Check Point
SOFTWARE TECHNOLOGIES LTD

CPX 360

ZEROING-IN TO ZERO TRUST

JUDGEMENT DAY 2021

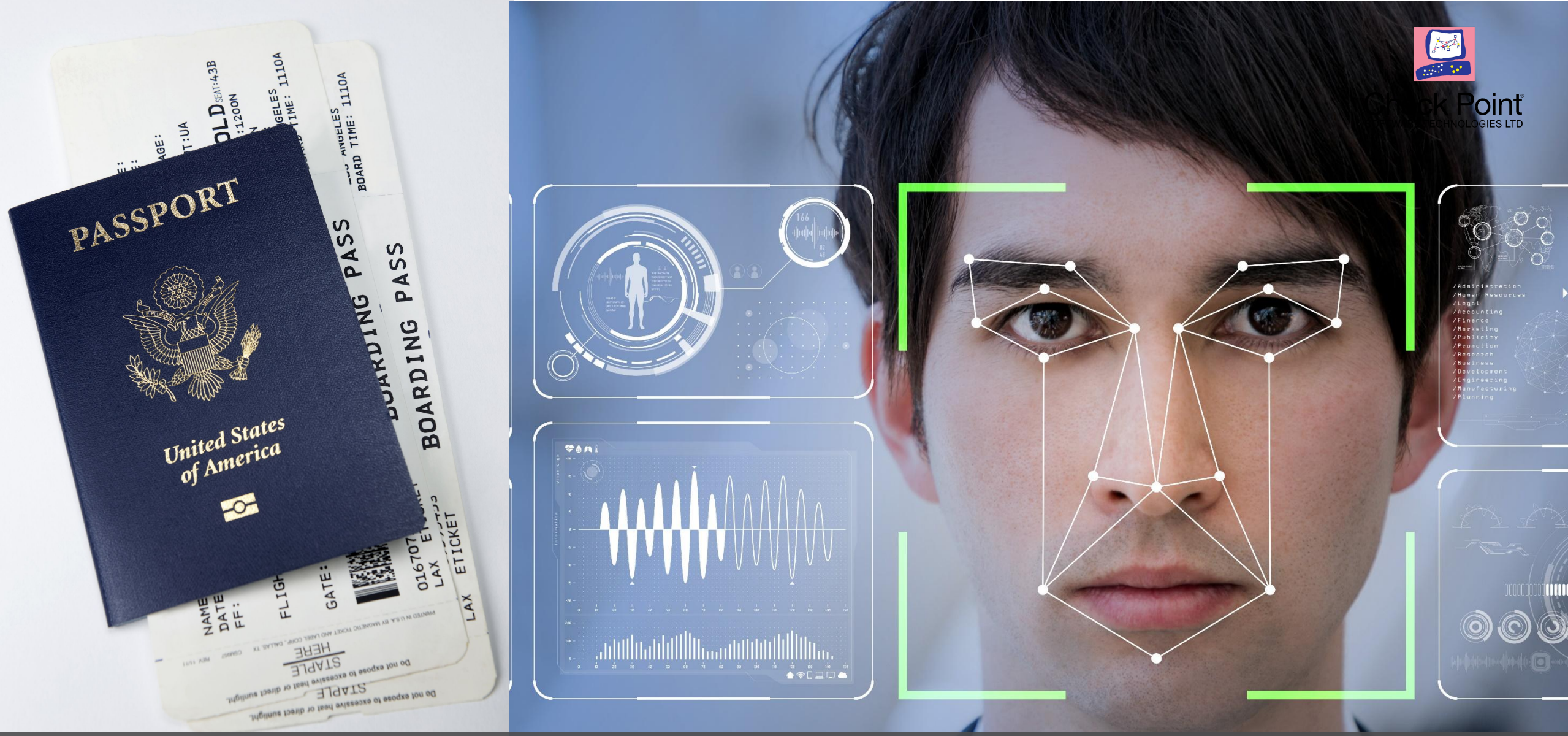
Tomáš Vobruba | Check Point

WELCOME TO THE FUTURE OF CYBER SECURITY

Check Point
SOFTWARE TECHNOLOGIES LTD

WELCOME TO THE FUTURE OF CYBER SECURITY

LEAST PRIVILEGED ACCESS STRATEGY



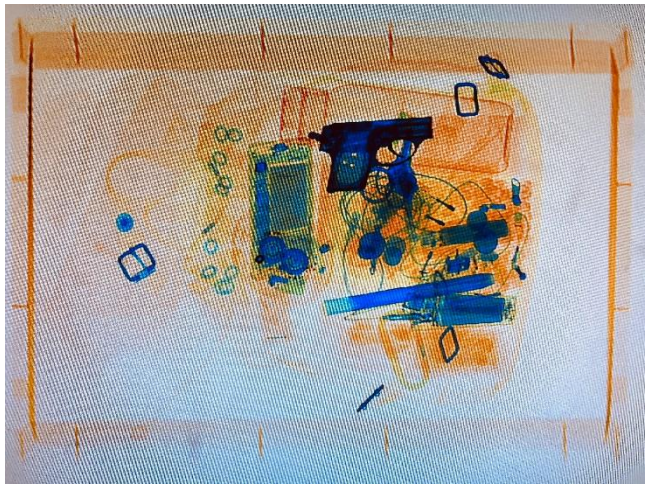
STRICT USER AUTHENTICATION

VISIBILITY IS A KEY

QUALITY OF CENTRAL INTELLIGENCE HAS A HUGE IMPACT

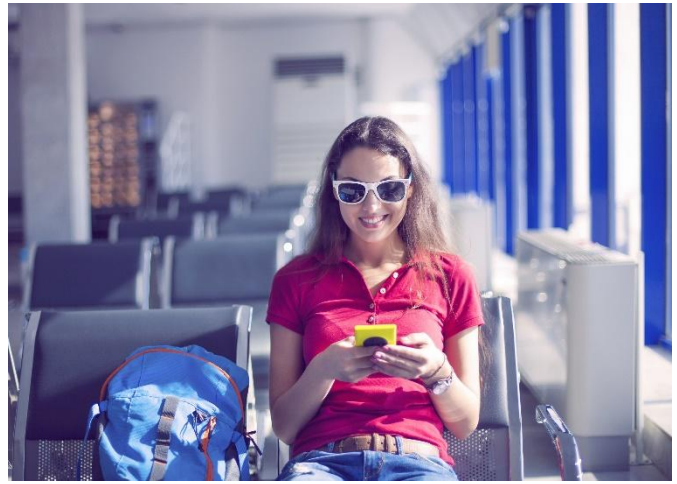
THREAT PREVENTION

3 CRITICAL OBJECTIVES



ZERO FALSE NEGATIVE

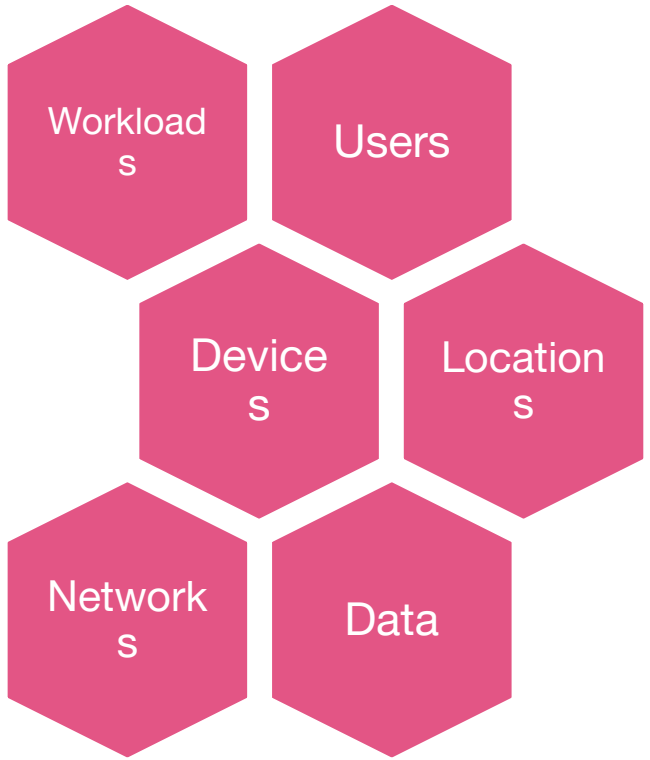
LOW FALSE POSITIVE



SEAMLESS USER EXPIRIENCE

What is Zero Trust

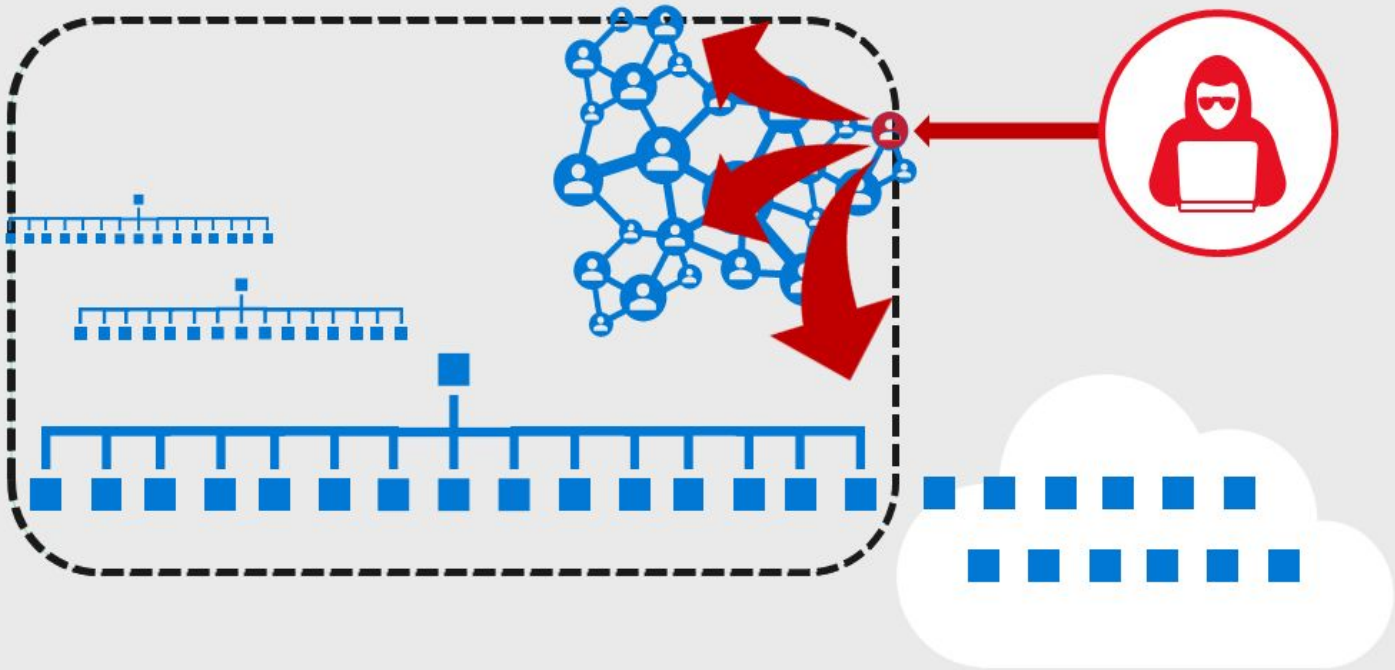
- Implementation of microperimeters
- Visibility into data assets
- Automated Response



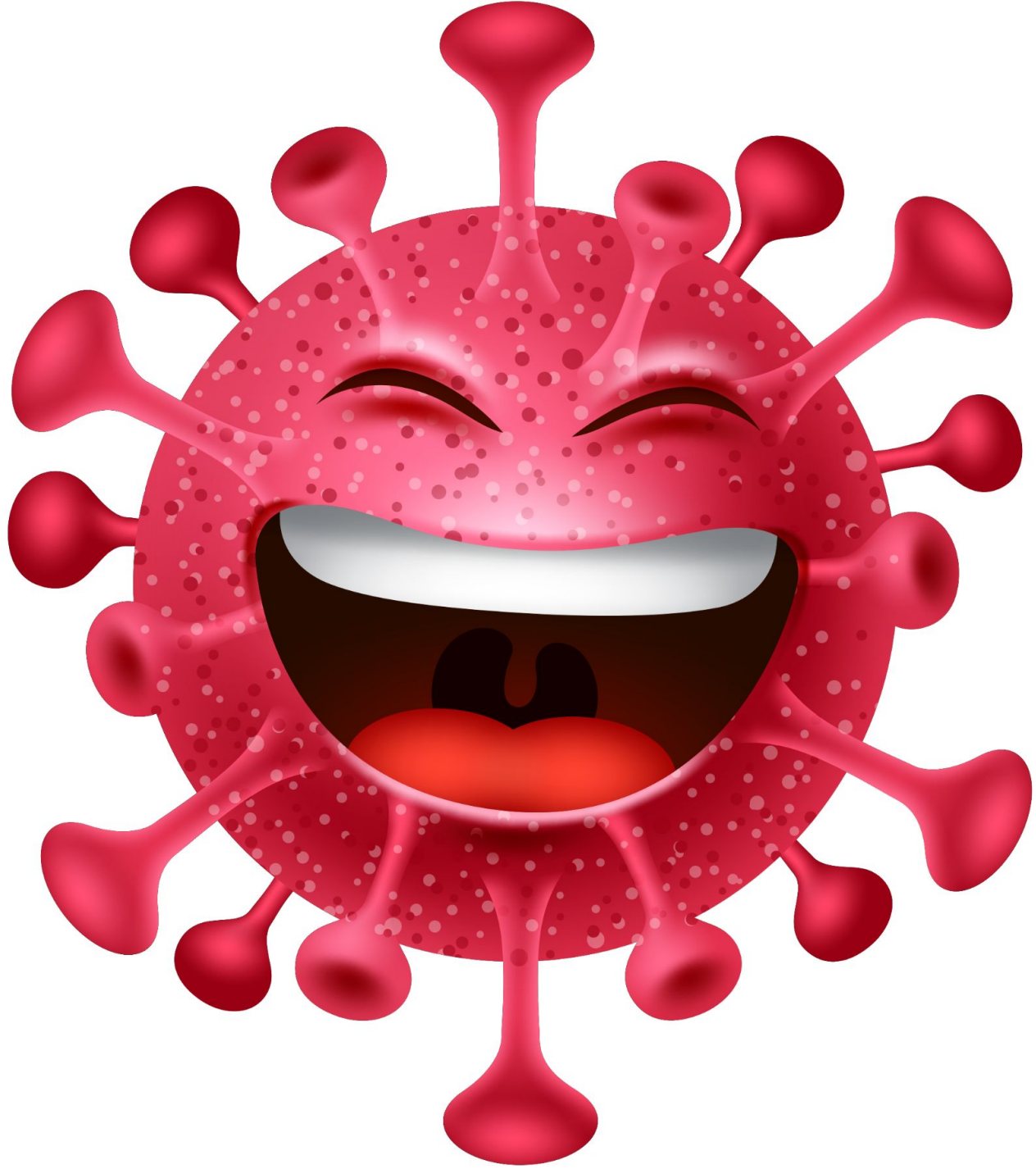
https://en.wikipedia.org/wiki/Zero_trust_security_model
https://doi.org/10.6028/NIST.SP.800-207

Why are we having a Zero Trust conversation?

Access Control: Keep **Assets** away from **Attackers**



1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within network
3. **Assets increasingly leave network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed




password
security
protection
internet
technology
login
hacking
secure
web
safety
business
software
digital
encryption
threat
scam
crime
data
virus
authorization
admin
user
verification
computer
network
secrecy
privacy
protect
forget
service
hacker
usermame
administrator
smartphone
attack
problem
webpage
website
code
safe
spyware
error
program
apppc
information
display
private
safeguard
denied
system
logon
unlock
online
hack
crack
screen
piracy
mobile
danger
interface
email
binary
cyber
hacked
access
net

Multi-Factor Authentication

Something you **have**

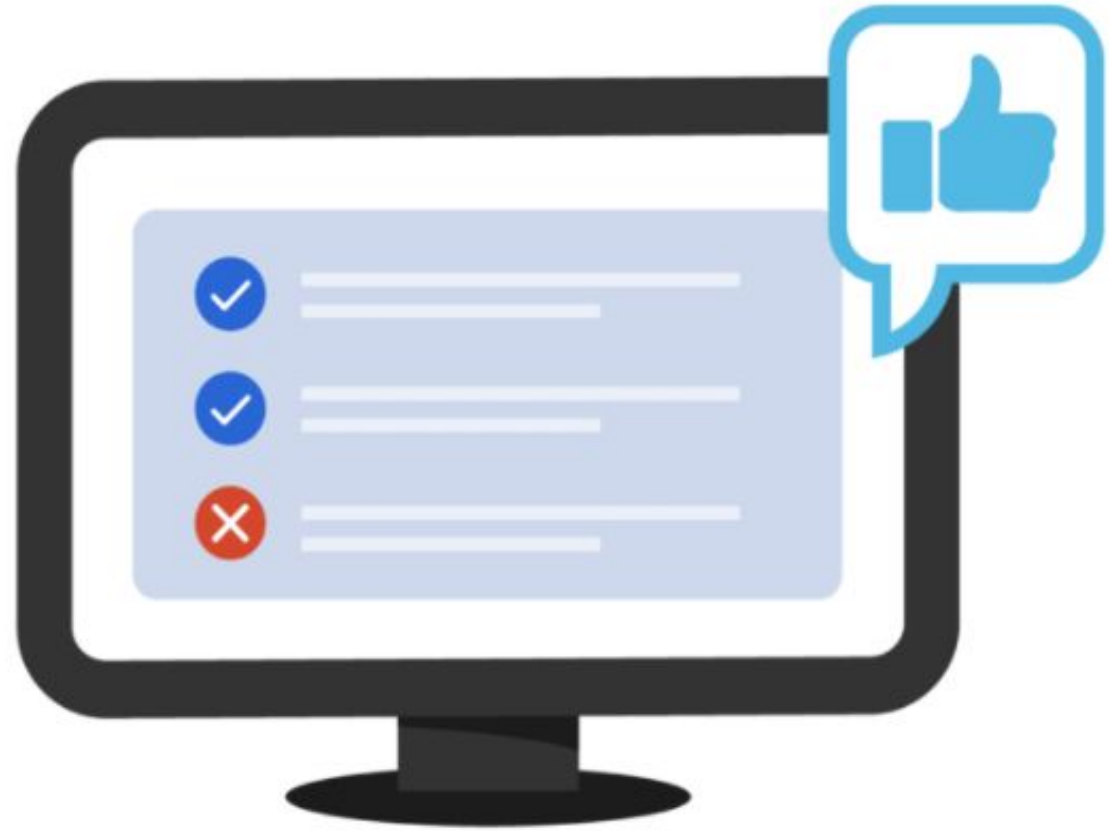
Something you **know**

Something you **are**

Authentication

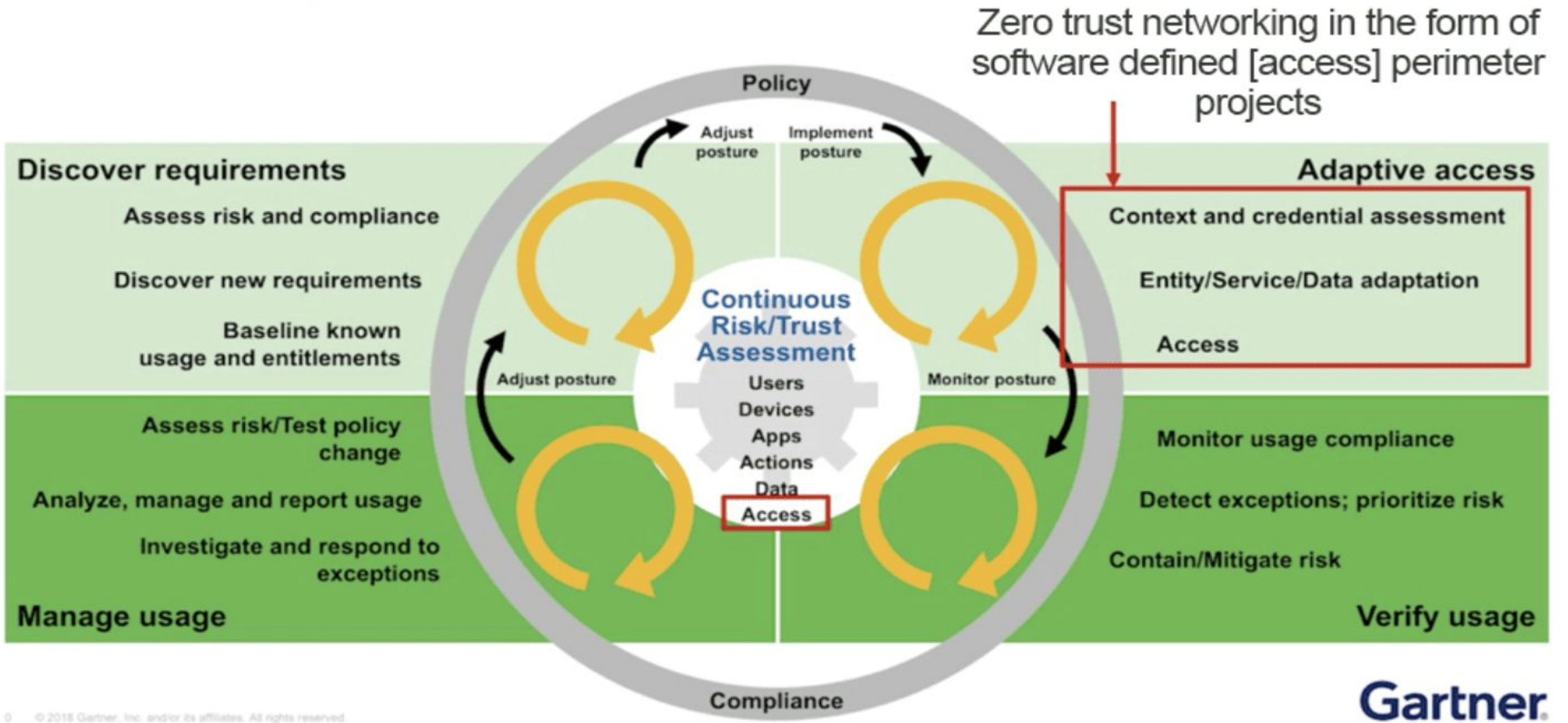
Confirms users
are who they say they are.

Authorization



Gives users permission
to access a resource.

CARTA Adaptive Access Protection Architecture



Source: Gartner (December 2018)

HOW TO AVOID COMPLEX DEPLOYMENT AND SECURITY GAPS?

ABSOLUTE ZERO TRUST SECURITY
7 PRINCIPLES

Check Point
SOFTWARE TECHNOLOGIES LTD

1 | COMPLETE

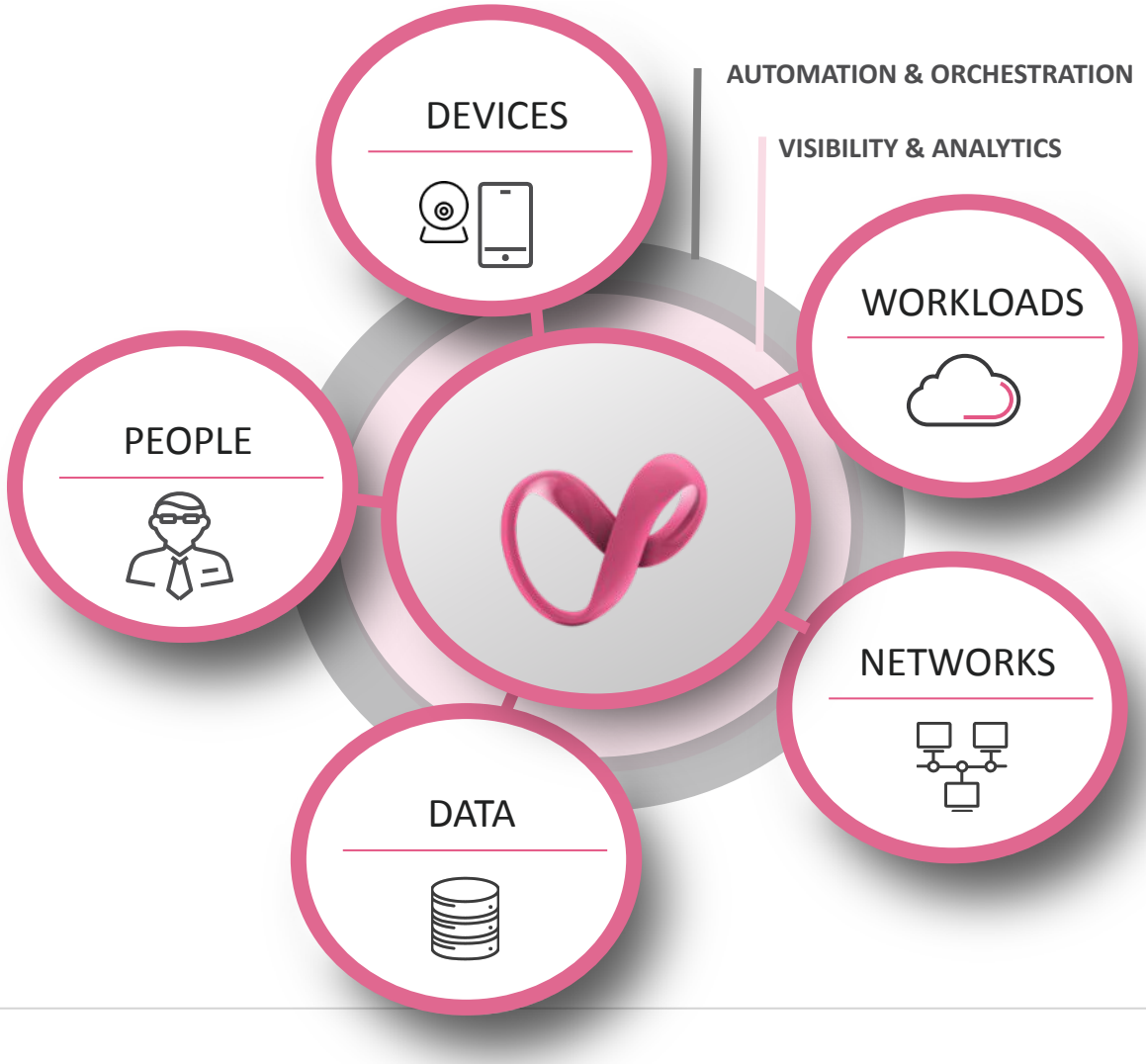
Supports all of the Zero Trust principles

2 | EFFICIENT

Centrally managed using a single console and a unified policy

3 | PREVENTIVE

Focused on threat prevention and protects from zero-day attacks



ZERO-TRUST PRINCIPLES

“NEVER TRUST, ALWAYS VERIFY”

Check Point
SOFTWARE TECHNOLOGIES LTD

Always Verify

Authenticate and Authorize from trusted users & devices

Least Privileges

Minimize user access to applications & data

Expect Breach

Minimize attack surface & prevent lateral movements

Identity	Endpoints	Applications	Networks	Workloads	Data	Monitor
Authentication Authorization Accounting	Threat protection Compliance	Least Privilege Conditional access	Lateral movements M-Segmentation	Compliance Anomalies	Classification Authorization	Security Posture Improvements

Architecting Microperimeters

Check Point
SOFTWARE TECHNOLOGIES LTD

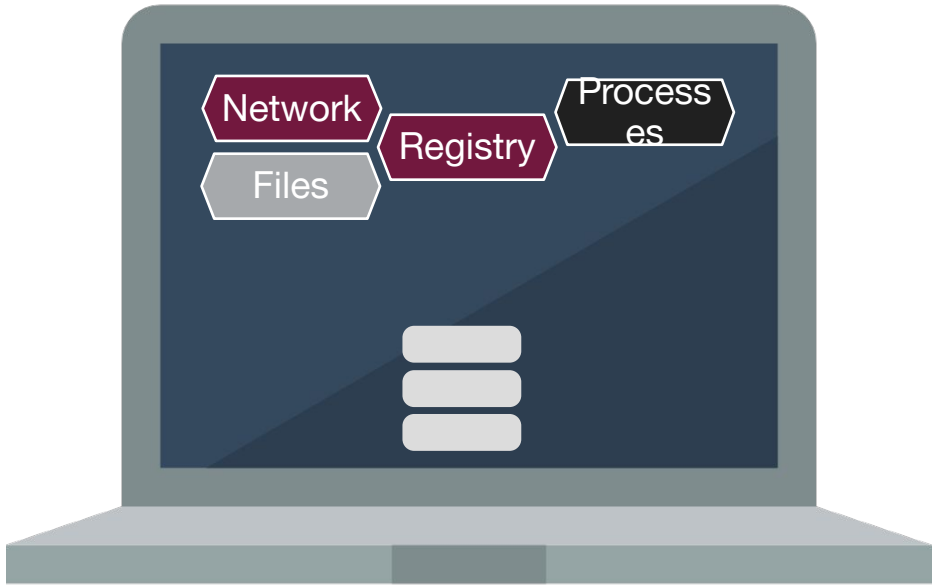
Site

(Host, Network)

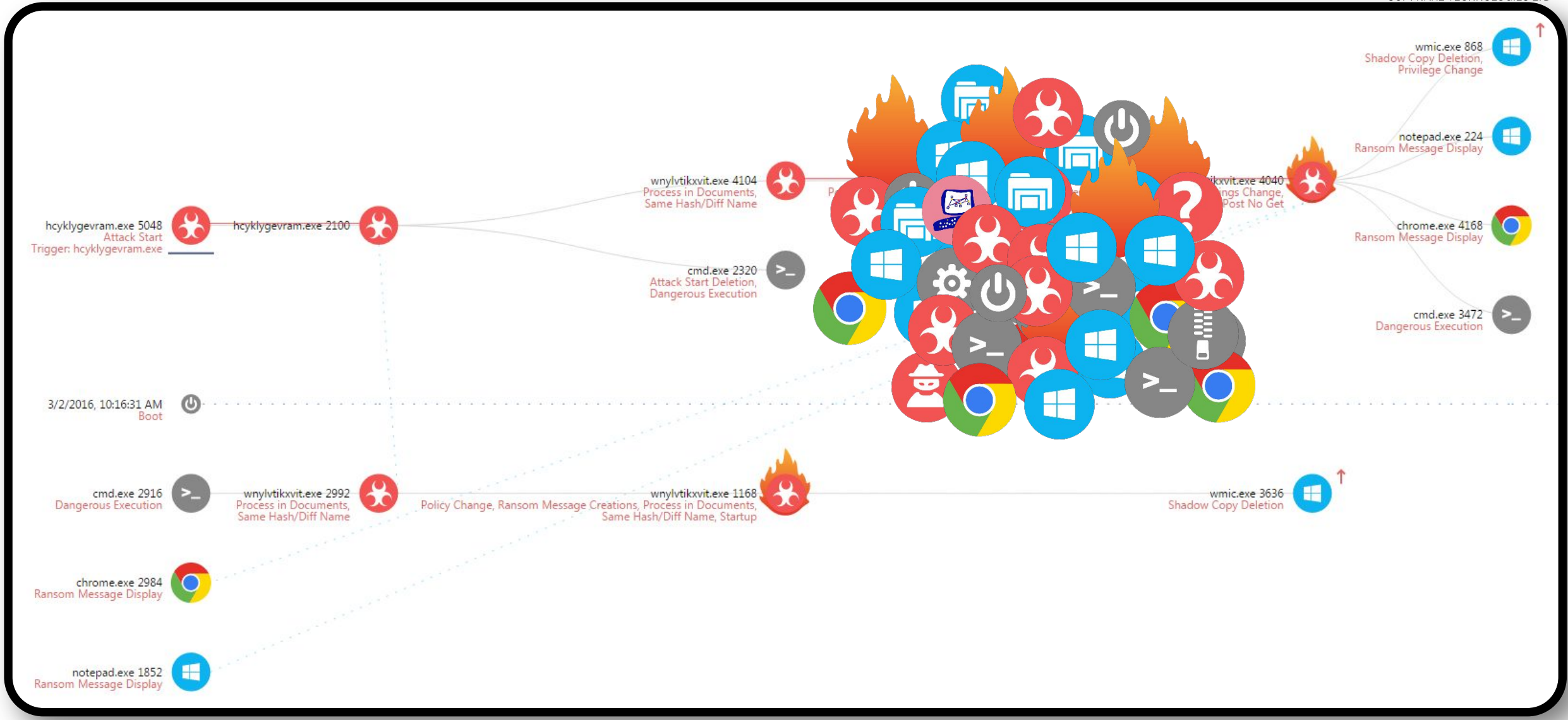
Cloud

Mobile

Monitoring (@ the microperimeter)



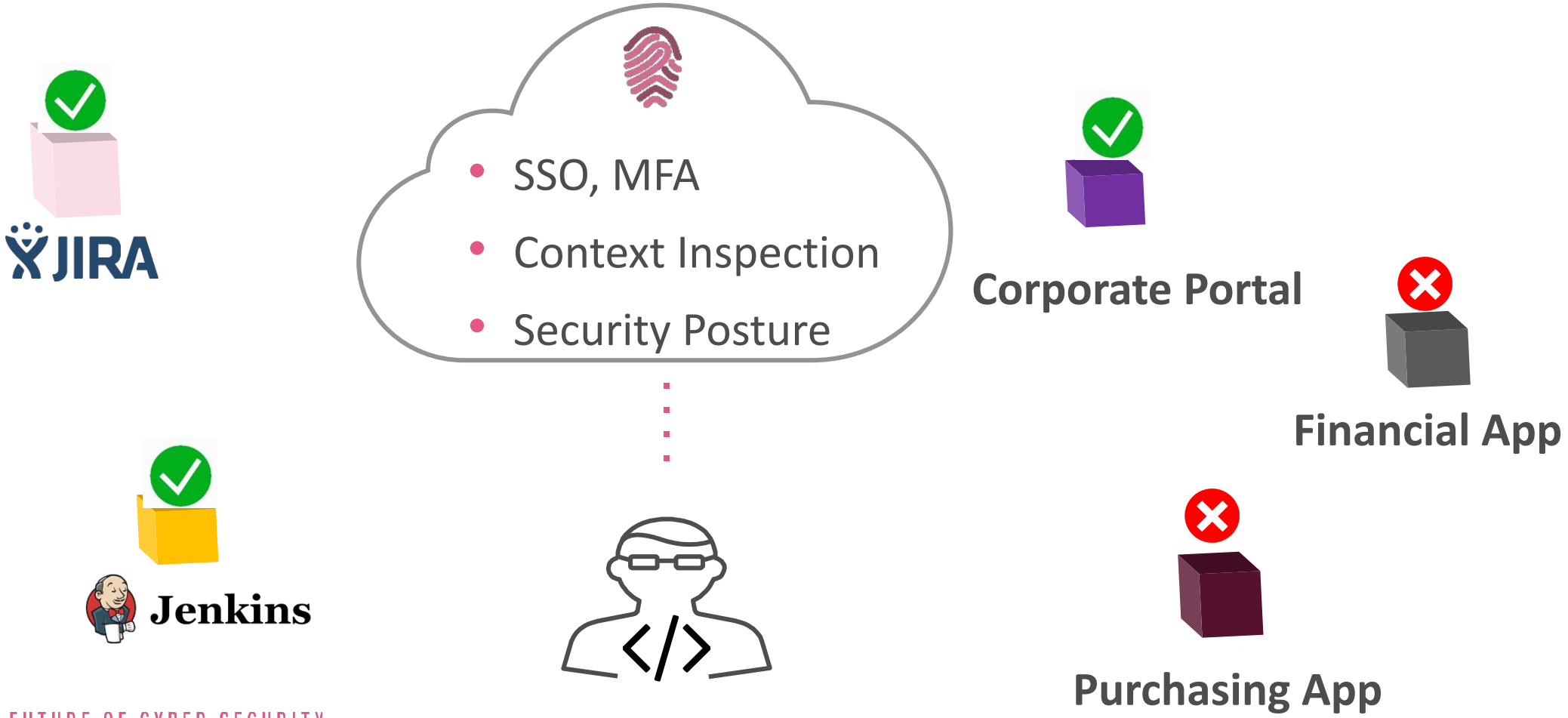
Monitoring (@ the microperimeter)



AUTO-SEGMENTATION
AUTO-GENERATED POLICY FOR EVERY DEVICE/Application

Check Point
SOFTWARE TECHNOLOGIES LTD

ZERO TRUST PEOPLE
USER AWARE ACCESS CONTROL AS A SERVICE



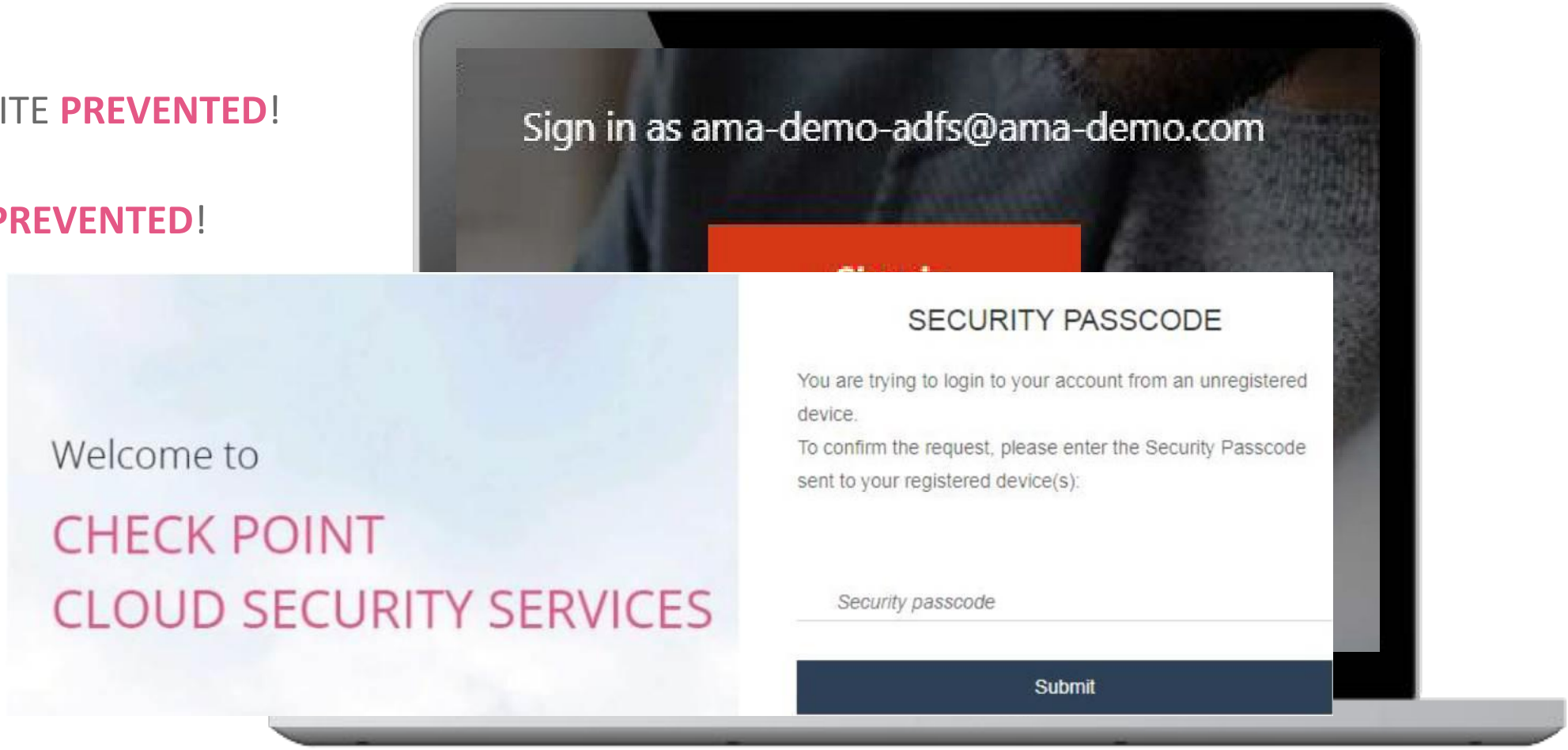
What Microsoft Sees:

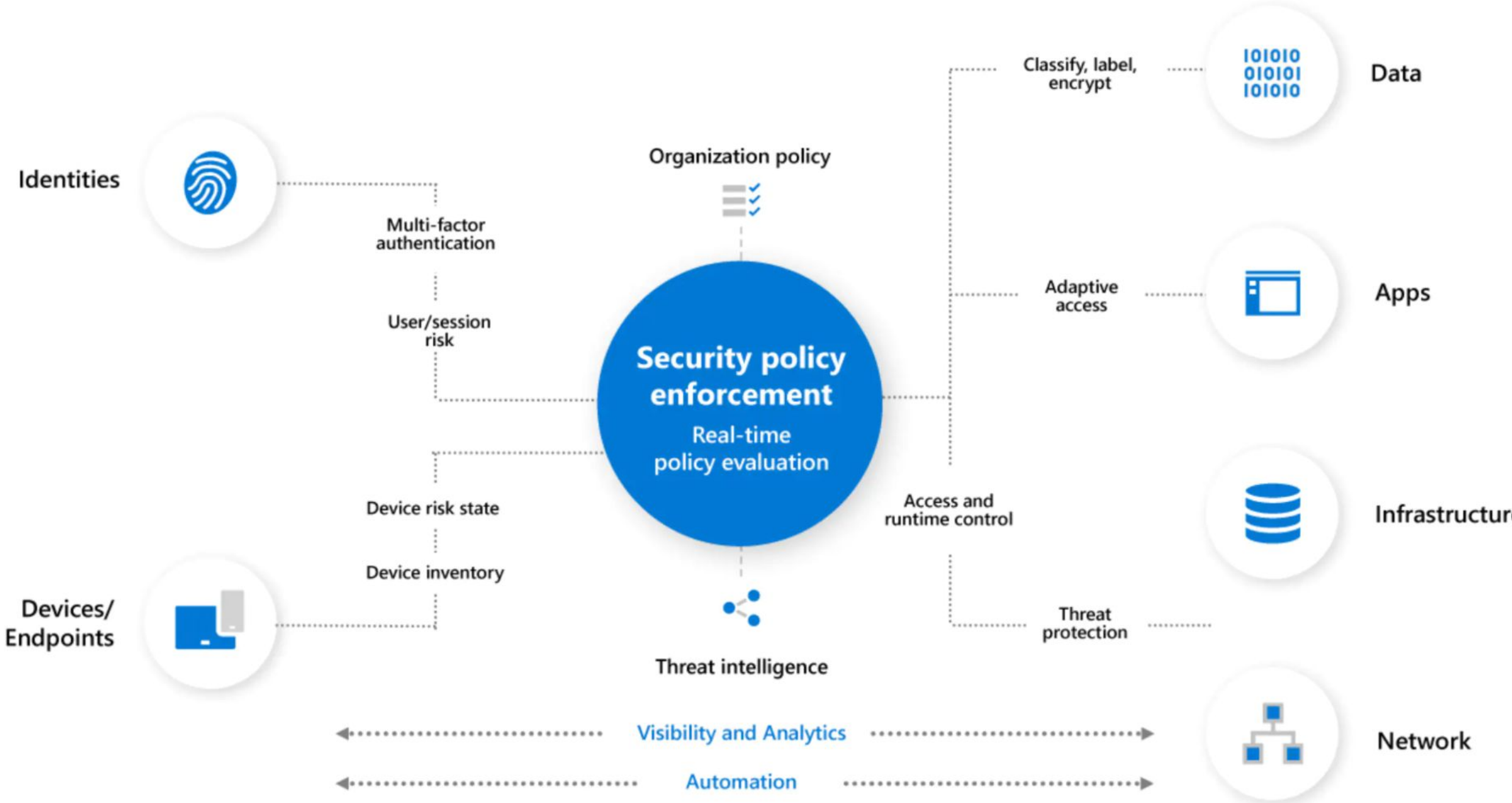
0h #$%©! 2 0ut of 18 Million Across Most of the Corporate World Have No Phish Protection.

SEAMLESS USER EXPIRIENCE

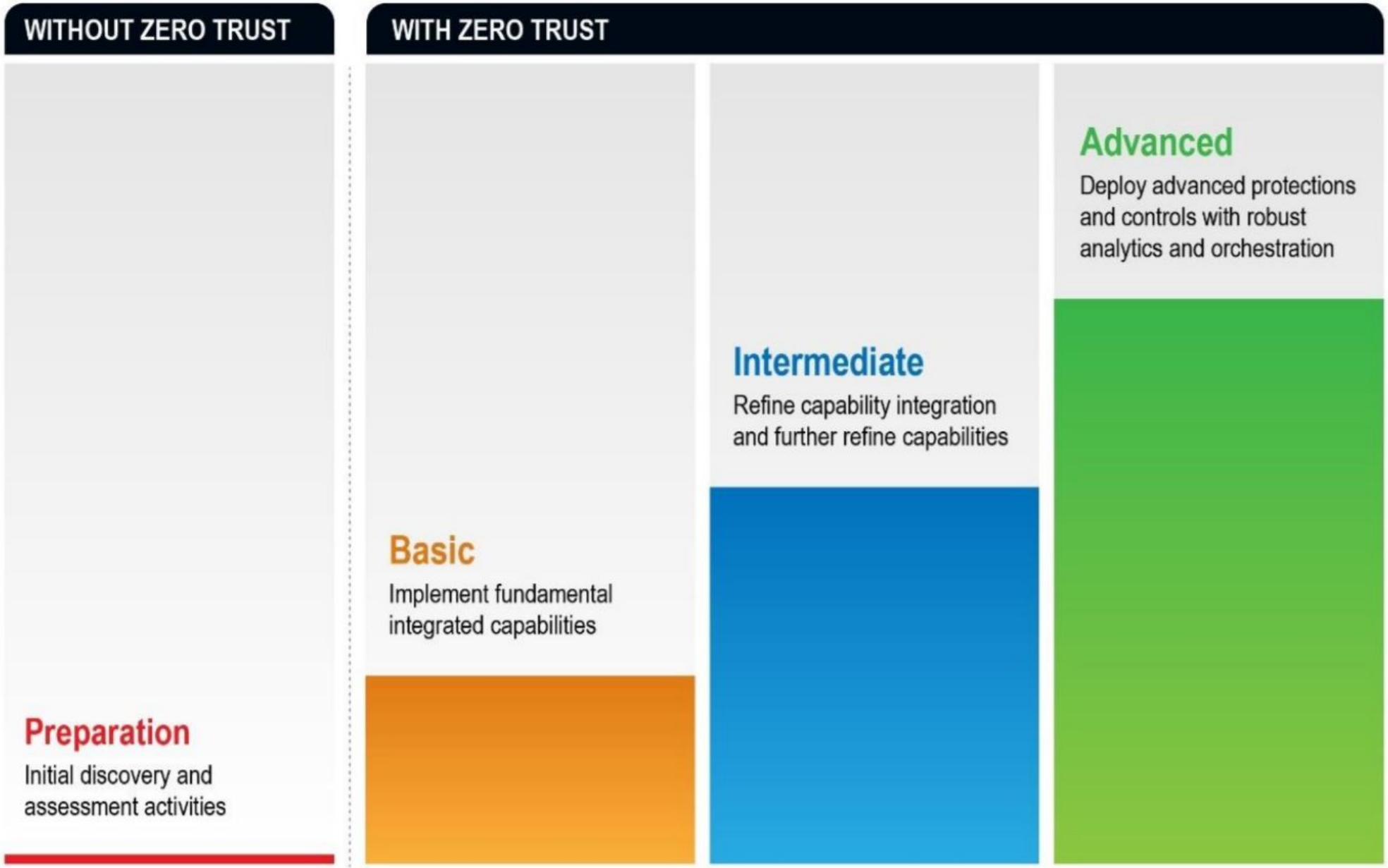
ZERO-DAY PHISHING SITE **PREVENTED**!

ACCOUNT TAKEOVER **PREVENTED**!




Identities
Multi-factor authentication
User/session risk
Device risk state
Device inventory
Devices/ Endpoints
Organization policy
Security policy enforcement
Real-time policy evaluation
Threat intelligence
Classify, label, encrypt
Data
Adaptive access
Apps
Access and runtime control
Infrastructur
Threat protection
Visibility and Analytics
Automation
Network

ZERO TRUST MATURITY



Check Point
SOFTWARE TECHNOLOGIES LTD

Summary

- Zero Trust is an Essential Strategy
- Implementation should be practical and easy to consume
- You need proper tools

CPX 360

THANK YOU

WELCOME TO THE FUTURE OF CYBER SECURITY