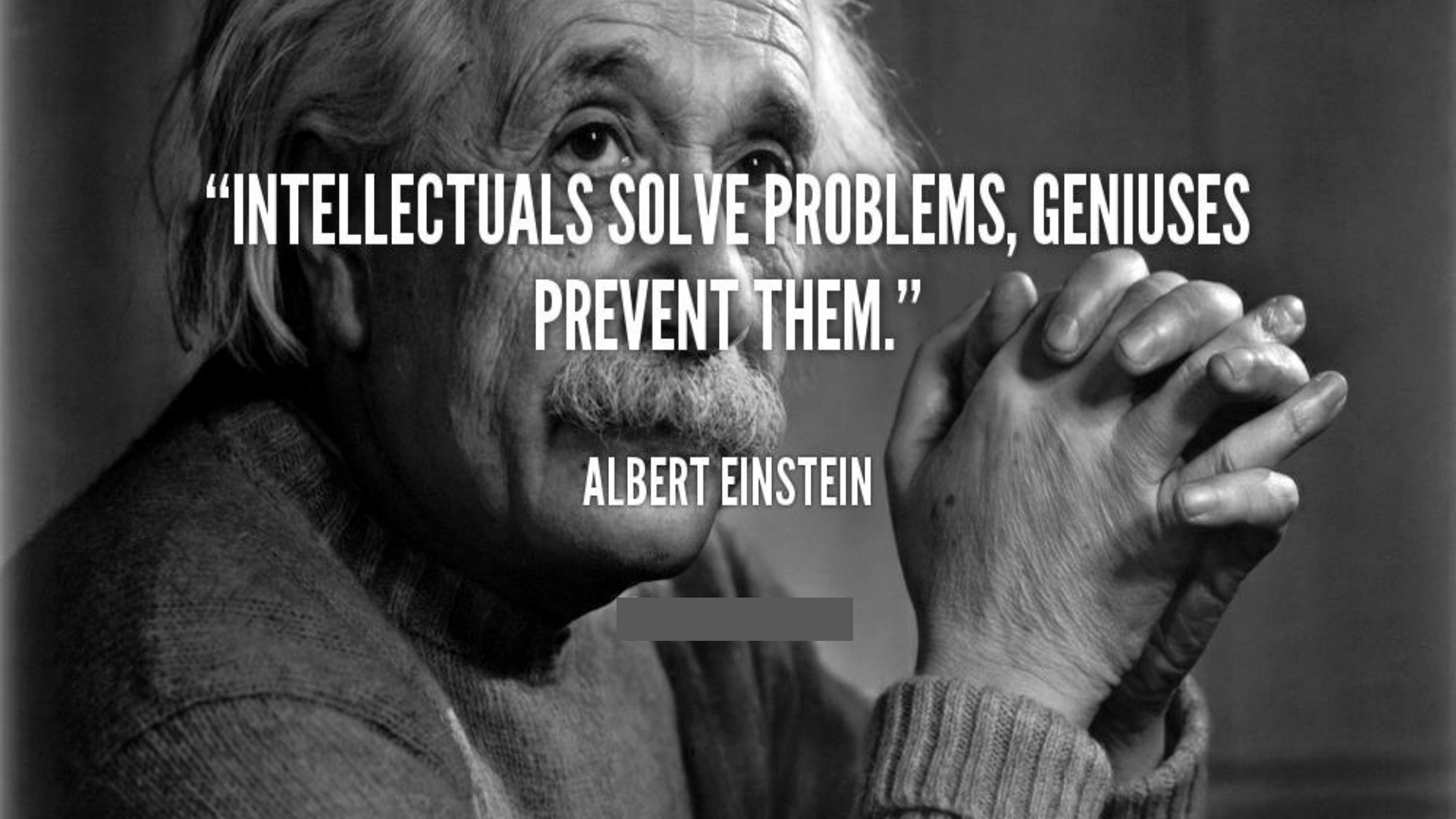
A practical strategy for Cyber Security

Fred Streefland
Cyber Security Strategist EMEA

paloalto NETWORKS®

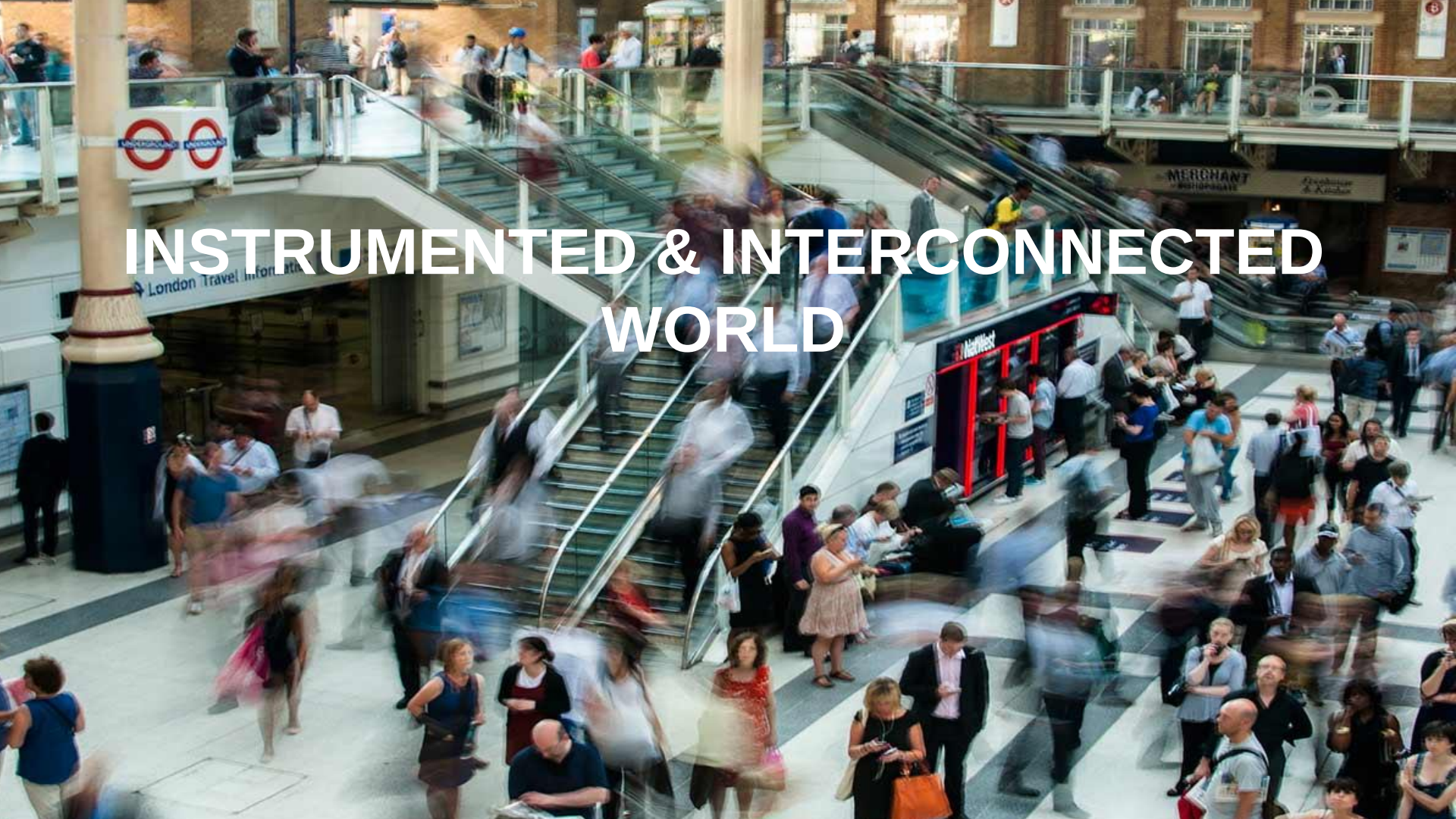
INTRODUCTION (SPEAKER)


“INTELLECTUALS SOLVE PROBLEMS, GENIUSES PREVENT THEM.”
ALBERT EINSTEIN

TO PROTECT OUR WAY OF LIFE IN THE DIGITAL AGE BY PREVENTING SUCCESSFUL CYBER ATTACKS

- Our Mission -

SO WHAT'S THE PROBLEM?


INSTRUMENTED & INTERCONNECTED WORLD
London Travel Inform
MERCHANT
NatWest

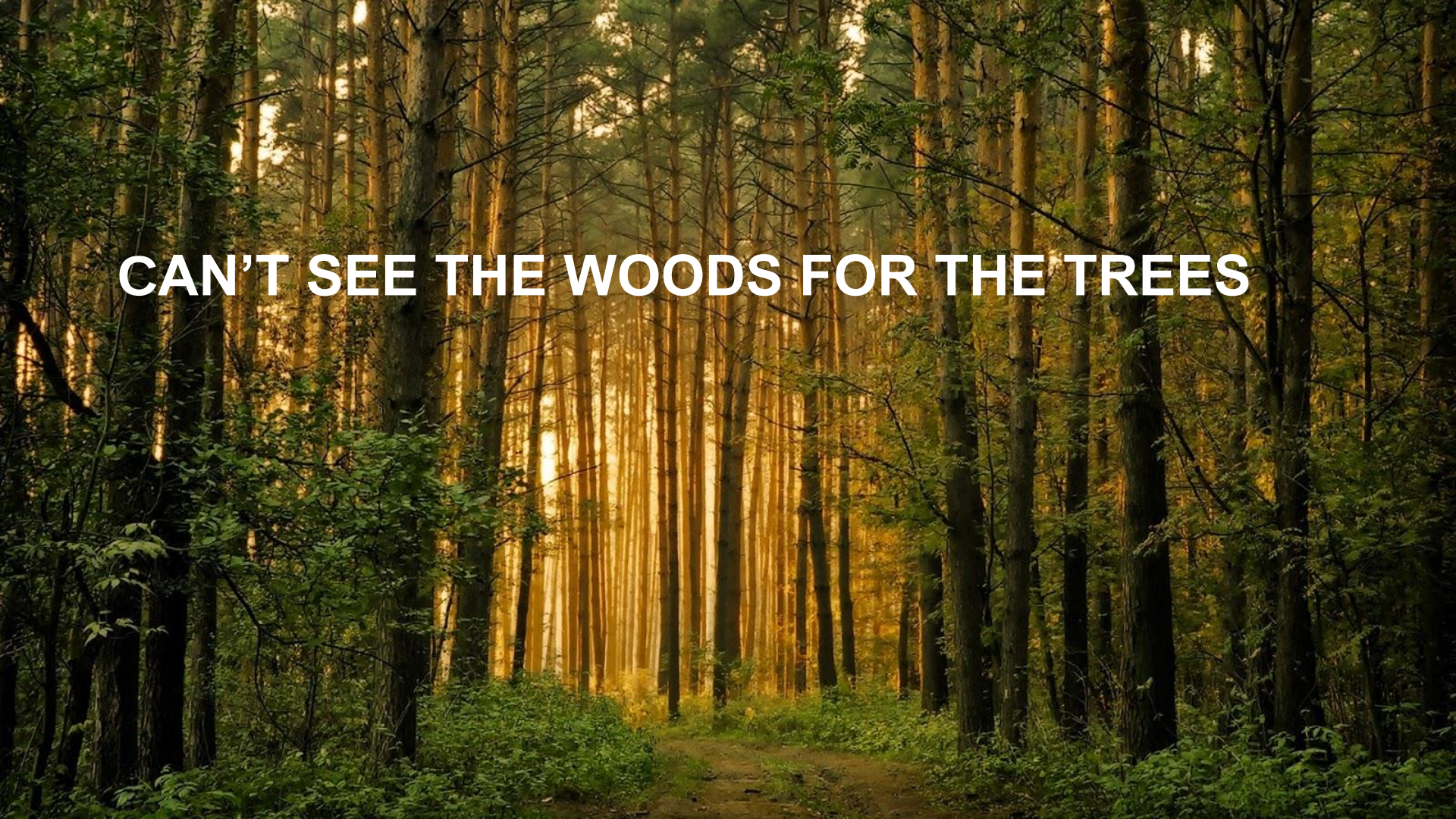
COMPLEX ORGANIZATIONS

COMPLIANCY & REGULATIONS

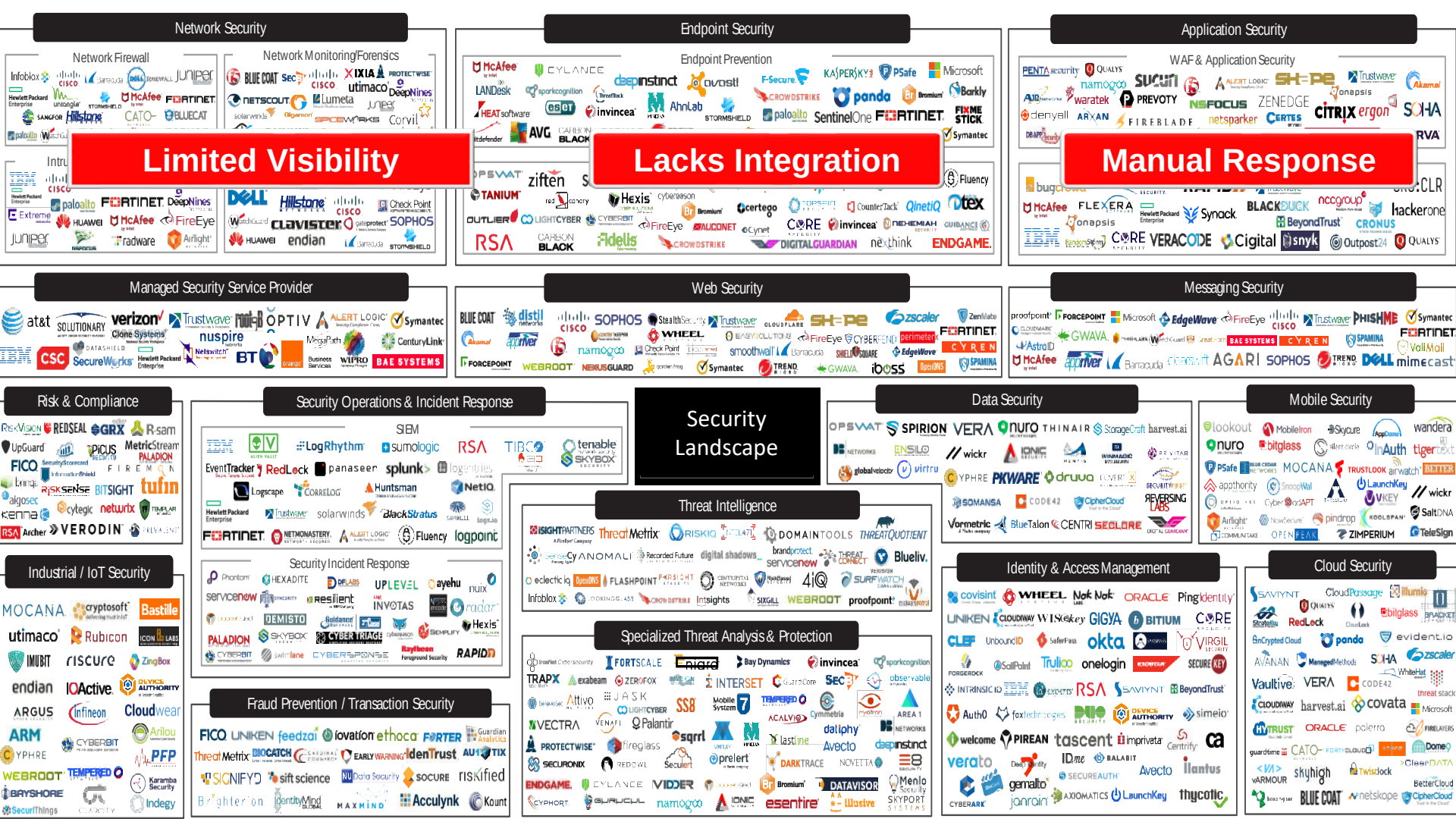
DIVERSE, EVOLVING AND HIGHLY AUTOMATED ADVERSARIES

BUSINESS GROWTH

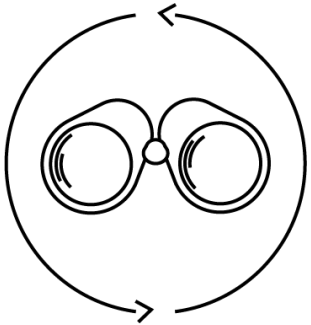

So, how can we handle these challenges…
…and secure the organization?

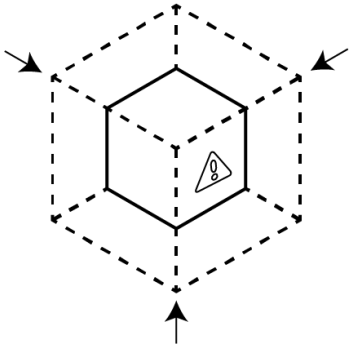

CAN’T SEE THE WOODS FOR THE TREES

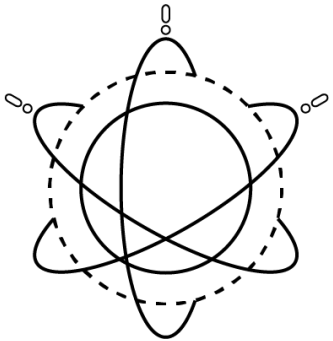

FROG BOG


Network Security
Network Firewall
Network Monitoring/Forensics
Endpoint Security
Endpoint Prevention
Application Security
WAF & Application Security
Limited Visibility
Lacks Integration
Manual Response
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Security Landscape
Threat Intelligence
Specialized Threat Analysis & Protection
Data Security
Mobile Security
Industrial / IoT Security
Fraud Prevention / Transaction Security
Identity & Access Management
Cloud Security

So, what's our approach?







COMPLETE VISIBILITY

REDUCE ATTACK SURFACE

PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

A holistic, integrated and automated approach…

COMPLETE VISIBILITY	REDUCE ATTACK SURFACE	PREVENT KNOWN THREATS	PREVENT UNKNOWN THREATS
• All applications • All users • All content • Encrypted traffic • SaaS • Cloud • Mobile	• Enable business apps • Block “bad” apps • Limit app functions • Limit file types • Block websites	• Exploits • Malware • Command & control • Malicious websites • Bad domains • Stolen credentials	• Static analysis • Machine Learning • Dynamic analysis • Bare metal anaylsis

...and consistent across ALL locations!

COMPLETE VISIBILITY → REDUCE ATTACK SURFACE → PREVENT KNOWN THREATS → PREVENT UNKNOWN THREATS

THINGS OR LOCATIONS THAT NEED TO BE SECURED


HEADQUARTERS


BRANCH OFFICES


DATA CENTER/ PRIVATE CLOUD

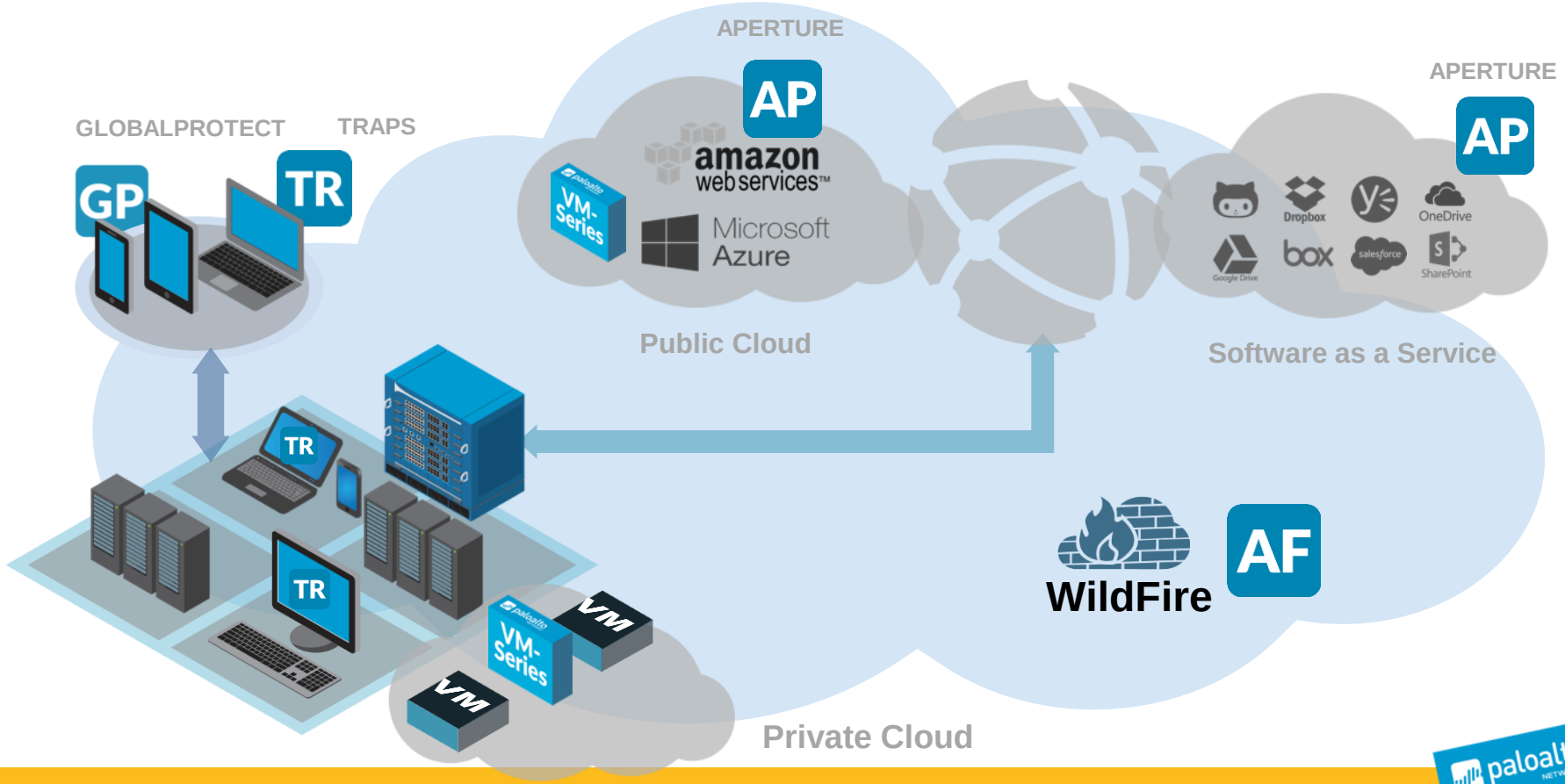
PUBLIC CLOUD

SAAS

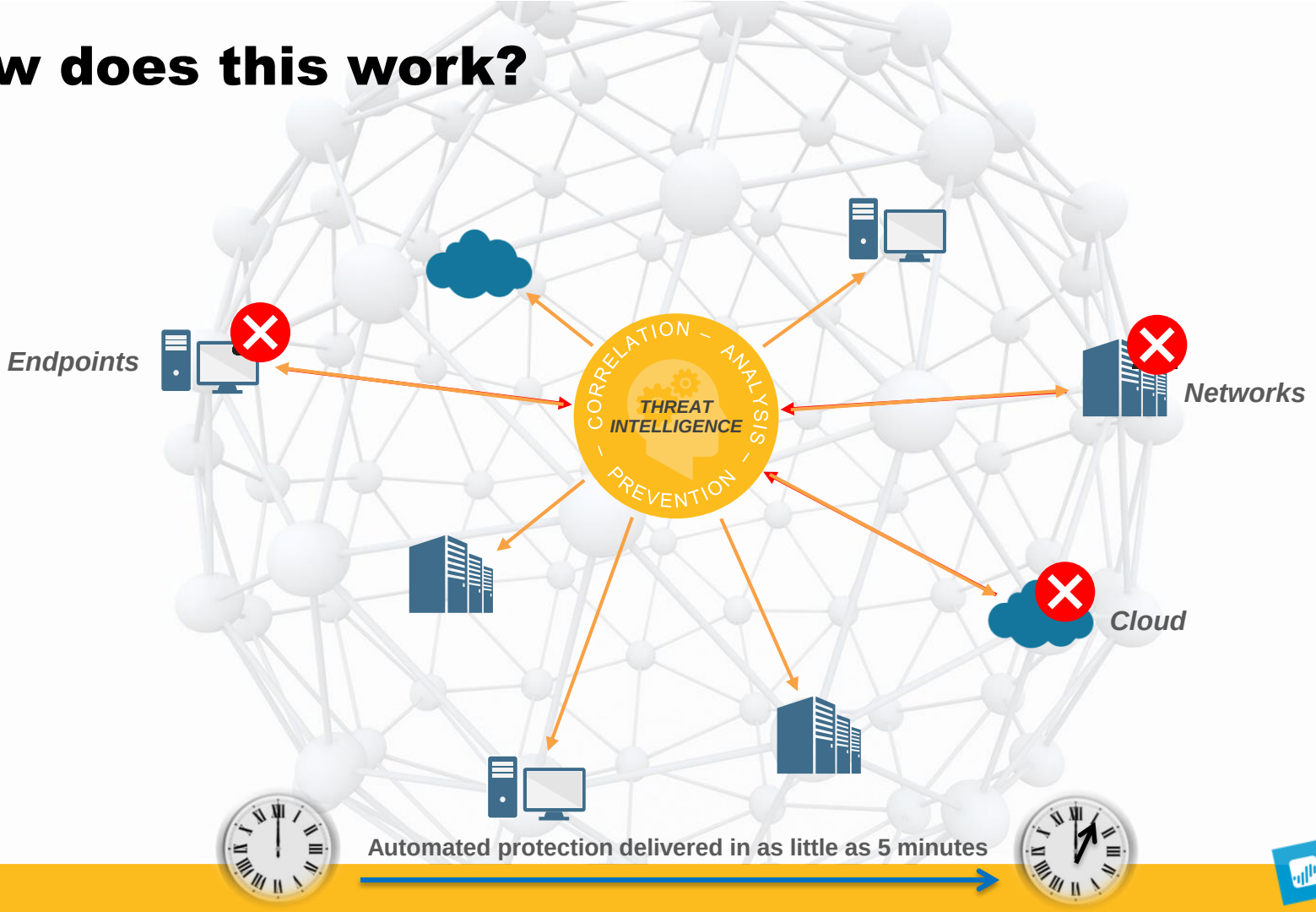

MOBILE USERS


IOT

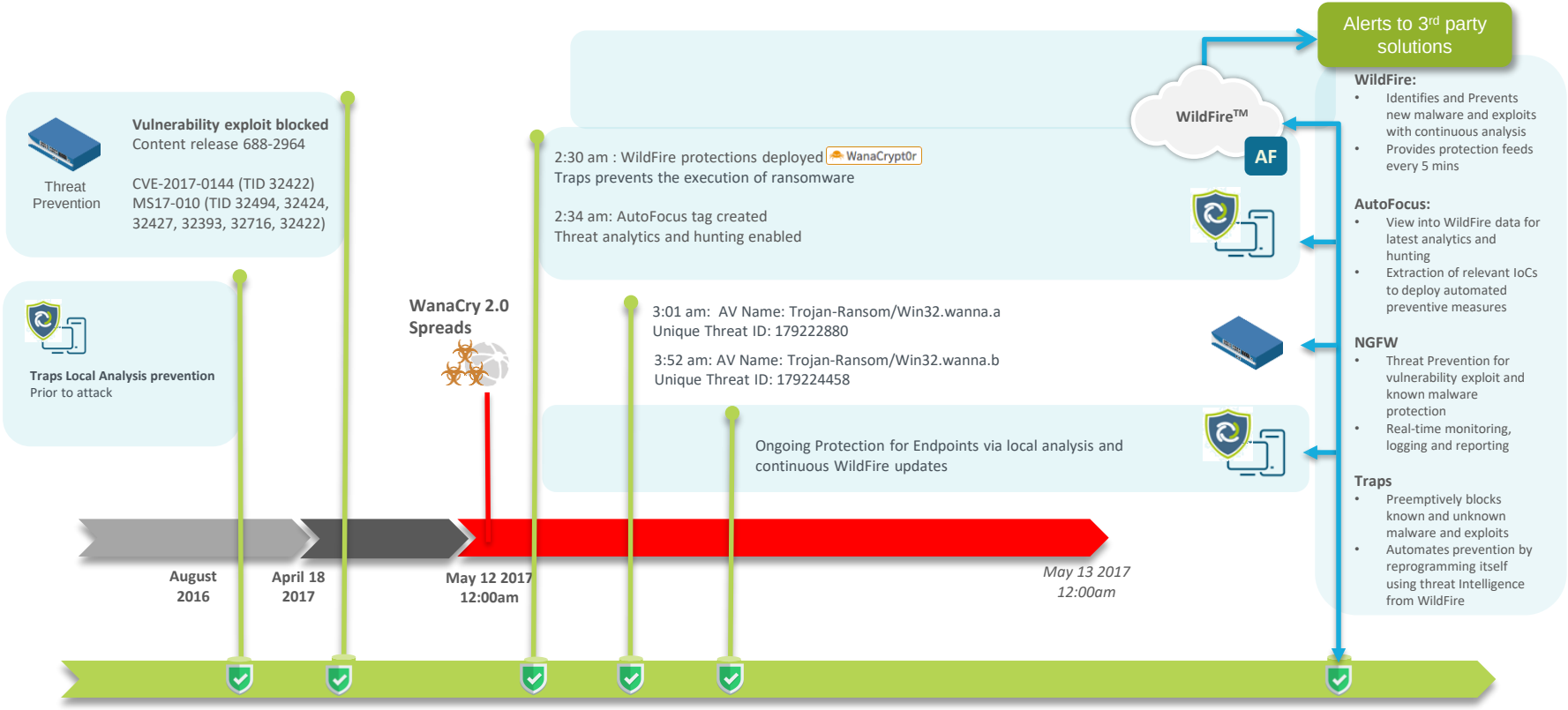
The Next-Generation Security Platform



How does this work?



How did this work?




RISKS
So, where do we….
START

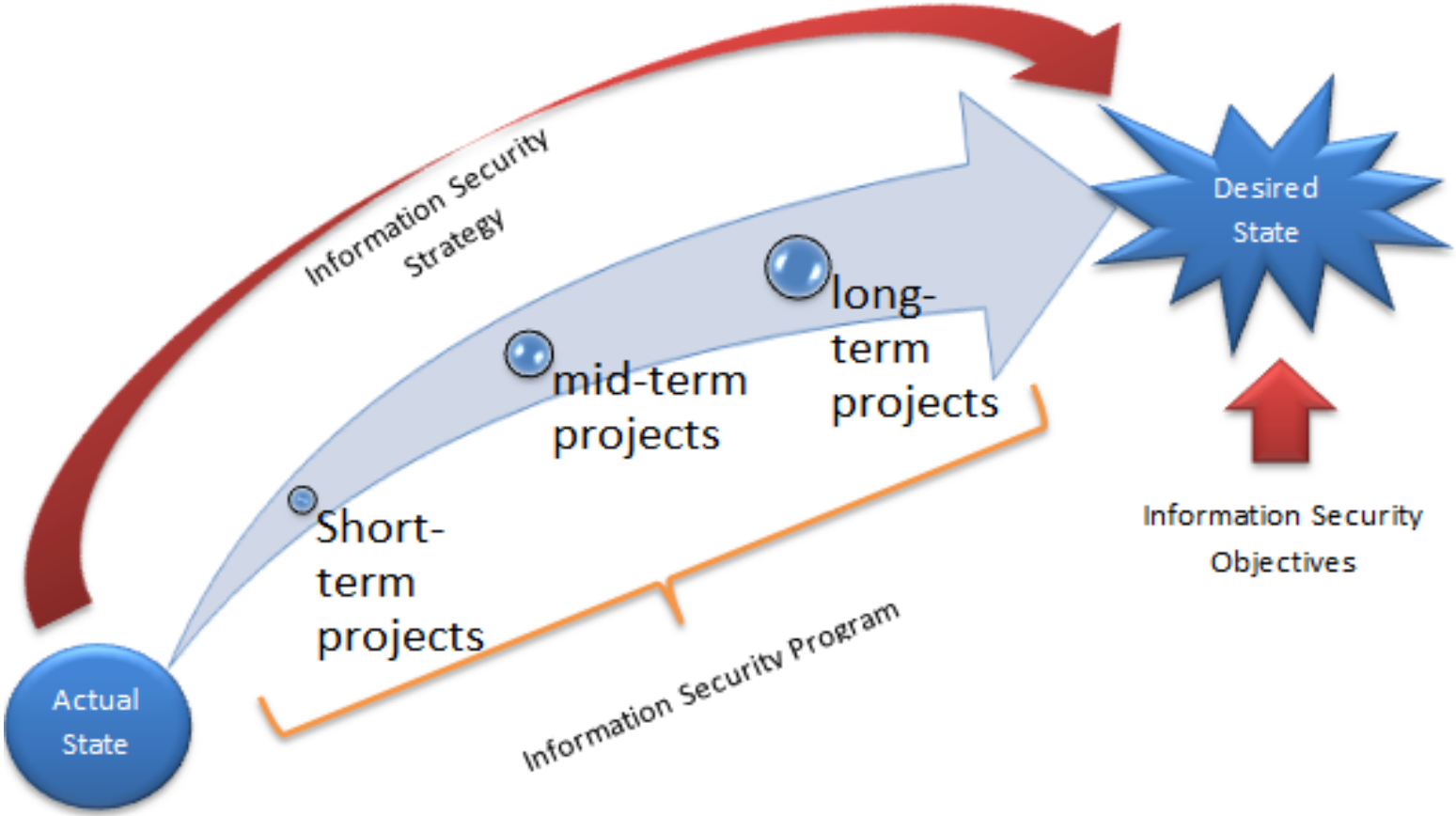

REDUCE
RISK


Zero Trust

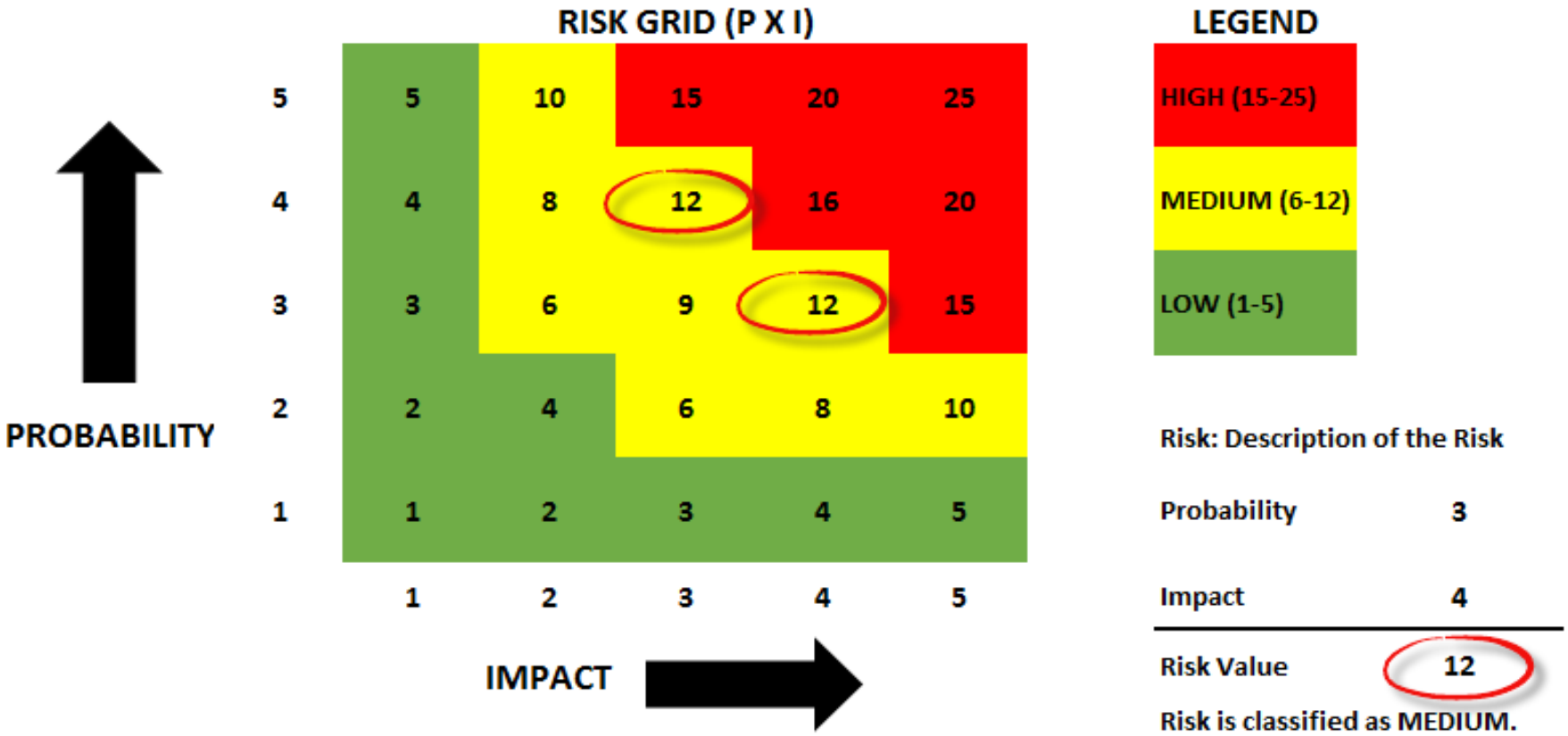
Zero Trust Design Concepts

- Focus on the business crown jewels (data)
- Design security from the Inside -> Out
  - Start with the assets or data that need protection
- Determine who or what needs access
  - Need to know/least-privilege
- Inspect and log all traffic

DESIRED END-STATE


Information Security Strategy
Desired State
long-term projects
mid-term projects
Short-term projects
Information Security Objectives
Actual State
Information Security Program


RISK ASSESSMENT WORKSHOPS


RISK GRID (P X I)
5 5 10 15 20 25
4 4 8 12 16 20
3 3 6 9 12 15
2 2 4 6 8 10
1 1 2 3 4 5
1 2 3 4 5
PROBABILITY
IMPACT
LEGEND
HIGH (15-25)
MEDIUM (6-12)
LOW (1-5)
Risk: Description of the Risk
Probability 3
Impact 4
Risk Value 12
Risk is classified as MEDIUM.

Home
Cockpit
Security news room
Documents
Meetings & minutes
Standards library
Glossary of ISMS Terms
Recent
EDIT LINKS

new item or edit this list

All Items ... Find an item

✓	#	Risk		Domain	CIA	Impact	Probability	Risk score	Global risk owner	Annex A control	Control status	Control Maturity (0-3)	Risk treatment status	Current residual risk	Residual risk substantiation	Entity risk exposure	Locatio
	1	Every employee has a lot of different accounts and a wide variety of logical and physical accounts; we loose the complete overview	...	Access control	Confidentiality	3	4	12	Security manager	A.12.1.1 Documented operating procedures	Implemented	2	Risk treatment in progress	10	We have an in- en uitdienst procedure in place. This formal procedure is covering most vital applications but does not provide the complete overview.		
	2	Accounts of a former employee are not timely revoked	...	Access control	Confidentiality	4	5	20	Security manager	A.7.3.1 Termination or change of employment responsibilities; A.9.2.1 User registration and de-registration; A.9.2.2 User access provisioning; A.9.2.6 Removal or adjustment of access rights	Implemented; Implemented; Implemented; Implemented	2; 2; 1; 2	Risk treatment in progress	8	We have an "in- en uitdienst" procedure in place. User registration is done by SysAdmin, who also provides AD permissions. There is a checklist procedure agreed between HR and SysAdmin		
	3	Misconfigure of an infrastructure firewall, which results in unauthorized access	...	Communications security	Confidentiality	2	3	6	Network operations manager	A.9.1.1 Access control policy; A.9.1.2 Access to networks and network services	Implemented; Implemented	2; 3	Risk treatment in progress	4	We have a formal change process in place (Network Infrastructure Change Management Process), back-up configs are performed, and new employees do not get access to critical infrastructure components.		


Priorities
1
2
3

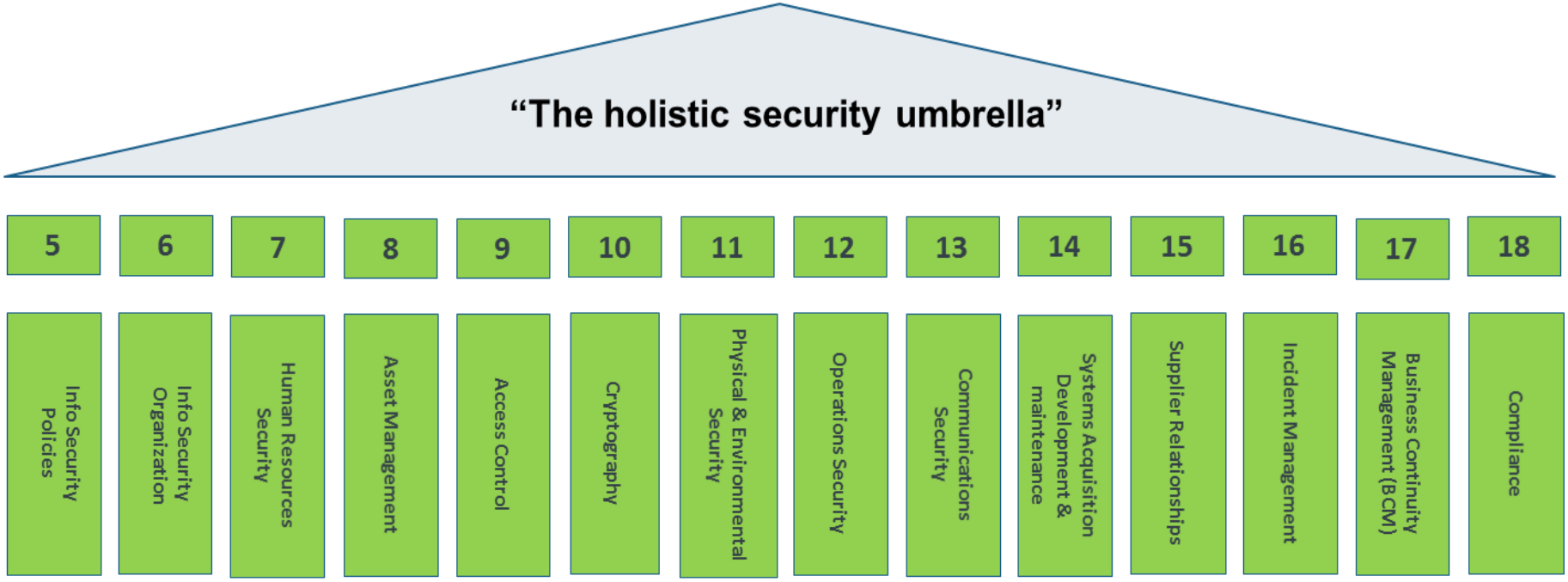

RISK APPETITE


FRAMEWORK

Figure 7—The 14 Control Domains of ISO/IEC 27001

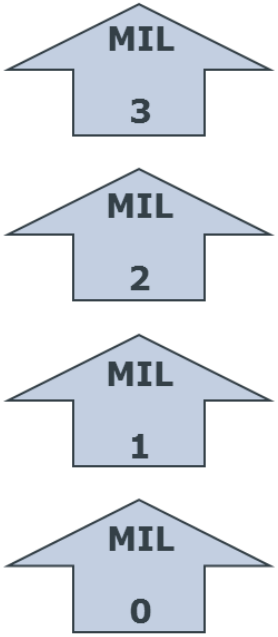
Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications security	7
A.14: System acquisition, development and maintenance	13
A.15: Supplier relationships	5
A.16: Information security incident management	7
A.17: Information security aspects of business continuity management	4
A.18: Compliance	8
TOTAL:	114

Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*


"The holistic security umbrella"
5
Info Security Policies
6
Info Security Organization
7
Human Resources Security
8
Asset Management
9
Access Control
10
Cryptography
11
Physical & Environmental Security
12
Operations Security
13
Communications Security
14
Systems Acquisition Development & maintenance
15
Supplier Relationships
16
Incident Management
17
Business Continuity Management (BCM)
18
Compliance


CYBER SECURITY MATURITY

Maturity Model*



- **Optimized:** Activities are guided by policies and reviewed periodically; responsibility and authority is clearly assigned and personnel have adequate skills and knowledge
- **Proficient:** Practices are documented; Stakeholders are involved; Resources are provided and Standards/guidelines are used
- **Basic**: Initial practices are performed, but may be ad hoc.
- **Incomplete**: Practices are not performed

* US DoE Cyber Security Maturity Model (CSM2)

Figure 7—The 14 Control Domains of ISO/IEC 27001

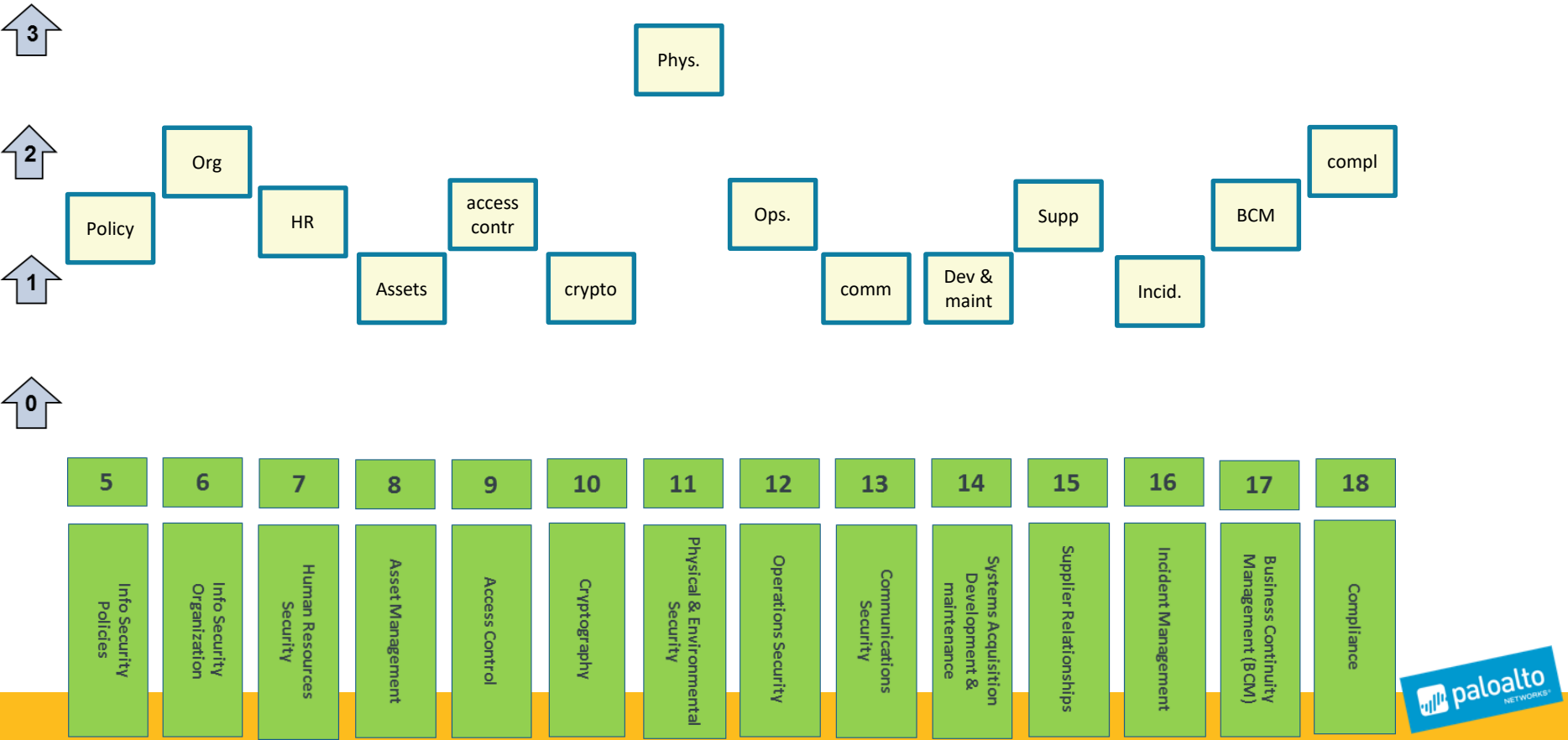
Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications security	7
A.14: System acquisition, development and maintenance	13
A.15: Supplier relationships	5
A.16: Information security incident management	7
A.17: Information security aspects of business continuity management	4
A.18: Compliance	8
TOTAL:	114

Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*

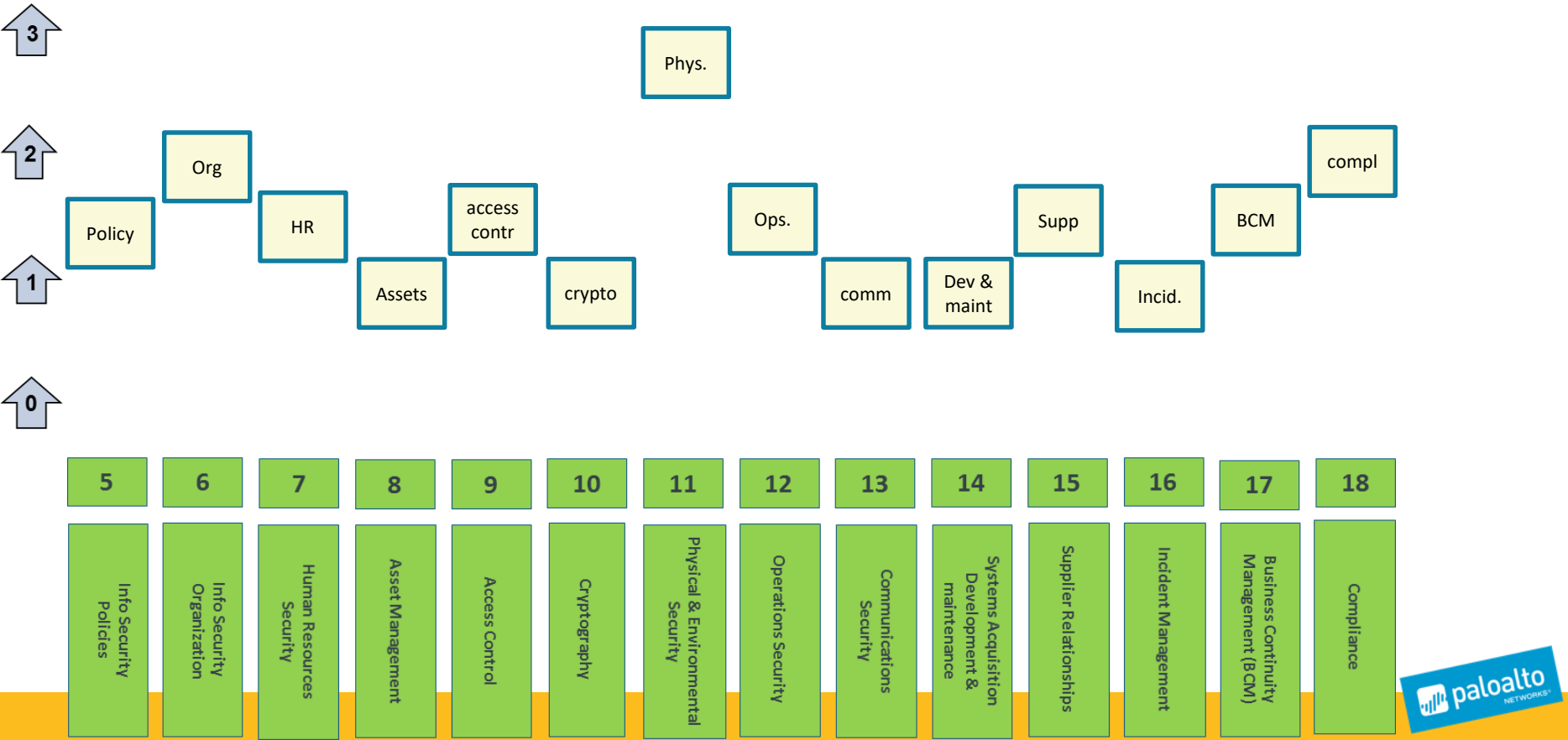
Maturity level 0, 1, 2 or 3 ?

Maturity level 0, 1, 2 or 3 ?

Start Situation



Desired End-state




HOW DO WE GET THERE?

Mitigating the risks with security projects…step-by-step

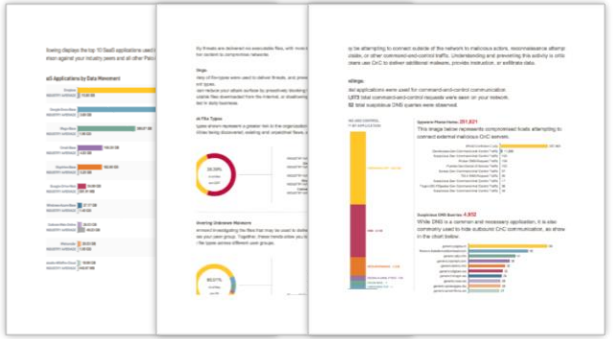
A. Security Policies
B. Next-Gen Firewalls (Palo Alto Networks, Fortinet, Checkpoint, etc.)
C. Security Awareness Program
D. Internal IT improvements like SMTP vulnerability
E. Laptop Encryption
F. Two-factor authentication (Safenet, OKTA, Ping, etc.)
G. Log Management (Splunk, LogPoint, Qradar, etc.)
H. End-point protection
I. Cloud/SaaS visibility & security (Aperture)
J. Local Admin rights take away
K. Network Segmentation
L. Skype for Business
M. Roles & Rights (Varonis)
N. SIEM/SOC project
O. Honeypots
P. Supplier Security requirements List

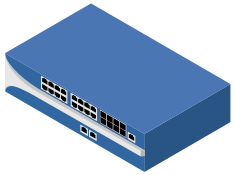
Your step-by-step security plan

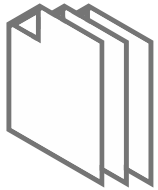
- **Get to know your IT environment**
  - Security Lifecycle Review (SLR)
- **Provide Security awareness training for all personnel**
- **Develop Information Security policies & Incident Response Plan**
- **Implement perimeter security & internal segmentation**
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- **Implement two-factor authentication**
- **Protect & manage Endpoints**
  - Local Admin, Encrypt & Install Traps
- **Implement Cloud security (Aperture)**
- **……**

Security Lifecycle Review (SLR)

- A customized **Risk Assessment** for your organization
- Visibility into the applications, malware, vulnerability exploits and more on your network







WE PUT THE DEVICE ON THE NETWORK

WE PASSIVELY MONITOR TRAFFIC FOR 1 WEEK

WE DELIVER THE REPORT & EXPLAIN THE FINDINGS

Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- **Provide Security awareness training for all personnel**
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……

Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- **Develop Information Security policies & Incident Response Plan**
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……

Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- **Implement perimeter security & internal segmentation**
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……

Perimeter security and segmentation

+

+

FORTINET

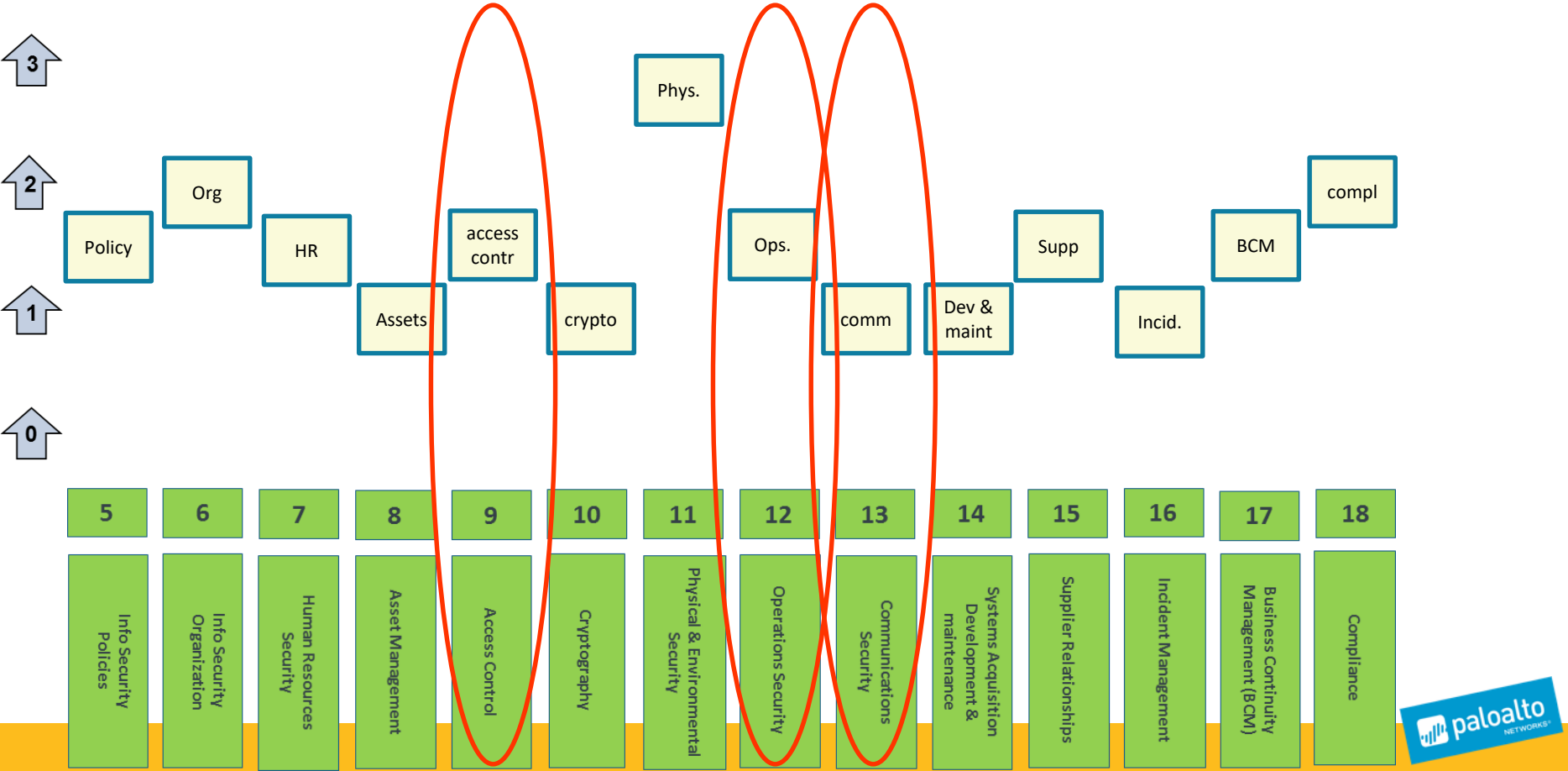
Check Point
SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

paloalto NETWORKS

paloalto NETWORKS

Next-Generation Firewalls & Threat Int. Cloud



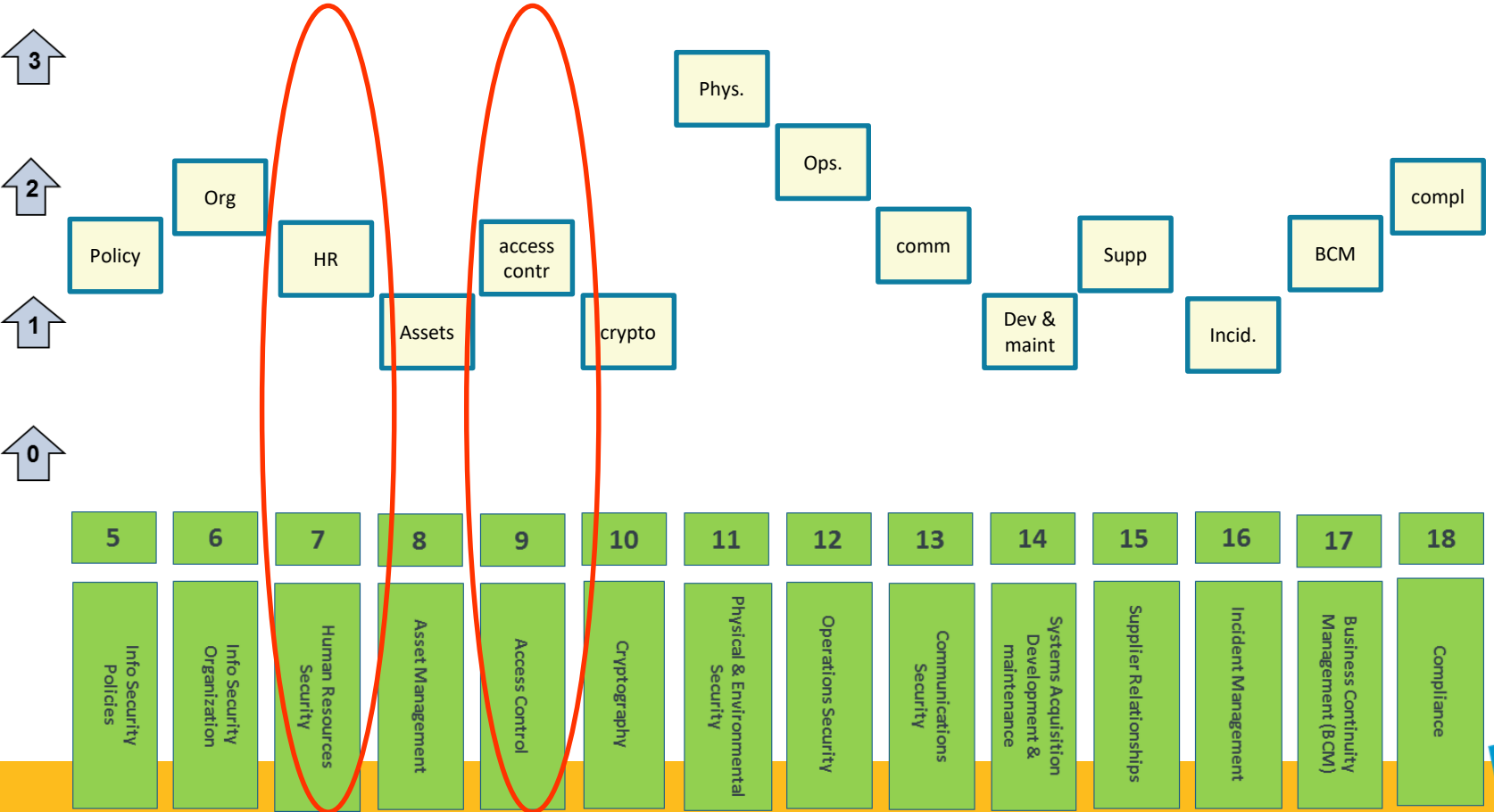
Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- **Implement two-factor authentication**
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- .....

Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- **Protect & manage Endpoints**
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- .....

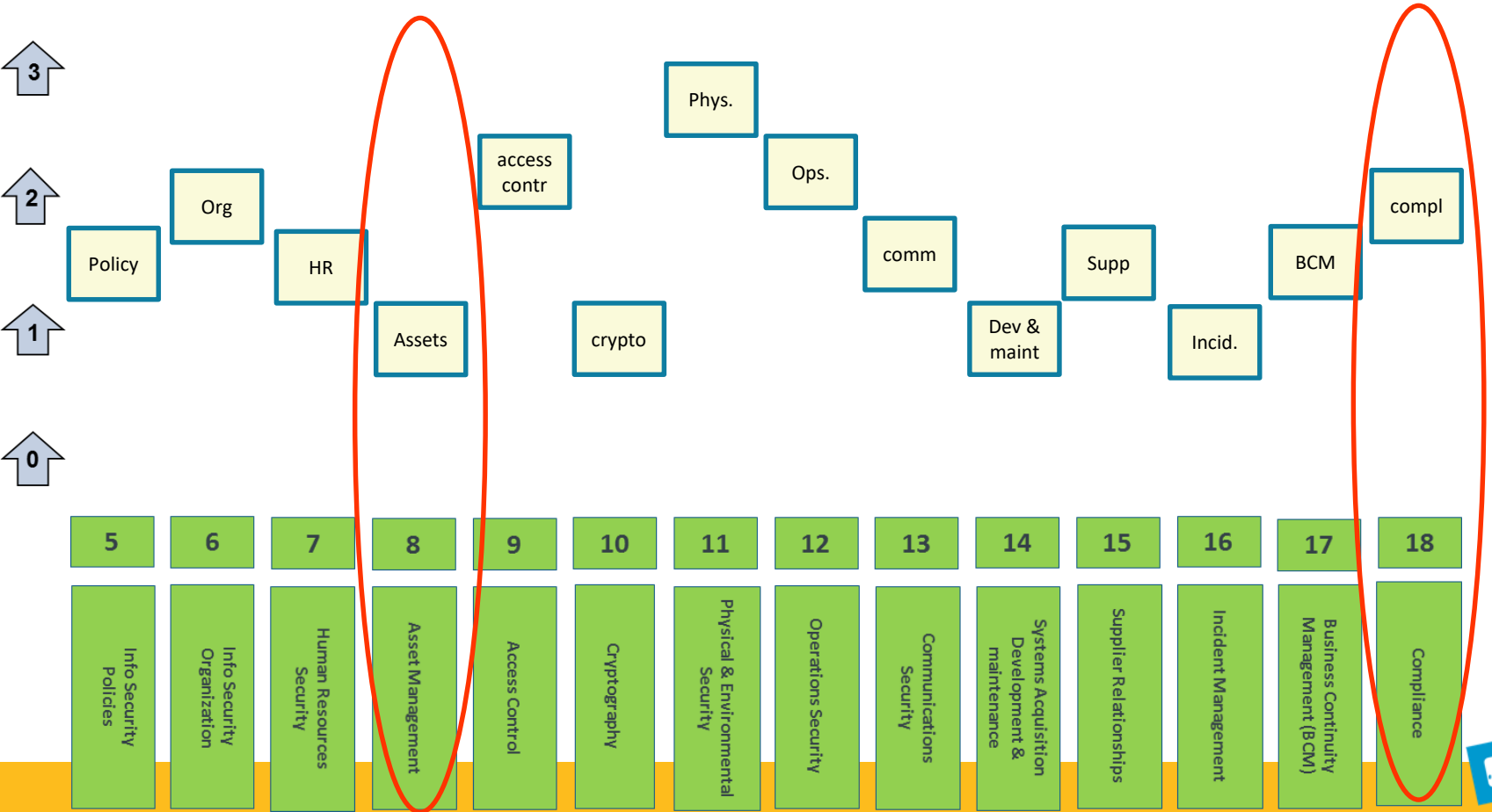
Protect & Manage Endpoints (Traps)



Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- **Implement Cloud security (Aperture)**
- ……

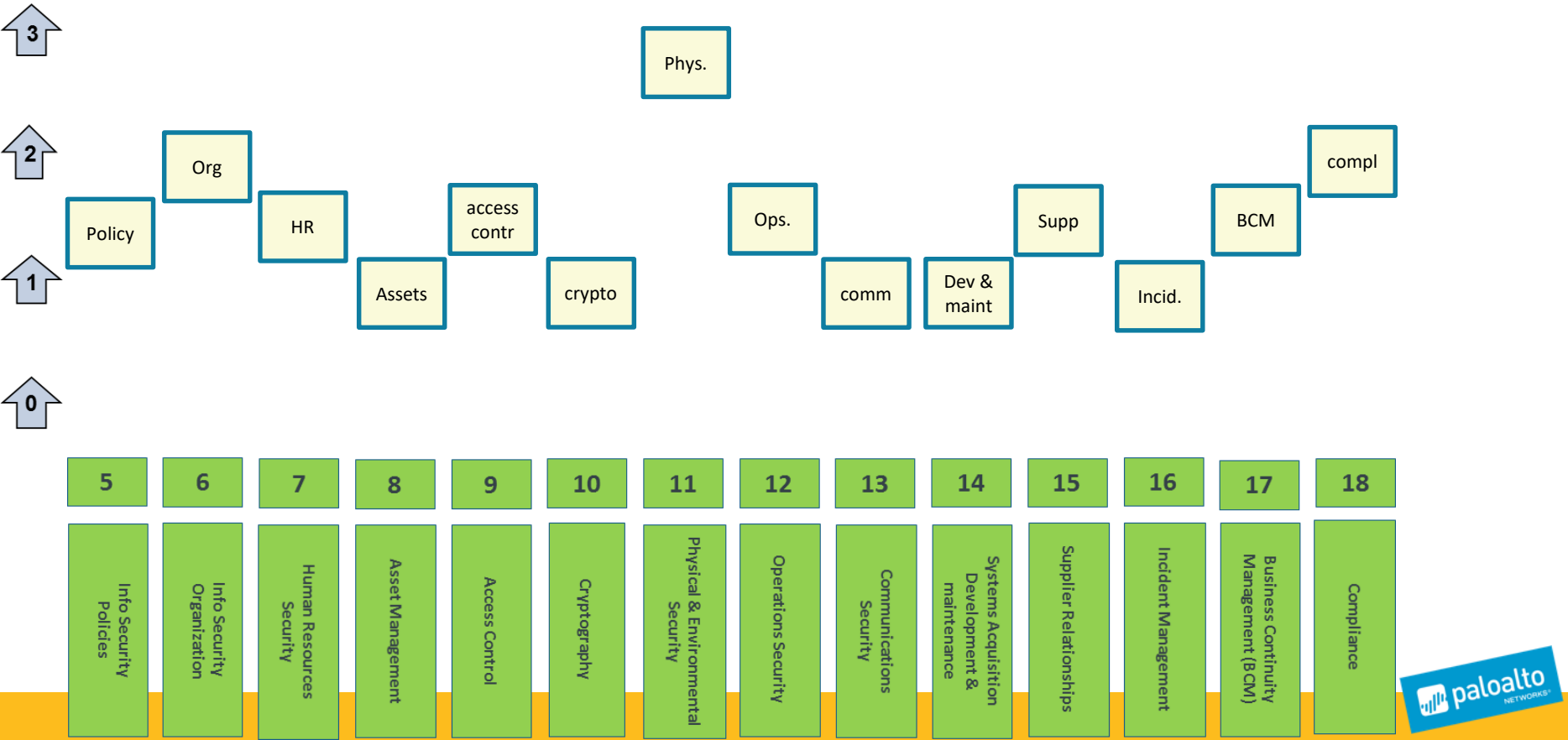
Implement Cloud Security (Aperture)

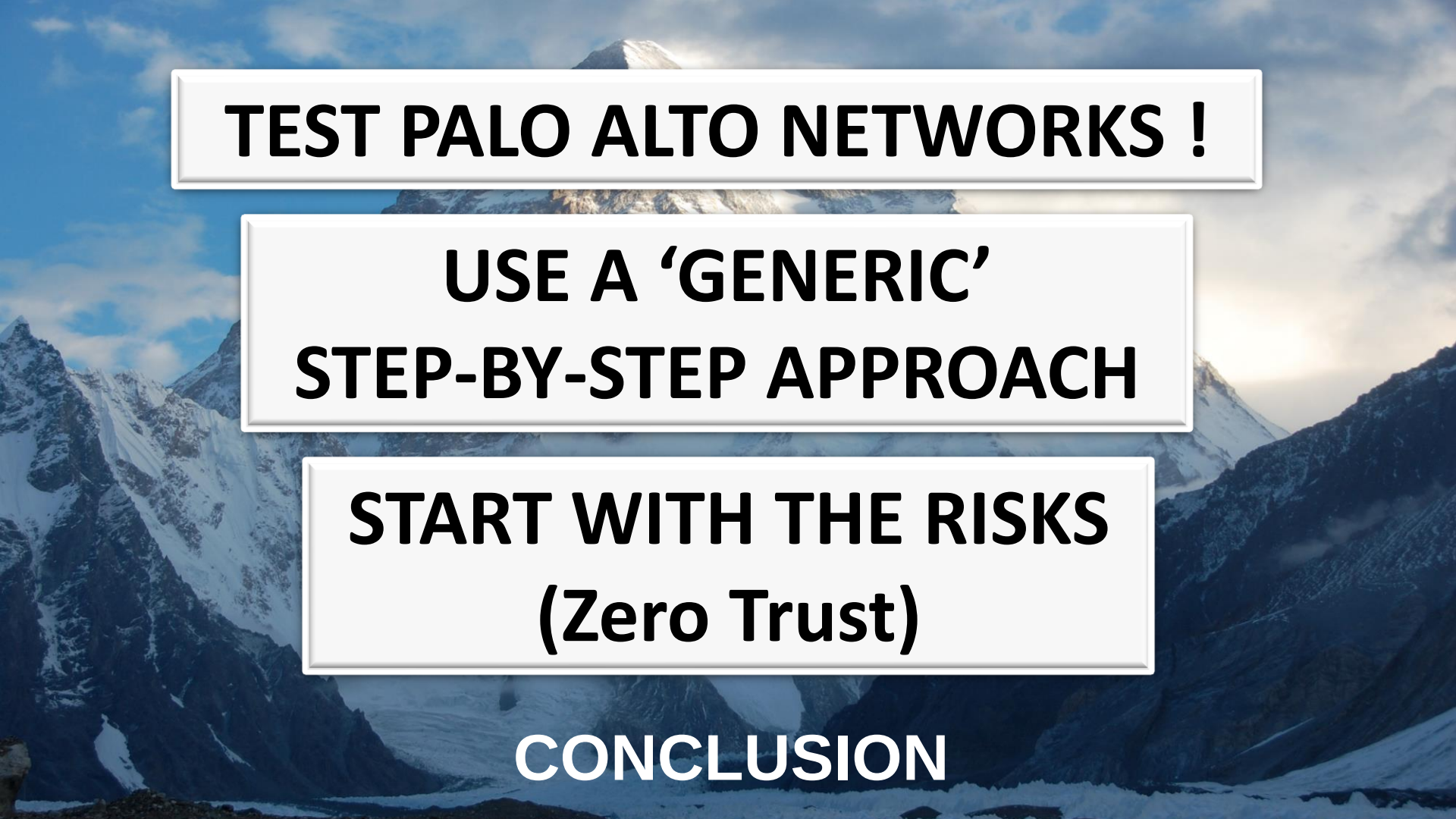


Your step-by-step security plan

- **Get to know your IT environment**
  - Security Lifecycle Review (SLR)
- **Provide Security awareness training for all personnel**
- **Develop Information Security policies & Incident Response Plan**
- **Implement perimeter security & internal segmentation**
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- **Implement two-factor authentication**
- **Protect & manage Endpoints**
  - Local Admin, Encrypt & Install Traps
- **Implement Cloud security (Aperture)**
- **……**

....so you can reach your goal !




TEST PALO ALTO NETWORKS !
USE A ‘GENERIC’
STEP-BY-STEP APPROACH
START WITH THE RISKS
(Zero Trust)
CONCLUSION

THANK YOU FOR YOUR ATTENTION !

FStreefland@PaloAltoNetworks.com

nl.linkedin.com/in/fredstreefland

+31 6 28461593