	Identity & Access Management	Privileged Identity Management	Data Security	Architecture & Research
Identity lifecycle, directory, authentication, federation, and entitlements	Directory and Authentication services	Creates, changes and exit accounts Integrates with HR, directories and applications	Defines and protects privileged accounts, passwords, certificates and keys	Protect from external & insider threats Data classification & risk determination Workstation security	Central team Visions, POC's & strategies Research risks/attacks & response

Security Intelligence
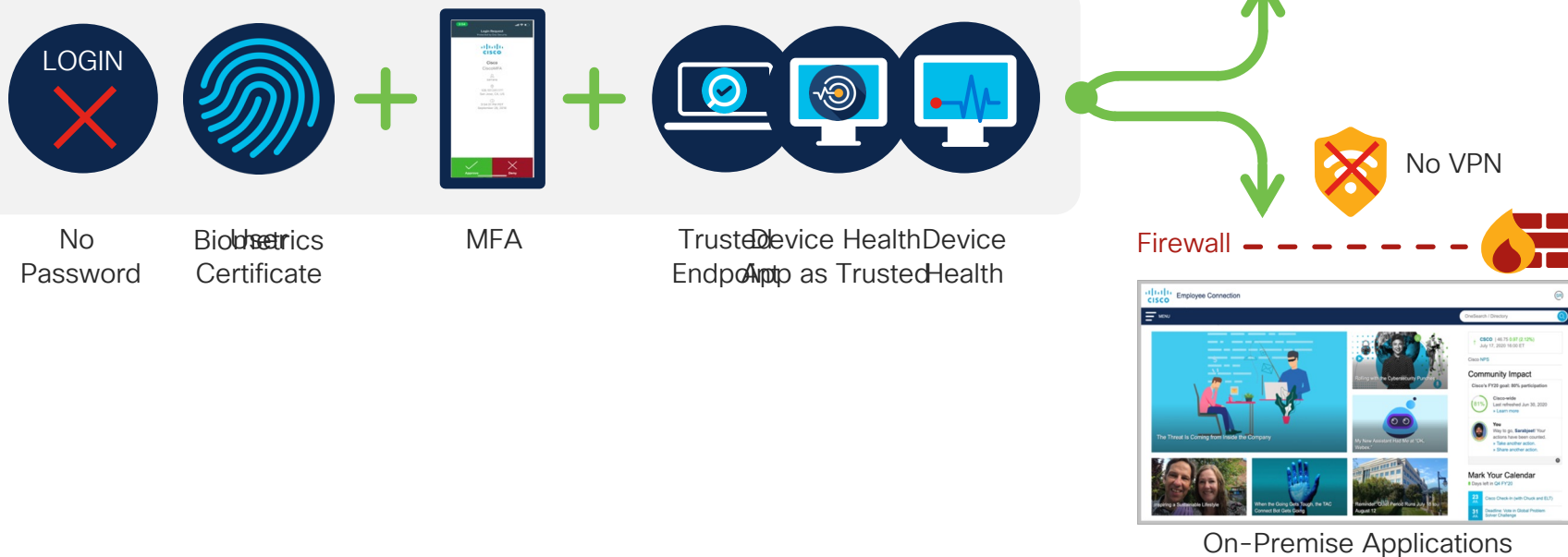### Monitoring & Response

Authentication, access, data usage/protection and device posture	Integrated with all security platforms and selected application	Supports Zero Trust & Removal of 90-day password changes

Zero Trust
Borderless Access with Improved Authentication

Cloud Applications

No VPN

Firewall – – – – – –

On-Premise Applications

| No Password | Biometrics User Certificate | MFA | Trusted Endpoint | Device Health App as Trusted | Device Health |

5-Month Deliverables

Initial deployment of Zero Trust leveraging Duo to 21% of the workforce.

Offered borderless application access	Improved authentication experience	Reduced information risk

Enable borderless (VPN-less) access to 10-15 identified applications

Deploy user/device certificates

Per-app access controls

Does not impact existing experience

Inventorizing Vulnerabilities

Goal

Efficiently remediate Observable/ Exploitable Vulnerabilities for the inventory of applications managed by an Organization.
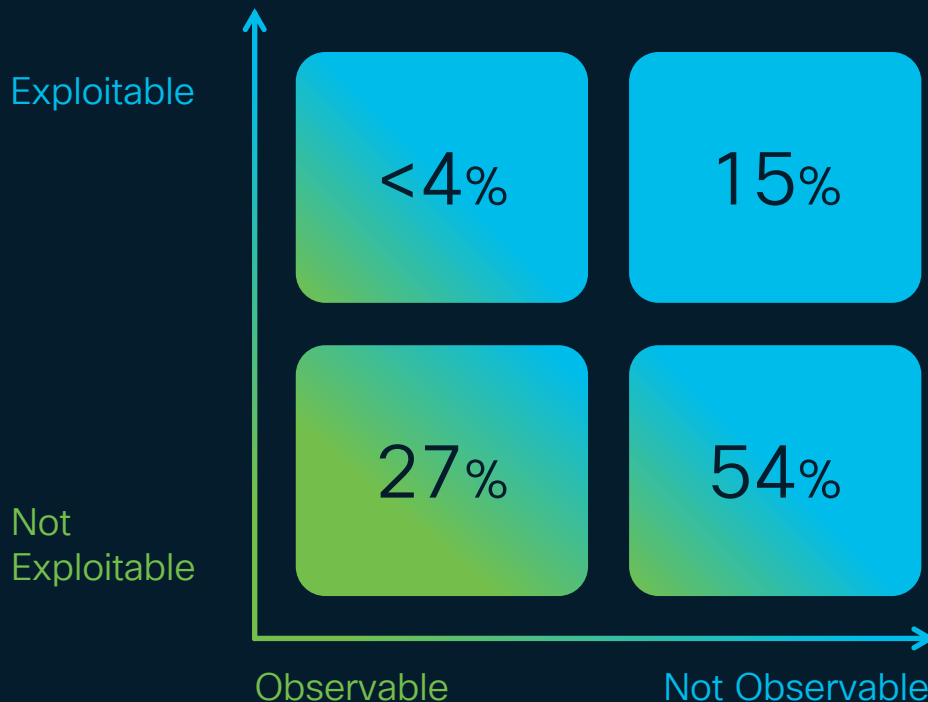
Communication Channels

Consistent Coverage/ Identification

Platform Efficiency

Velocity

Capacity

Exploitable

	Observable	Not Observable
Exploitable	<4%	15%
Not Exploitable	27%	54%

Key Takeaways & Lessons Learned

Accelerating through Standardization

Consolidate capabilities

Increase interoperability

Organizing around Industry Disciplines

Drive clear accountability

Align on a joint vision

Introducing Zero Trust principles to organization

Improve security AND user experience

Start small, gain experience, expand

Vulnerability Management
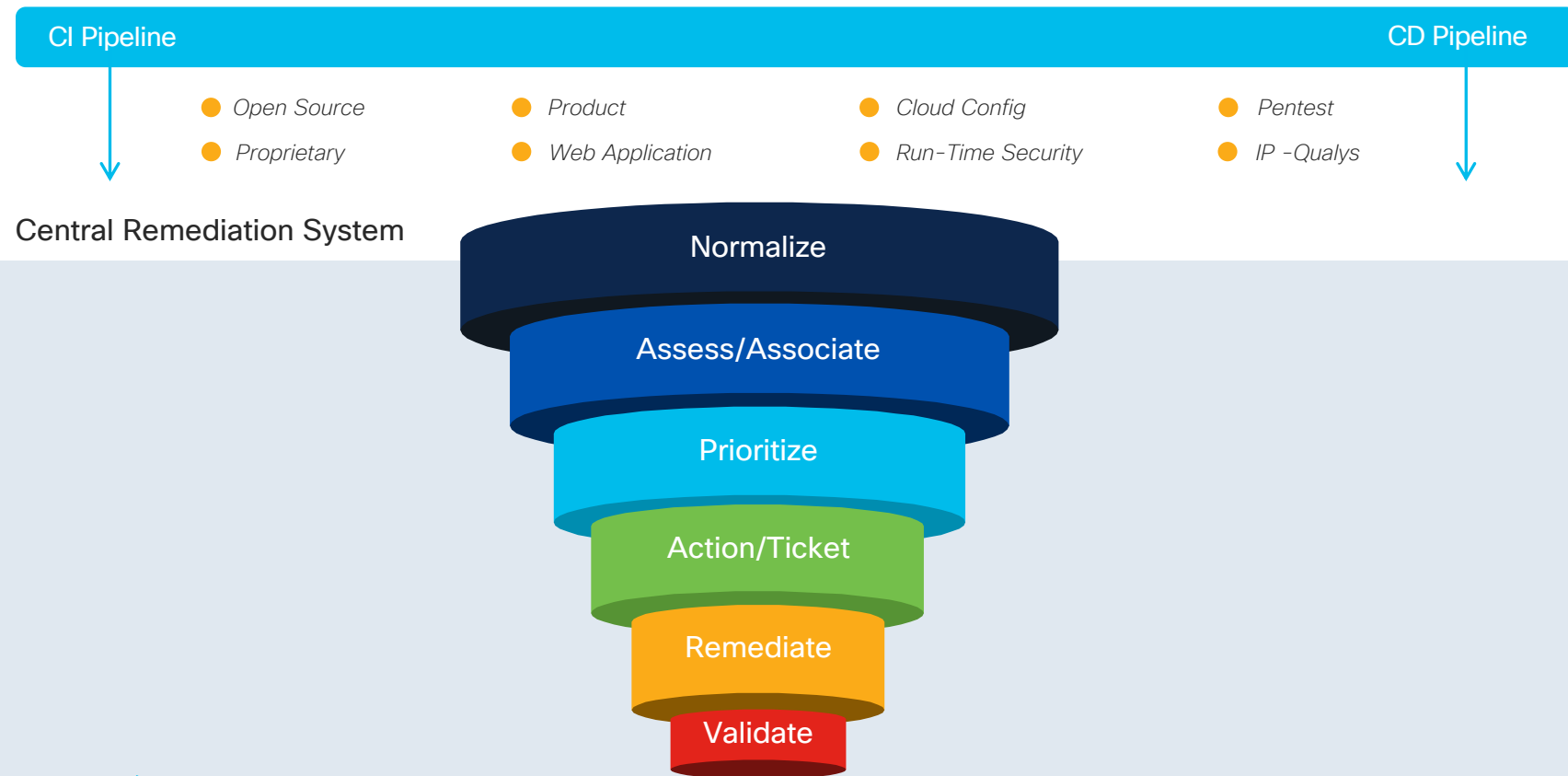
Prioritize Observable and Exploitable vulnerabilities

Thank you

Critical Stages of Remediation Workflow Cycles

CI Pipeline   CD Pipeline

- Open Source   - Product   - Cloud Config   - Pentest
- Proprietary   - Web Application   - Run-Time Security   - IP –Qualys

Central Remediation System

Normalize

Assess/Associate

Prioritize

Action/Ticket

Remediate

Validate

ITLGEN-2103

● Off-the-shelf

Industry Off-the-shelf Identity Solutions

New Internal & External Identity Provider

Align "Cloud First" and "Buy vs Build" principles

Address "Strengthen the Core"

"Co-development" and "showcasing Cisco technology at scale"

Identity Governance

Fulfillment & Verification

Reviews & Certification

Risk Assessments

Role Mining, Analysis & Management

Privileged Identity Management

Privilege Accounts

Identity Administration

Cloud Service Administration

Critical Business Administration

Security & Management Tools

Closing

- Visit the Cisco Showcase for related demos.

- Book your one-on-one meeting.

- Attend the interactive education, Capture the flag

- Visit the On-Demand library for more sessions at www.CiscoLive.com/on-demand

Add your own take-away bullets

Key Takeaways & Lessons Learned

Executive Buy-in/ Sponsorship

Introducing Zero Trust principles to organization

Lean team structure for the cross functional team

Active communications

'Air Cover' enables team to be bold and move quickly

Share benefits to employees/leadership

Start small, gain experience, expand

Empower individuals who make decisions for their organization

Respond publicly to public input/critique

Leveraging weekly newsletter for momentum and sense of urgency

CISCO Live!