Zero Trust + AI

Chris Burchell

Senior Sales Engineer – Western Canada, Zscaler

Michael Cavallin

Senior Manager, Cyber Security and Risk, BCI

Zero Trust Vision and Founding

New Business World

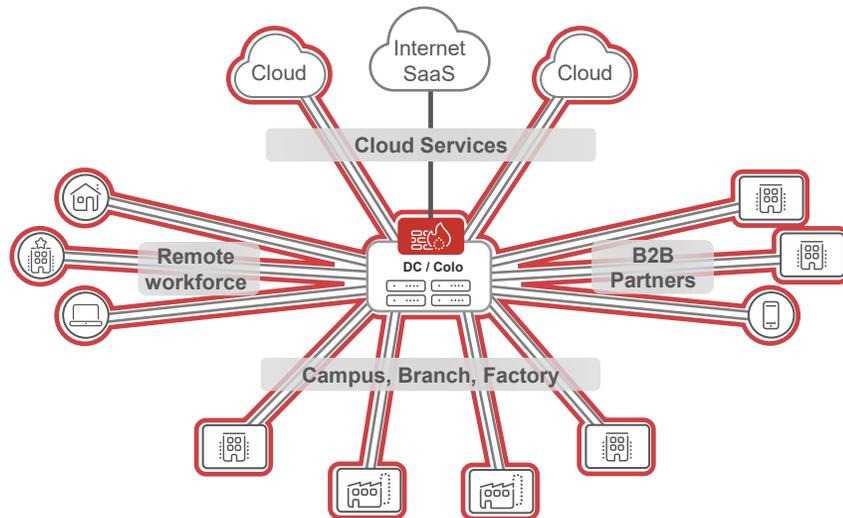Leverage disruptive technologies to become more Agile and Competitive

Mobility   **Cloud**   **IoT/OT**   **AI/ML**

But traditional network and security architectures become a liability.

Traditional Network and Firewall Architecture

Internet SaaS

Cloud   Cloud

Cloud Services

**Remote workforce**   DC / Colo   **B2B Partners**

Campus, Branch, Factory

A trusted private network connects everything

Secure the network with perimeter firewalls

Worked well in the old world, but is now a liability

Expensive, Security Risk, Poor Experience

A new cyber architecture is needed

Zscaler Vision: Reimagined a New Architecture for Networking and Security

Cloud   Internet SaaS   DC /Colo
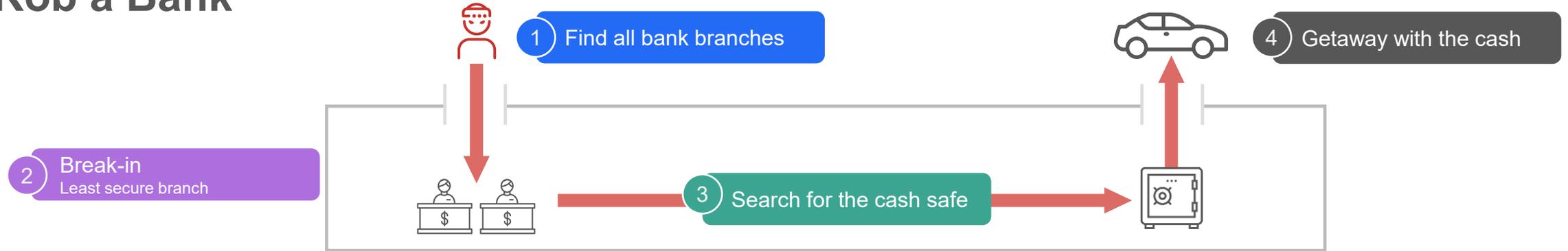
Zero Trust Exchange
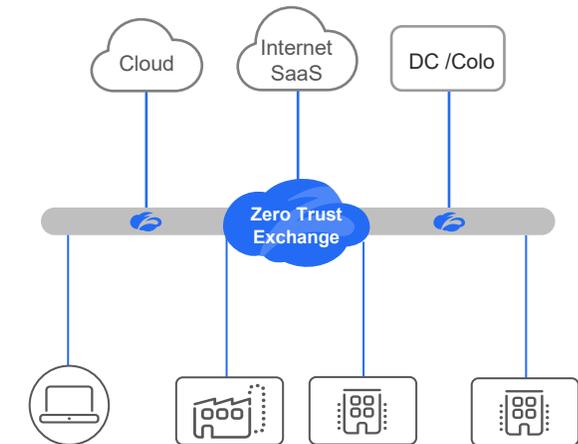
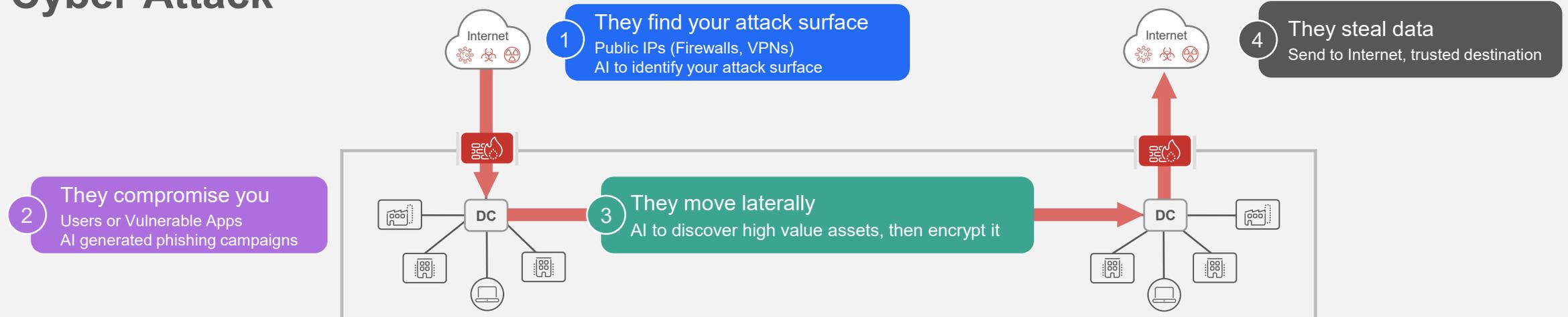**Workforce**   **Campus, Branch, Factory**   **B2B Partners**

An exchange / a switchboard to connect user, devices, and workloads using business policies over any network

Lower TCO, Superior Security, Great Experience

How Cyber Breaches Happen

4 Steps to Rob a Bank

1. Find all bank branches
2. Break-in
   Least secure branch
3. Search for the cash safe
4. Getaway with the cash

4 Steps for a Cyber Attack

Internet

1. They find your attack surface
   Public IPs (Firewalls, VPNs)
   AI to identify your attack surface
2. They compromise you
   Users or Vulnerable Apps
   AI generated phishing campaigns

DC

3. They move laterally
   AI to discover high value assets, then encrypt it

DC

Internet

4. They steal data
   Send to Internet, trusted destination

How a Zero Trust Architecture Works

Managed by others

Internet   SaaS

Managed by you

Cloud   Data Center

ZC

Adaptive Access
per Session

Zscaler AI Fabric

Risk Factors: User, Device
Destination & Content

Third-party Intel

Context is the New Perimeter
Identity can be stolen

SaaS/Internet	Private Apps

What action to take?
Allow, Block, Isolate, Caution, Deceive, Privileged

What's the risk? (Compute Risk)
Continuous Analysis

Where are you going? (App Policy)

Stop! Who are you? (Identity)

Internet replaces private networks

Workforce   Workloads   IoT / OT   B2B

Everything is invisible from the Internet (no public IPs)
You can't attack what you can't see

Enforce policy on a per session basis
Adapt as context changes

Proxy architecture for proper content inspection
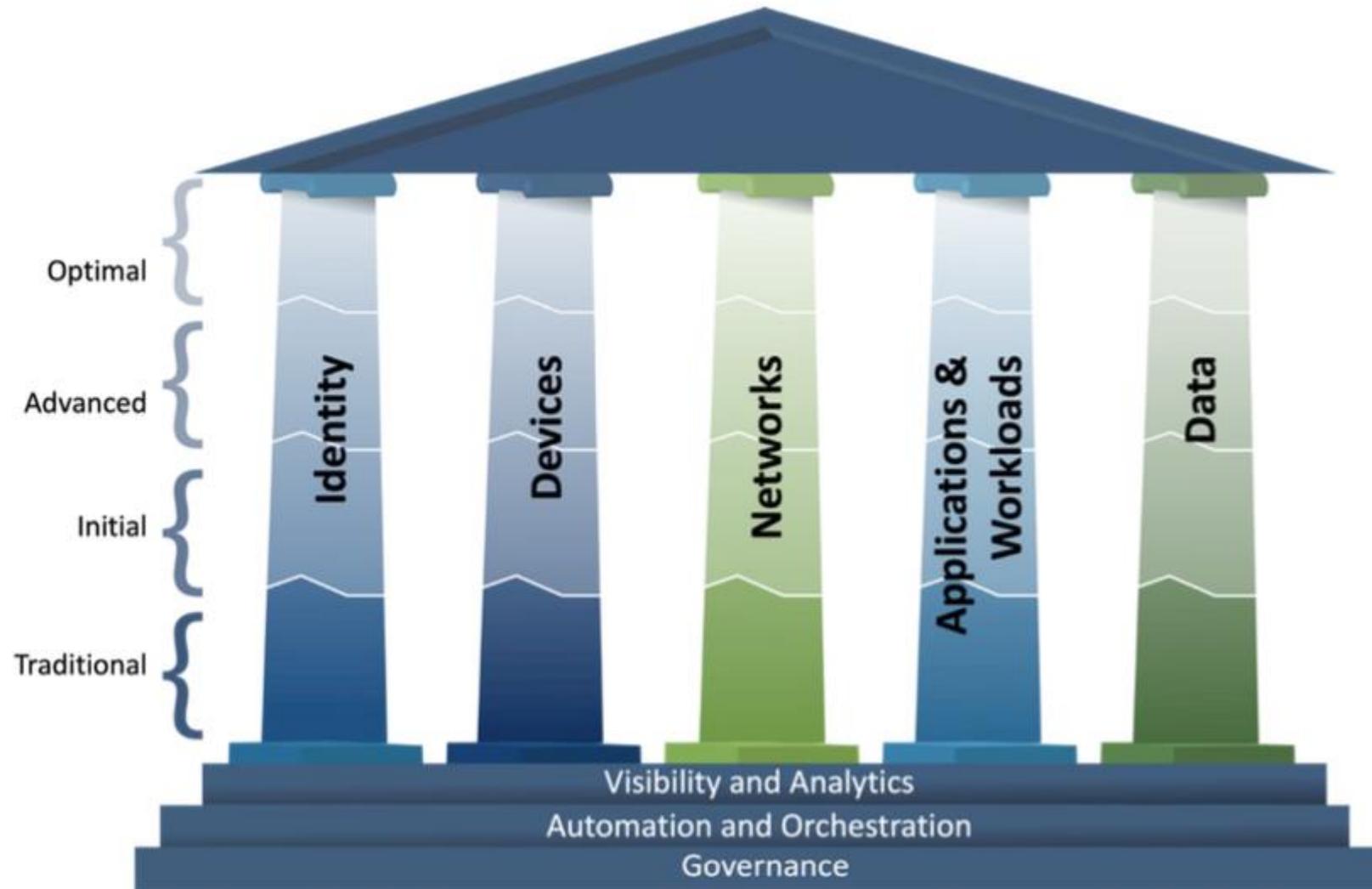Cyber and data protection

Connections are made to apps, not networks
Prevents lateral movement

Everyone is untrusted
No implicit trust, not trusted network

Two Opposing Architectures
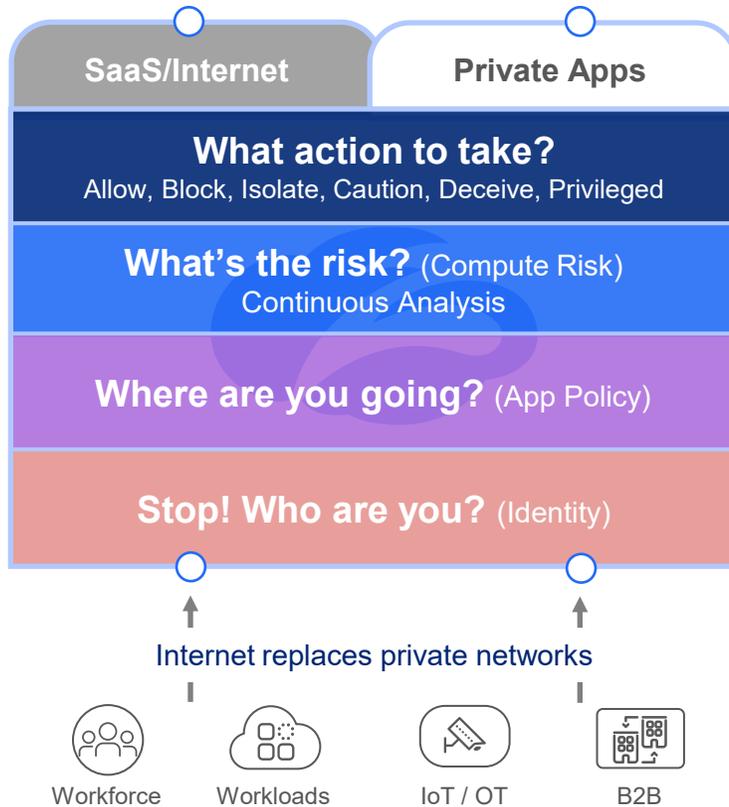Switchboard
Escorting Visitors

Zero Trust architecture can't be bolted on firewalls and VPNs

CISA Zero Trust Maturity Model

Zero Trust is a journey, not a destination

Zero Trust = AI enablement

SaaS/Internet	Private Apps

What action to take?
Allow, Block, Isolate, Caution, Deceive, Privileged

What's the risk? (Compute Risk)
Continuous Analysis

Where are you going? (App Policy)

Stop! Who are you? (Identity)

Internet replaces private networks

Workforce   Workloads   IoT / OT   B2B

Full access? Browser isolate? Limit file uploads?

Is my device healthy? Up to date? Any threats observed? BYOD?

Do I have a licence for the enterprise AI platform (or am I going to the free version)?

Any risks with my session (e.g. impossible travel)? Phishing-resistant MFA used?

Rise of the machines…

Home > News > AI

Meta Security Researcher's AI Agent Accidentally Deleted Her Emails

Meta's Summer Yue says she ran OpenClaw on her inbox, but its size 'triggered compaction [and] lost my original instruction' to get her permission before deleting.

By Jon Martindale   February 24, 2026

OpenClaw

Build systems that assume breach, minimize impact

Thank you

Please come find us afterwards if you have any questions or comments