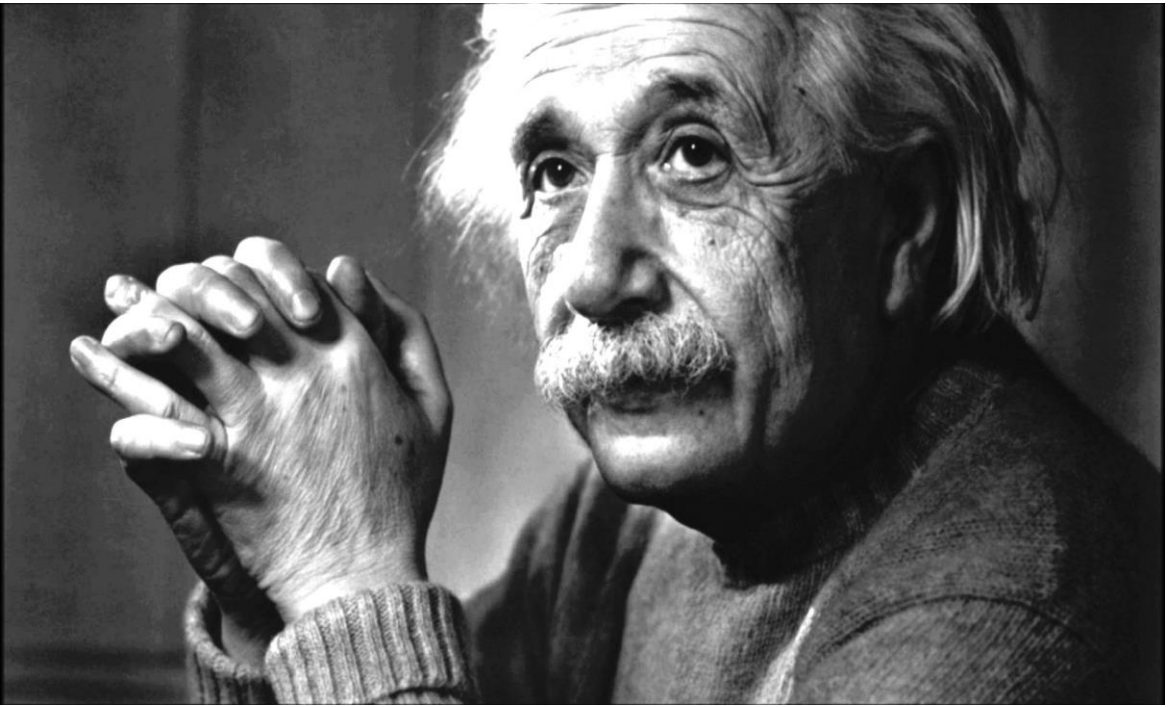
How to secure On-premise and Cloud?

- *'war stories' of a former CISO* -

Fred Streefland
Sr. Product Marketing Manager EMEA

paloalto NETWORKS®

INTRODUCTION (SPEAKER)



“INTELLECTUALS SOLVE PROBLEMS, GENIUSES PREVENT THEM.”

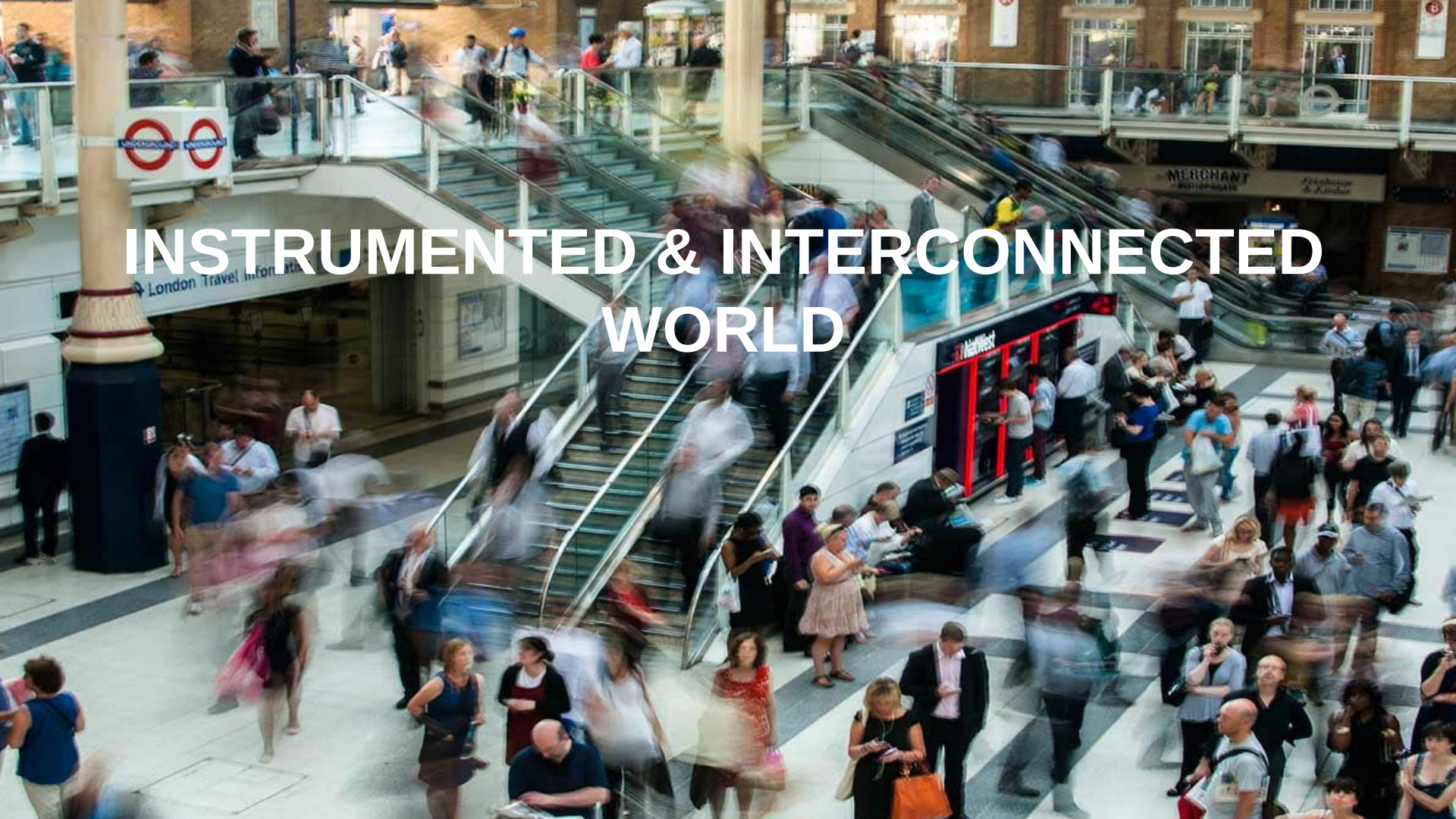
ALBERT EINSTEIN

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

- Our Mission -

PROTECT OUR BUSINESS!

SO, WHAT'S THE PROBLEM?


INSTRUMENTED & INTERCONNECTED WORLD
London Travel Inform
MERCHANT
NatWest

COMPLEX ORGANIZATIONS

COMPLIANCY & REGULATIONS

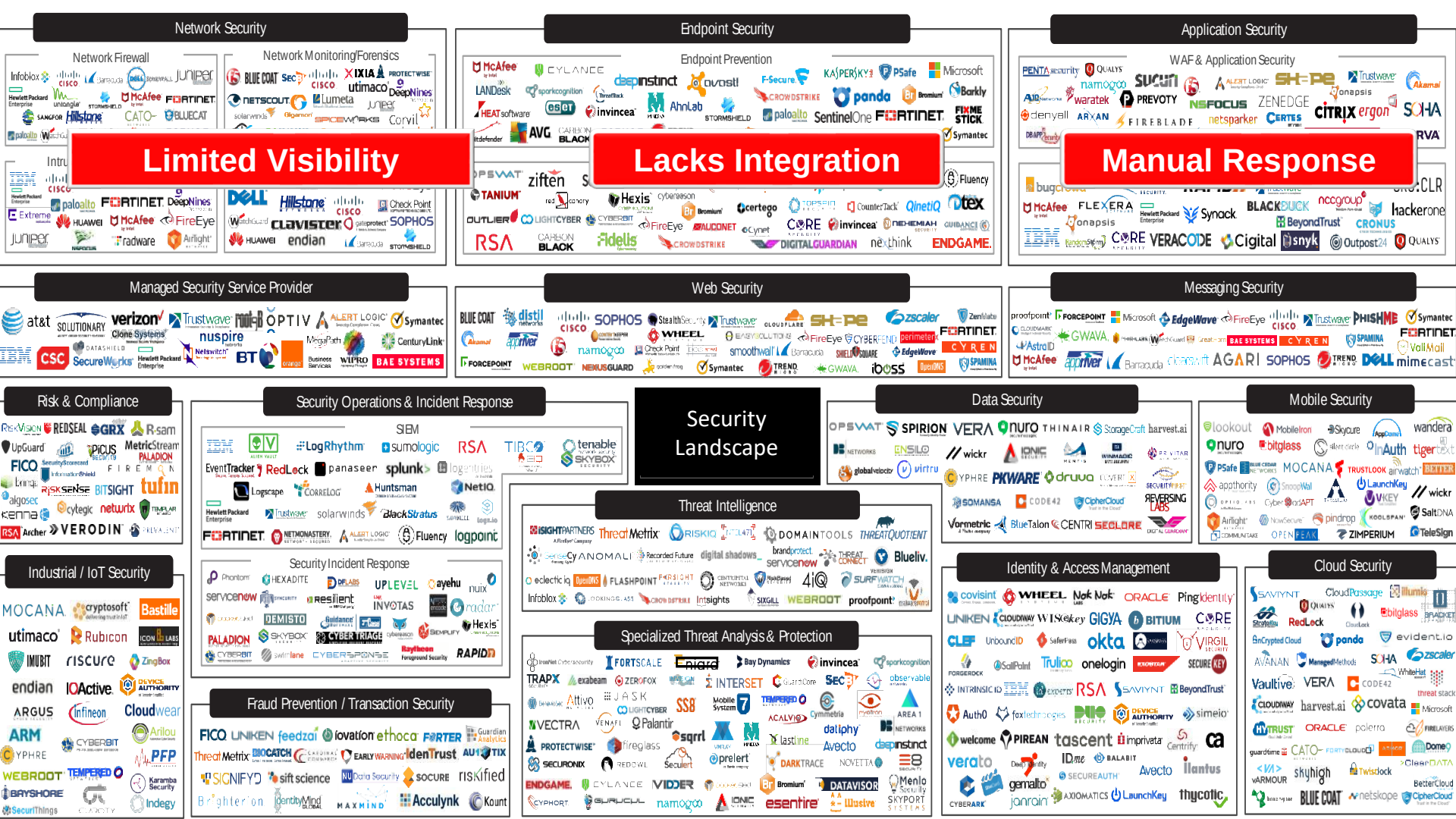
DIVERSE, EVOLVING AND HIGHLY AUTOMATED ADVERSARIES

BUSINESS GROWTH

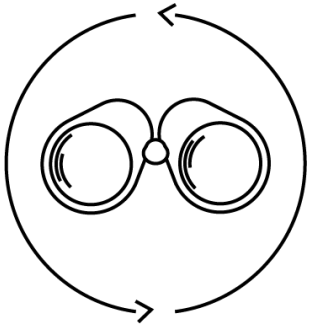

So, how can we handle these challenges…
…and secure the organization?

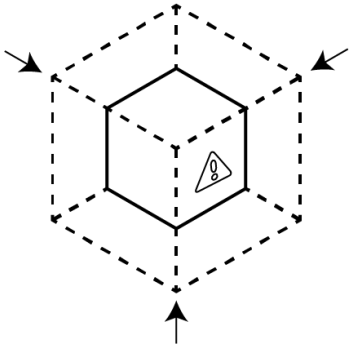

CAN’T SEE THE WOODS FOR THE TREES

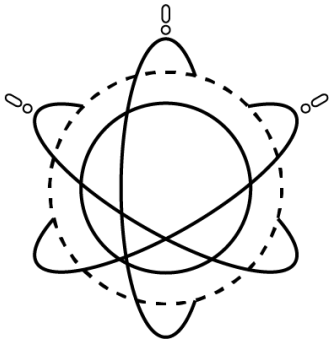

FROG BOG


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

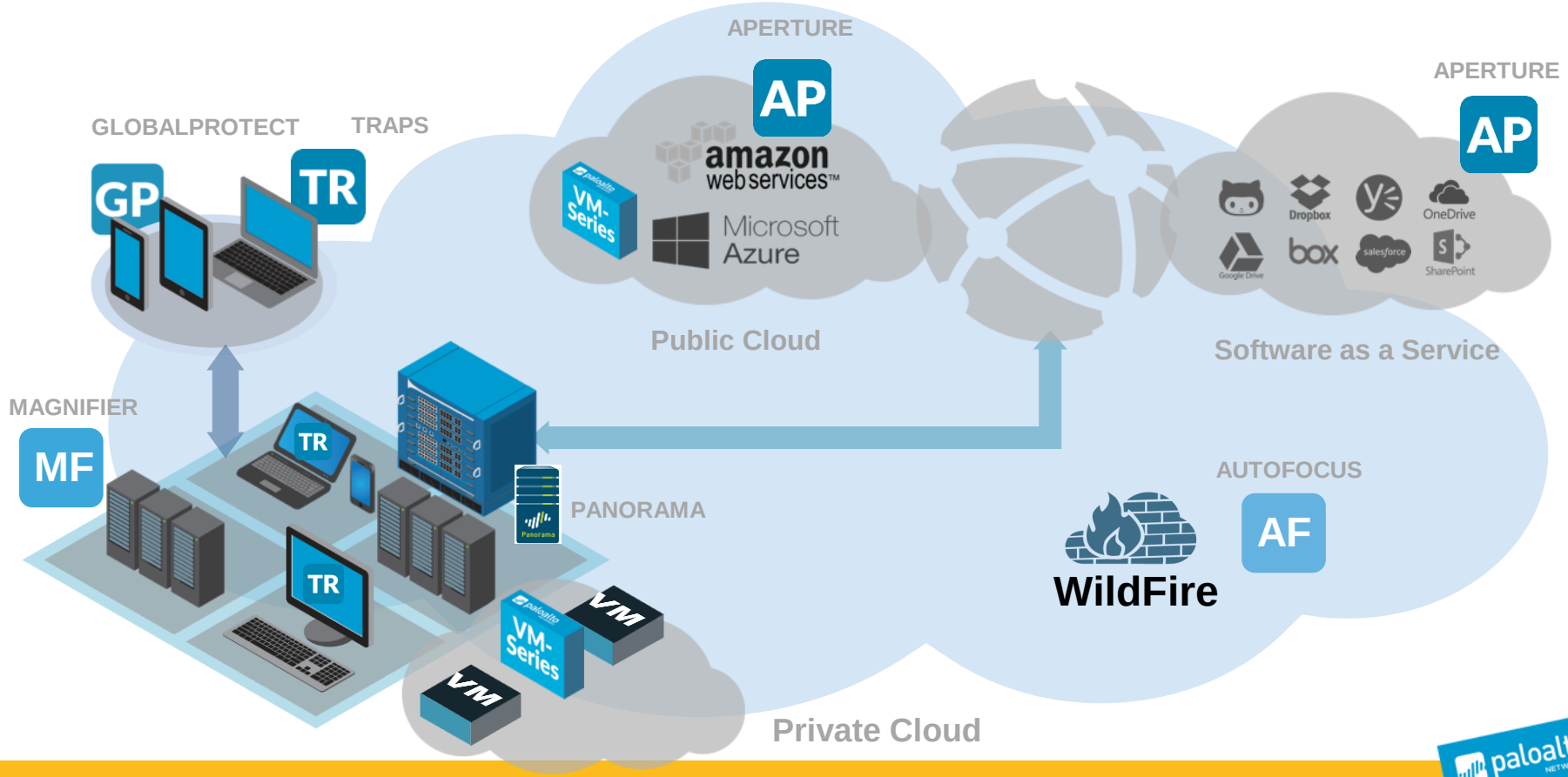
PUBLIC CLOUD

SAAS


MOBILE USERS


IOT

The result: Next-Generation Security Platform

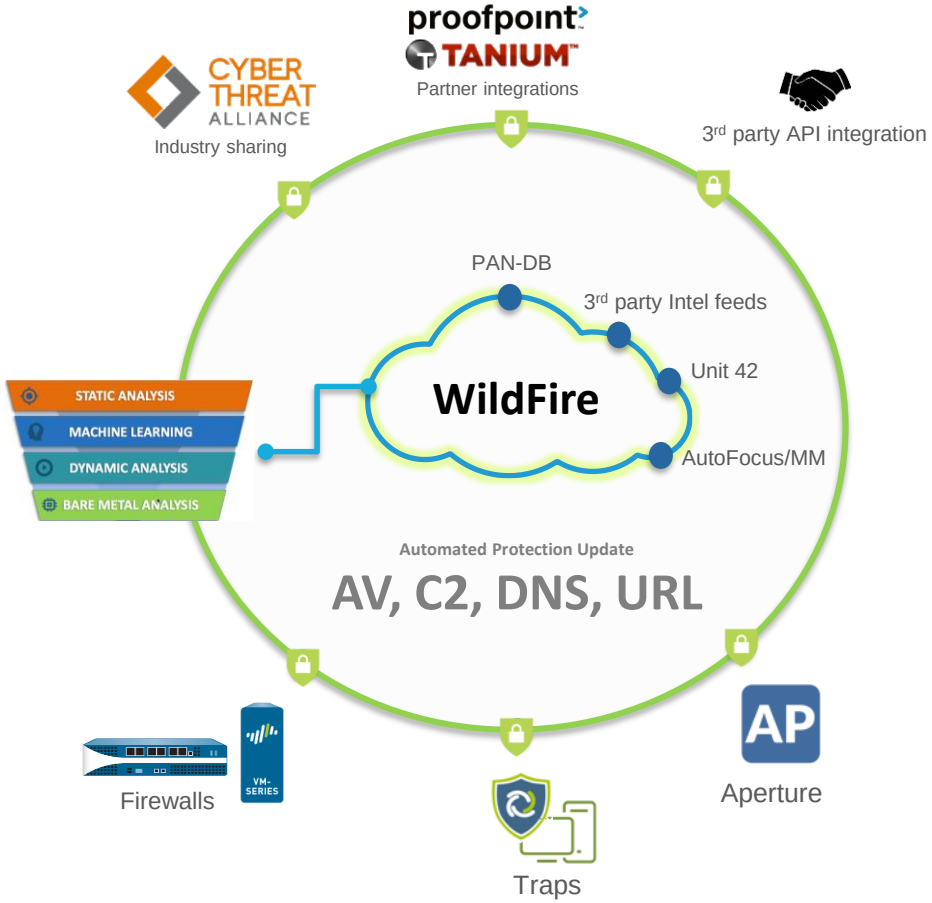


How does this work? (1)

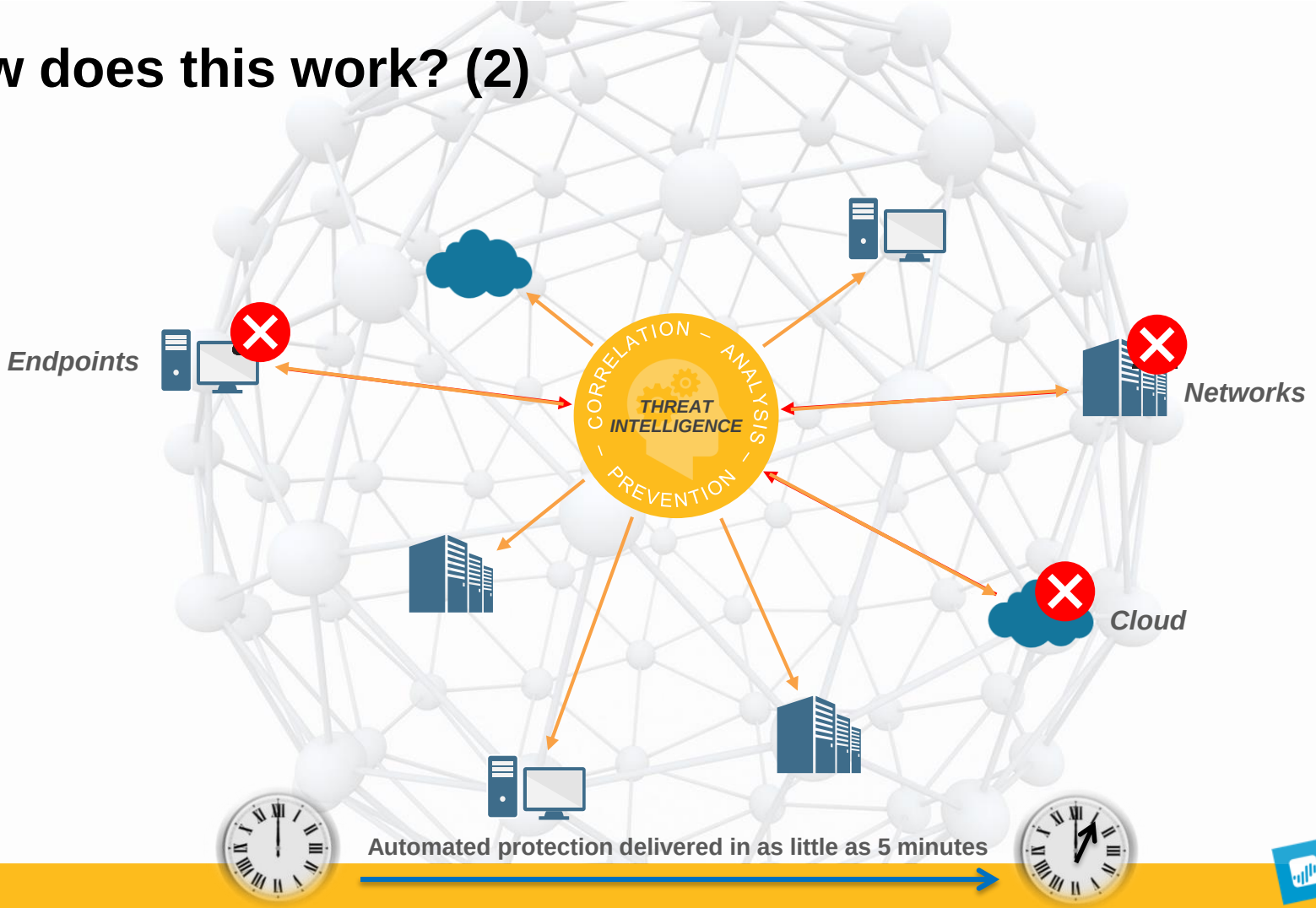
215M+
Never-before-seen samples every month

230,000+
New protections delivered daily

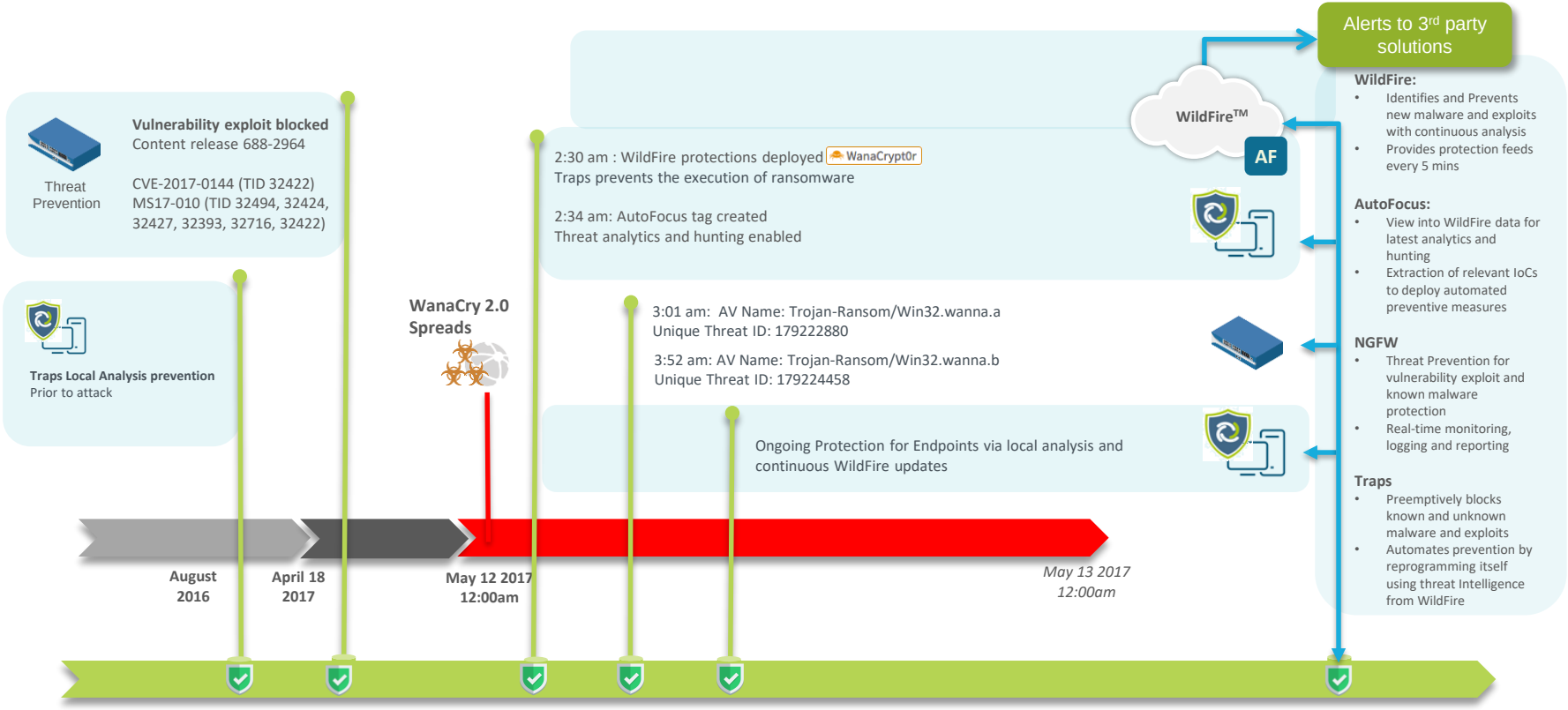
5min
Automated Protection Update



How does this work? (2)



How did this work?




SO, WHERE DO WE….
START


REDUCE
RISK


ZERO TRUST
Who is the President?
Where is the President?
Who has access to the President?

ZERO TRUST principles:

1) What & where are your crown jewels?

2) Design Security ‘Inside-Out’
   - Start with the core assets that need protection

3) Who or what has access?
   - Least Privilege

4) Inspect & log all traffic

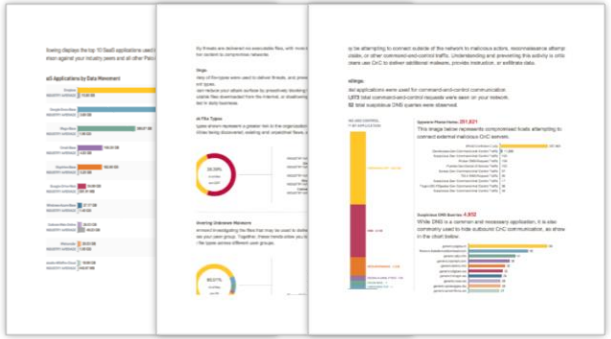

SECURITY PLAN
Information systems
Protection
Internet attack
Cyber security
Internet
Mobile devices
Computer

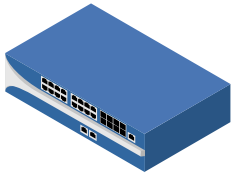
Priorities

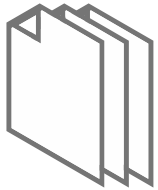
1. KNOW YOUR IT ENVIRONMENT (SLR & SUR)
2. IDENTIFY & MITIGATE THE RISKS
3. EXECUTE THE PLAN & COMMUNICATE !

Security Lifecycle Review (SLR)

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





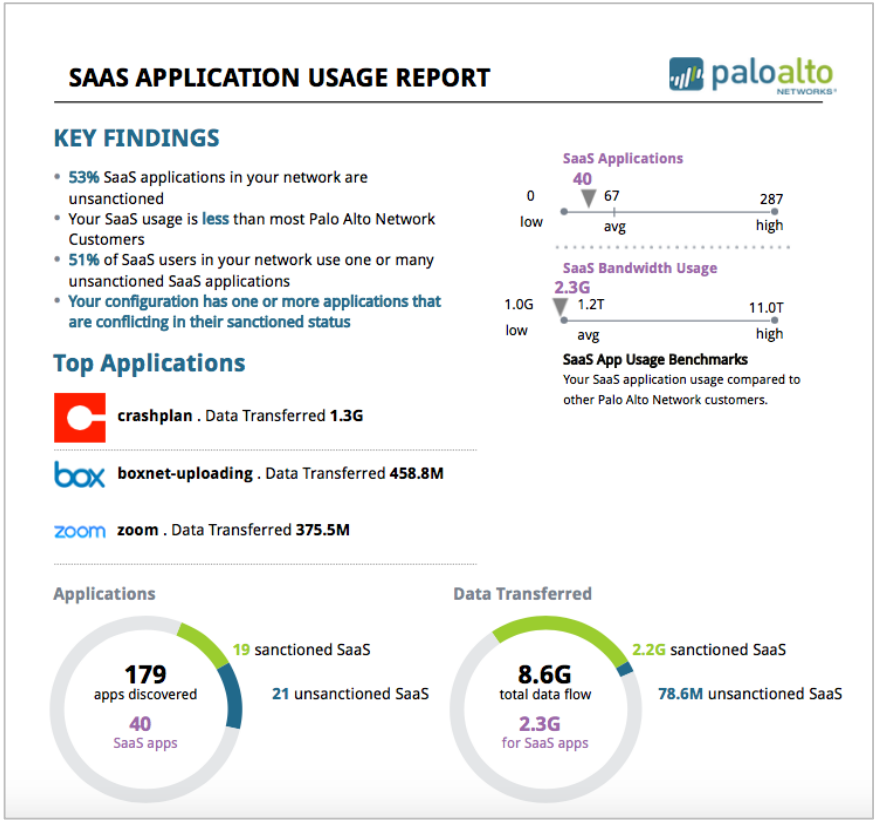


WE PUT THE DEVICE ON THE NETWORK

WE PASSIVELY MONITOR TRAFFIC FOR 1 WEEK

WE DELIVER THE REPORT & EXPLAIN THE FINDINGS

SaaS Usage Report (SUR)



SAAS APPLICATION USAGE REPORT

paloalto NETWORKS

KEY FINDINGS

- 53% SaaS applications in your network are unsanctioned
- Your SaaS usage is less than most Palo Alto Network Customers
- 51% of SaaS users in your network use one or many unsanctioned SaaS applications
- Your configuration has one or more applications that are conflicting in their sanctioned status

SaaS Applications

40

0 low | 67 avg | 287 high

SaaS Bandwidth Usage

2.3G

1.0G low | 1.2T avg | 11.0T high

SaaS App Usage Benchmarks

Your SaaS application usage compared to other Palo Alto Network customers.

Top Applications

crashplan . Data Transferred 1.3G

boxnet-uploading . Data Transferred 458.8M

zoom . Data Transferred 375.5M

Applications

179 apps discovered

40 SaaS apps

19 sanctioned SaaS

21 unsanctioned SaaS

Data Transferred

8.6G total data flow

2.3G for SaaS apps

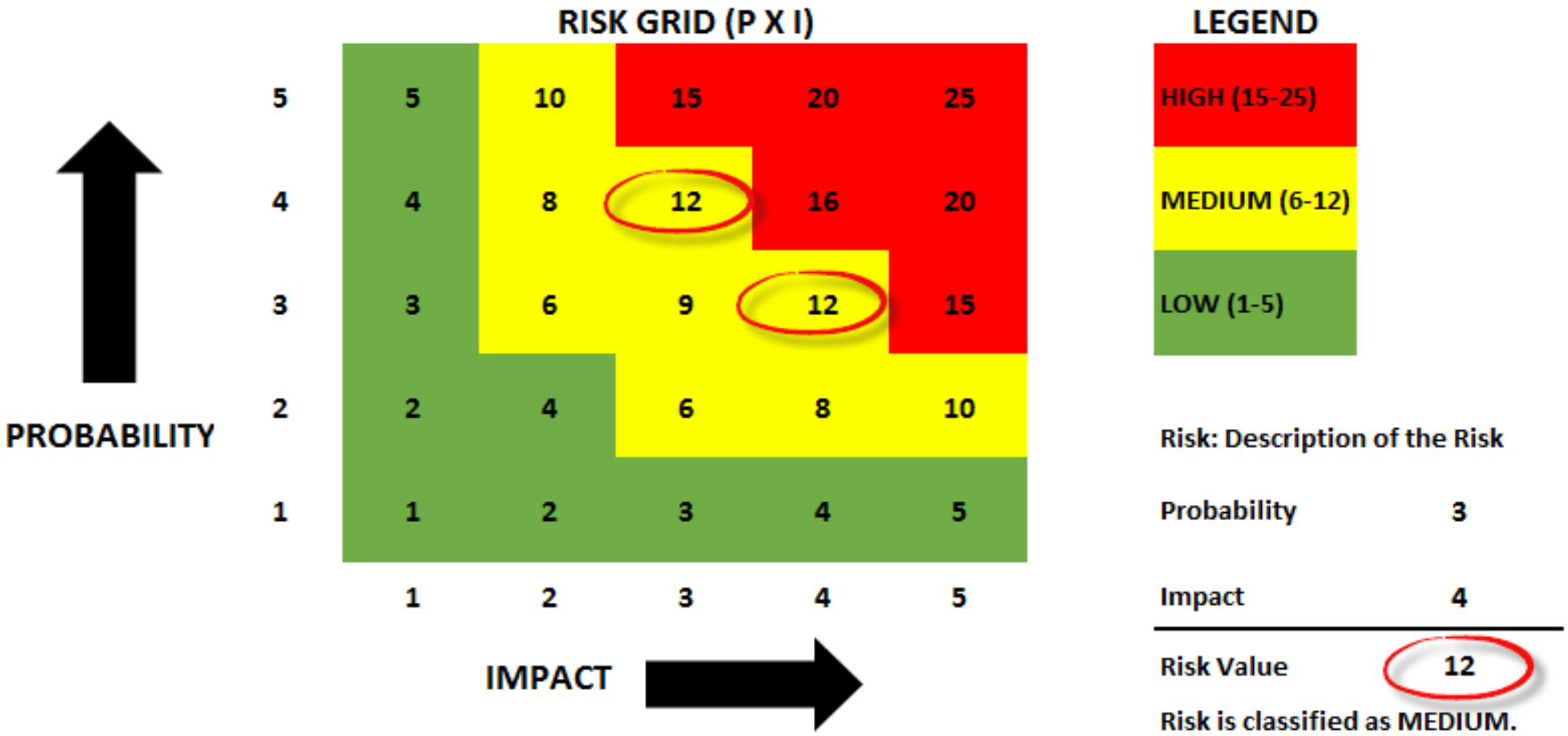
2.2G sanctioned SaaS

78.6M unsanctioned SaaS

- View apps by risk or sanctioned state (Sanctioned, Tolerated, Unsanctioned)
- Create targeted reports based on user groups and zones
- Summarize SaaS application usage by group

paloalto NETWORKS


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	Cur...	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				...dure 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					...mination 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.

225 risks identified with residual risk scores between 20-1

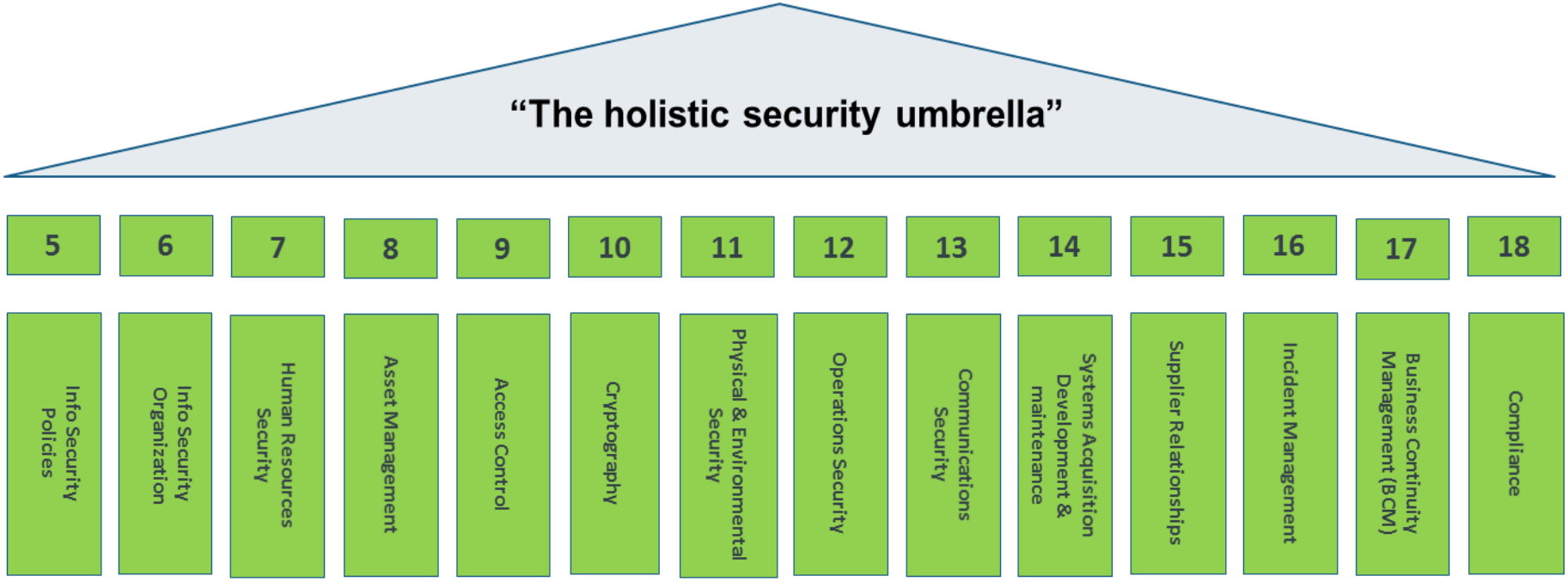

RISK APPETITE


FRAMEWORK

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

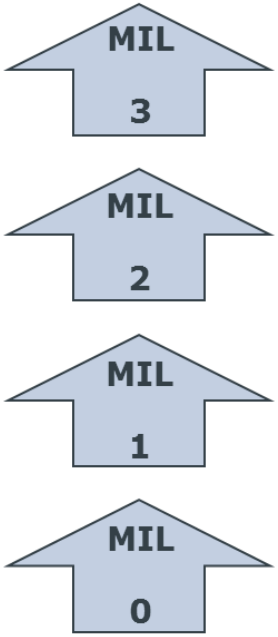
Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications 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

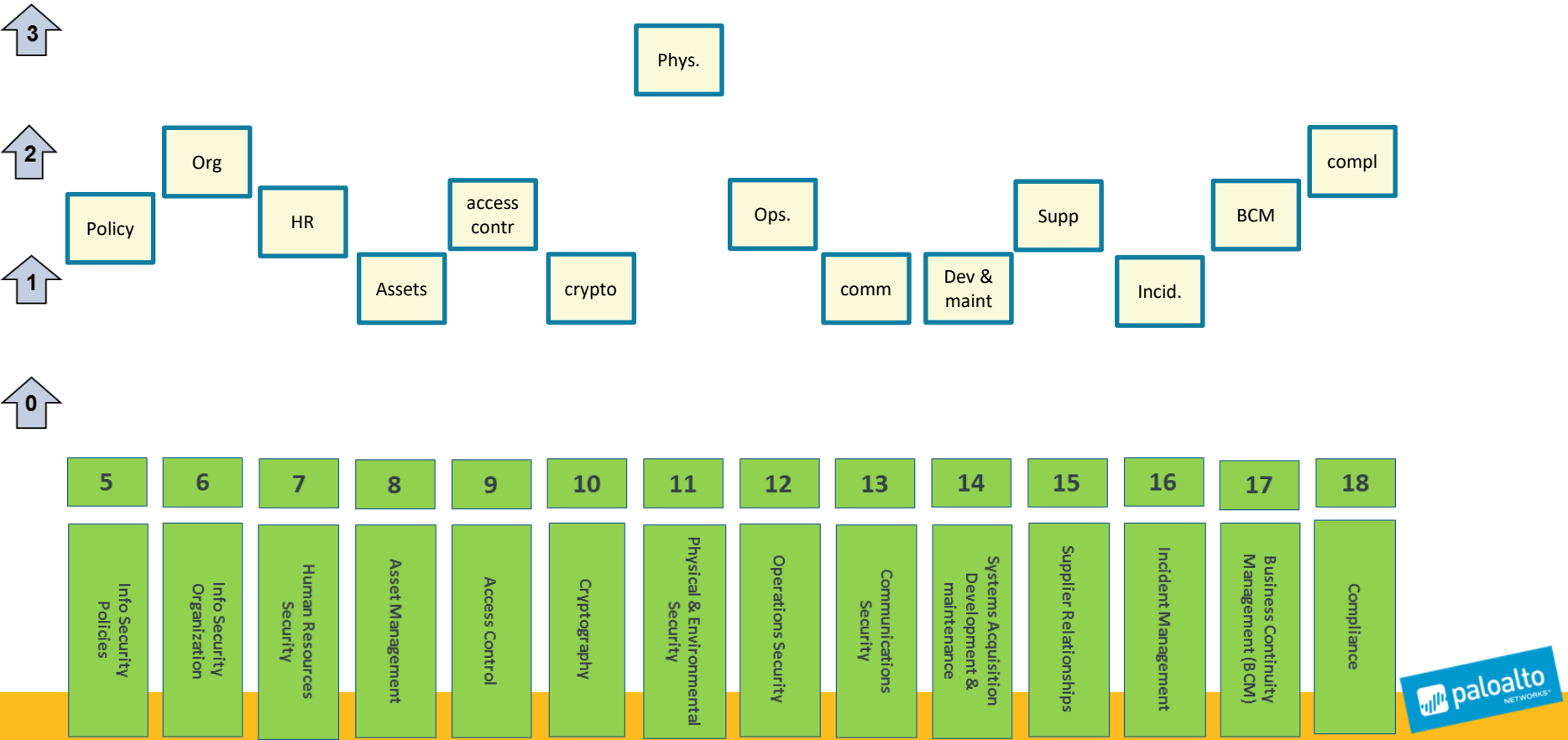
Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*

Maturity level 0, 1, 2 or 3 ?

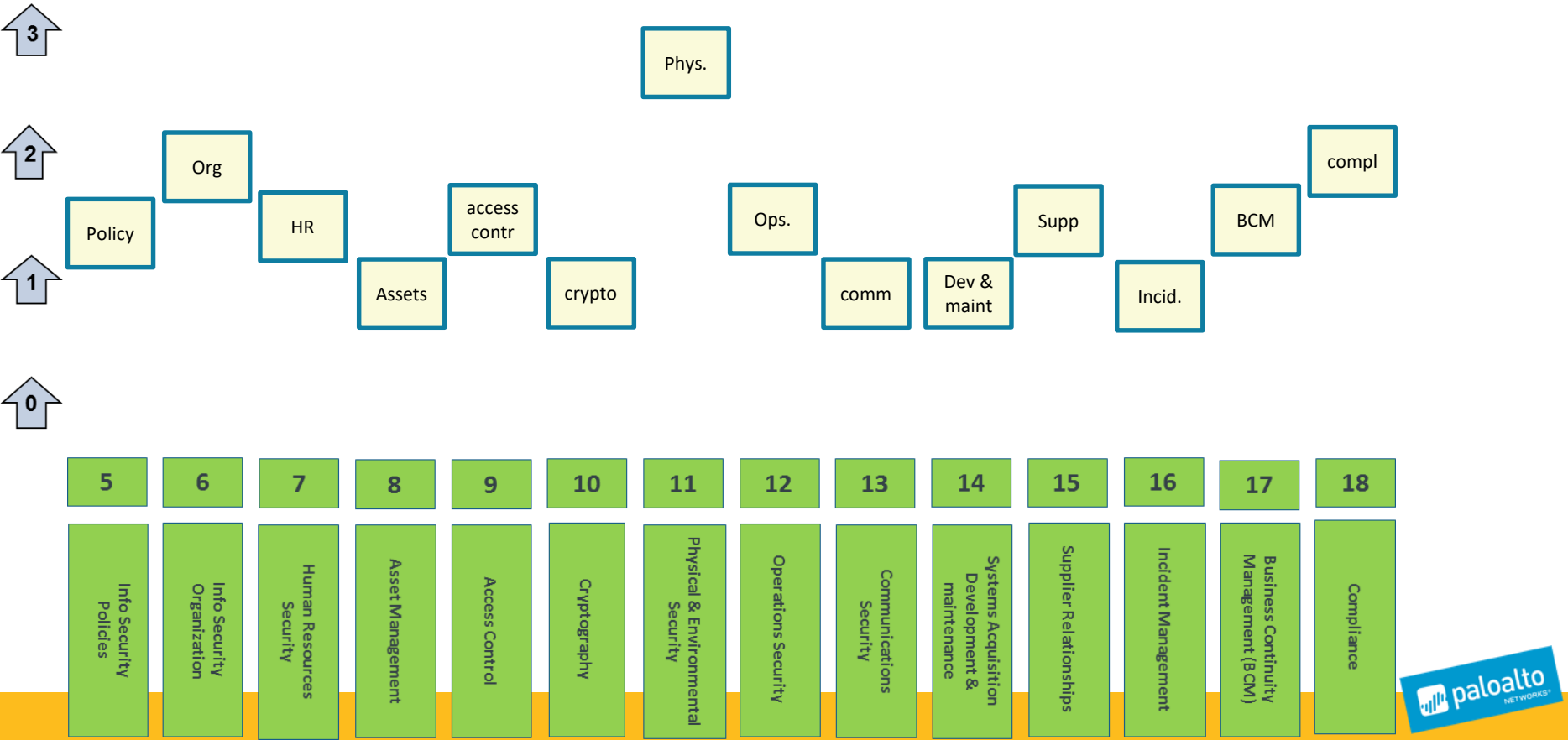
Maturity level 0, 1, 2 or 3 ?

Maturity level 0, 1, 2 or 3 ?

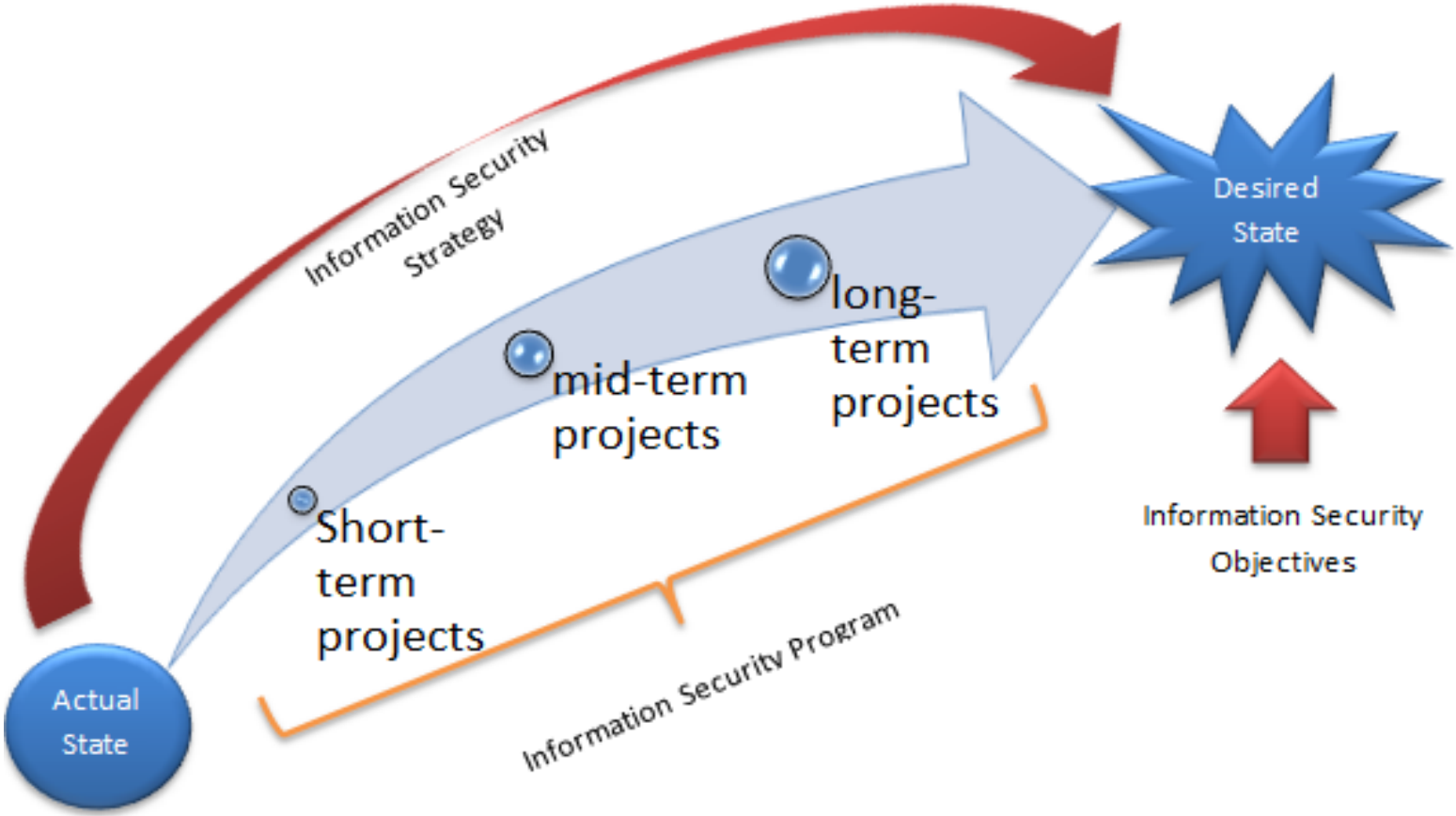
Start Situation



Desired End-state



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


HOW DO WE GET
THERE?

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

- **Get to know your IT environment**
- **Provide Security awareness training for all personnel**
- **Develop Information Security policies & Incident Response Plan**
- **Implement Network Security (NGFW)**
- **Implement two-factor authentication (Okta)**
- **Implement Endpoint Security (Traps)**
- **Implement Cloud Security (VM Series & Aperture)**
- **……..**

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

- **Get to know your IT environment**
- **Provide Security awareness training for all personnel**
- **Develop Information Security policies & Incident Response Plan**
- **Implement Network Security (NGFW)**
- **Implement two-factor authentication (Okta)**
- **Implement Endpoint Security (Traps)**
- **Implement Cloud Security (VM Series & Aperture)**

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

- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement Network Security (NGFW)
- Implement two-factor authentication (Okta)
- Implement Endpoint Security (Traps)
- Implement Cloud Security (VM Series & Aperture)

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

- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement Network Security (NGFW)
- Implement two-factor authentication (Okta)
- Implement Endpoint Security (Traps)
- Implement Cloud Security (VM Series & Aperture)

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

- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement Network Security (NGFW)
- Implement two-factor authentication (Okta)
- Implement Endpoint Security (Traps)
- Implement Cloud Security (VM Series & Aperture)

Implement Network Security (Next-Generation Firewalls)

+

+

FORTINET

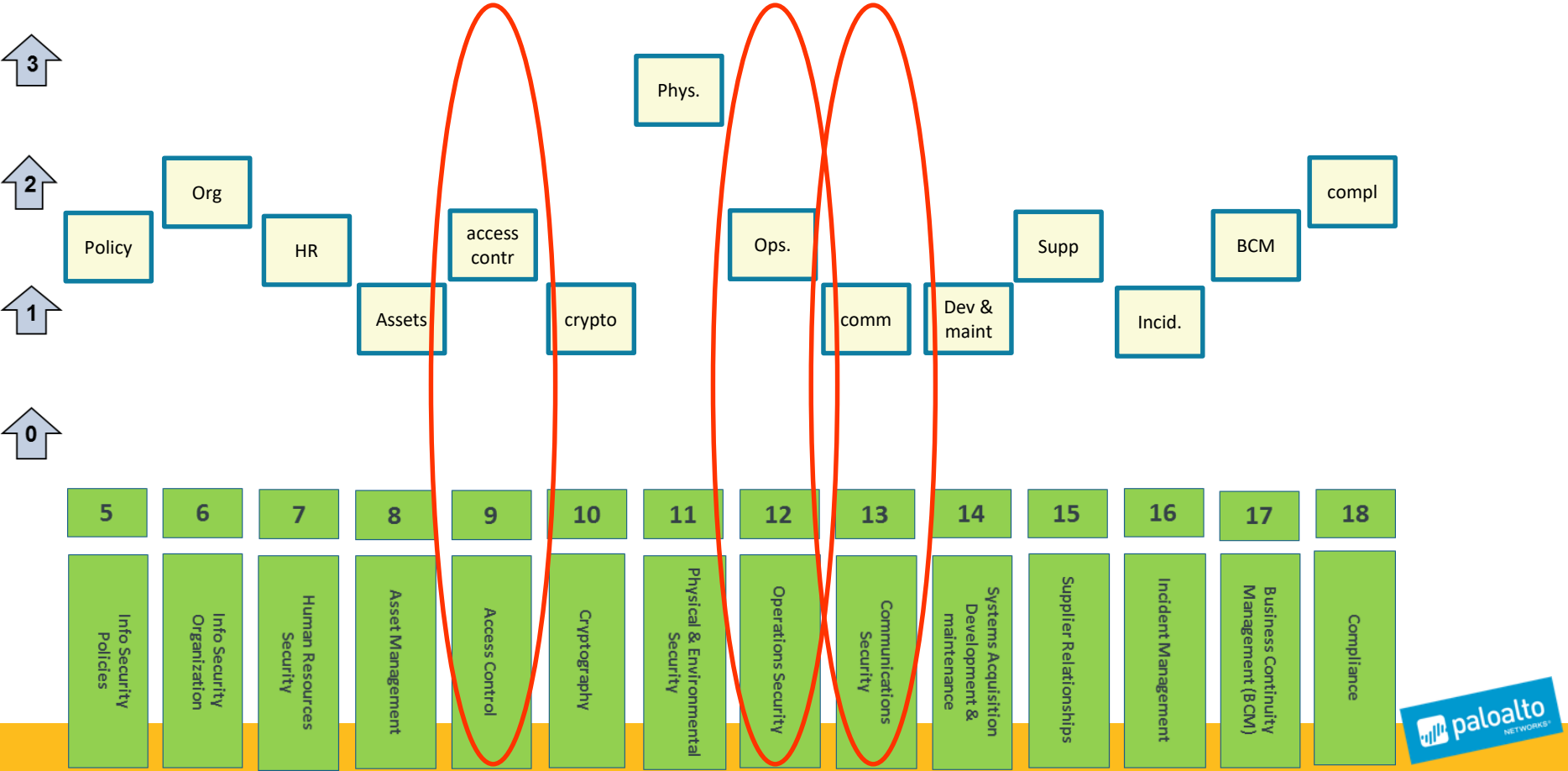
Check Point
SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

paloalto NETWORKS

paloalto NETWORKS

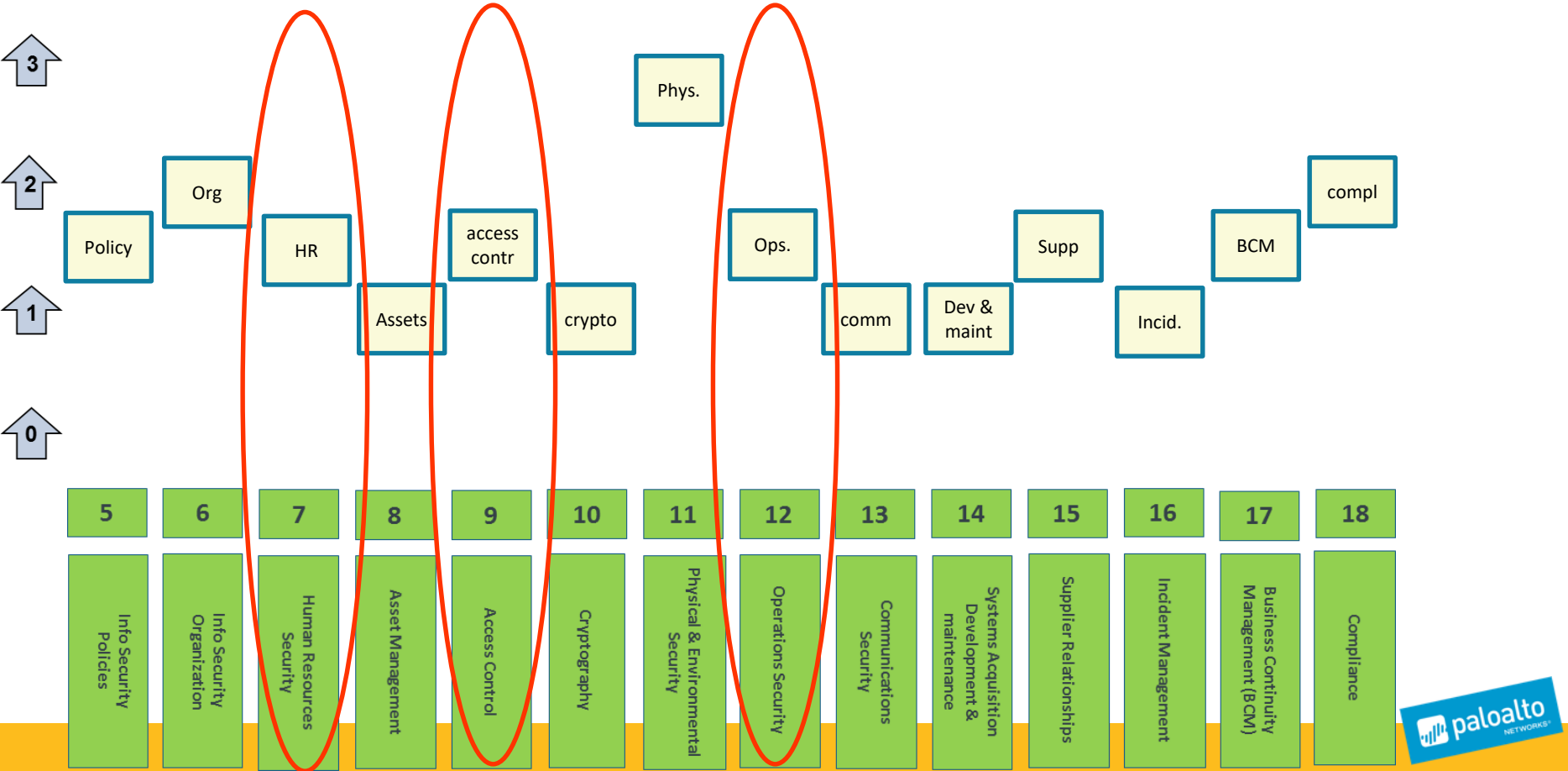
Implement Network Security (NGFW)



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

- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement Network Security (NGFW)
- Implement two-factor authentication (Okta)
- Implement Endpoint Security (Traps)
- Implement Cloud Security (VM Series & Aperture)

Implement two-factor authentication (Okta)

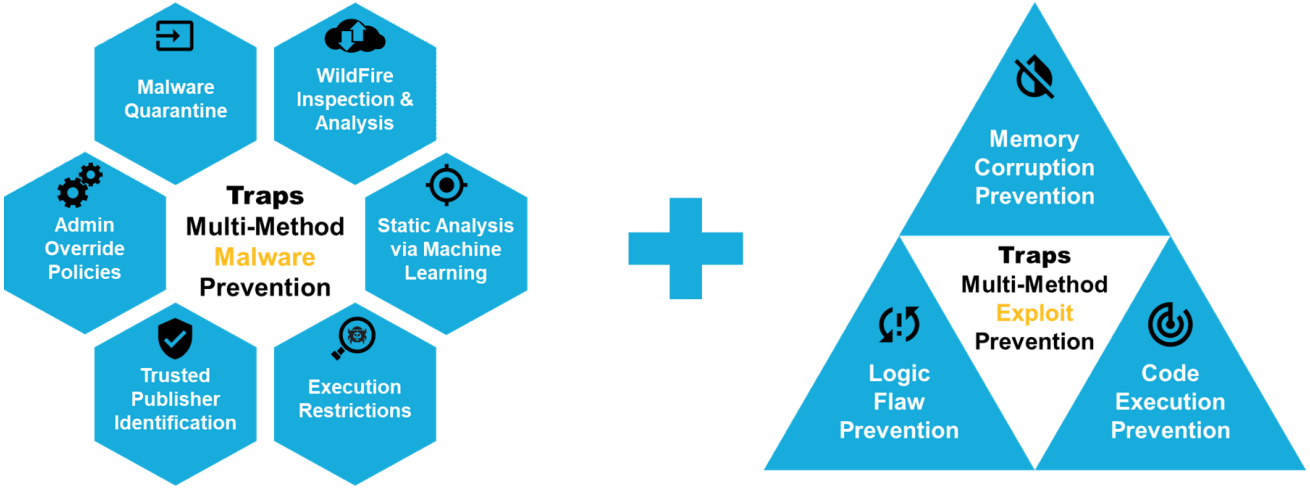


Mitigating the risks with security projects…step-by-step

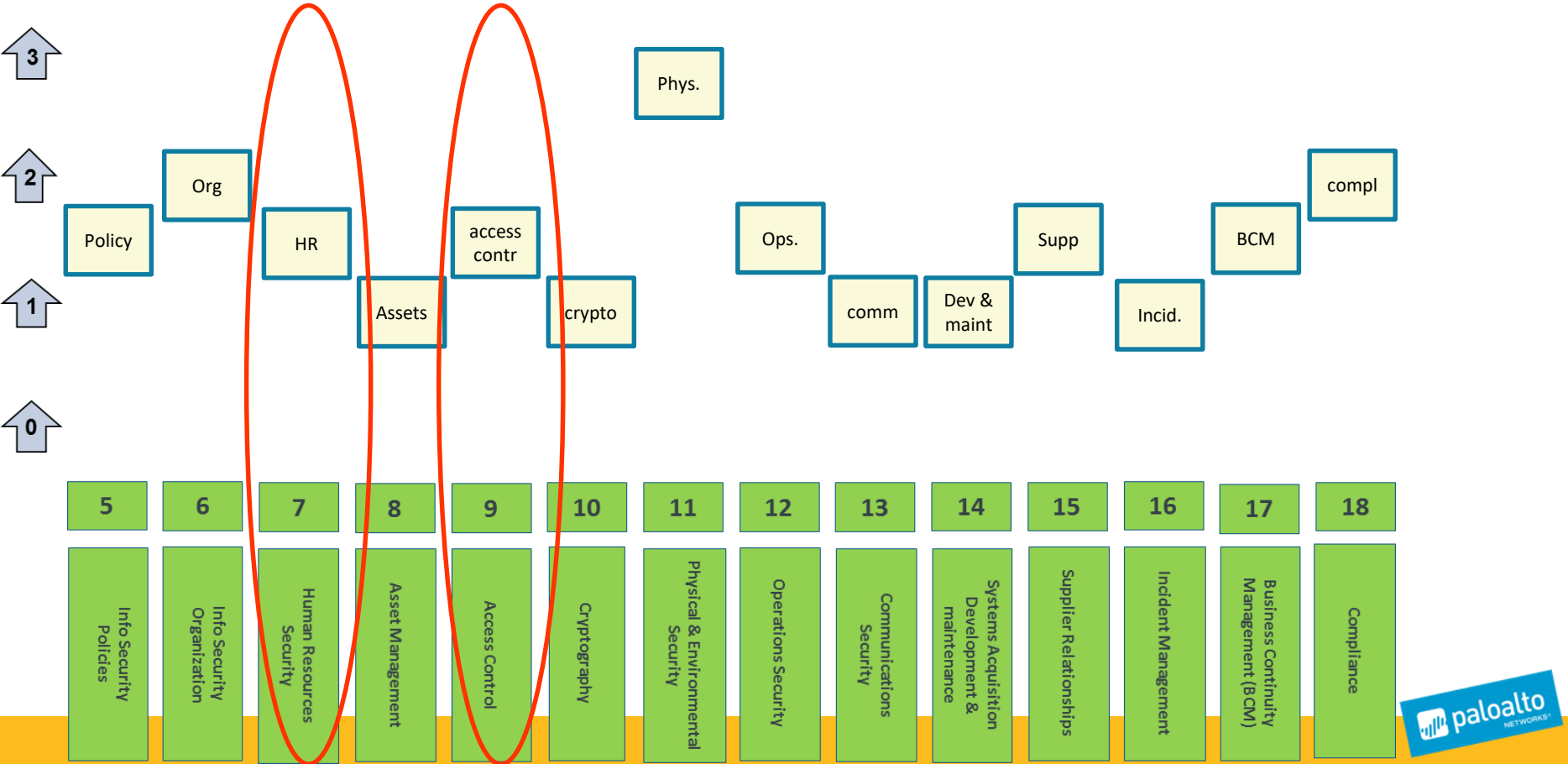
- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement Network Security (NGFW)
- Implement two-factor authentication (Okta)
- Implement Endpoint Security (Traps)
- Implement Cloud Security (VM Series & Aperture)

Implement Endpoint Security (Traps)

1. Security policy & take away local admin rights
2. Encrypt mobile devices
3. Test & Install Traps



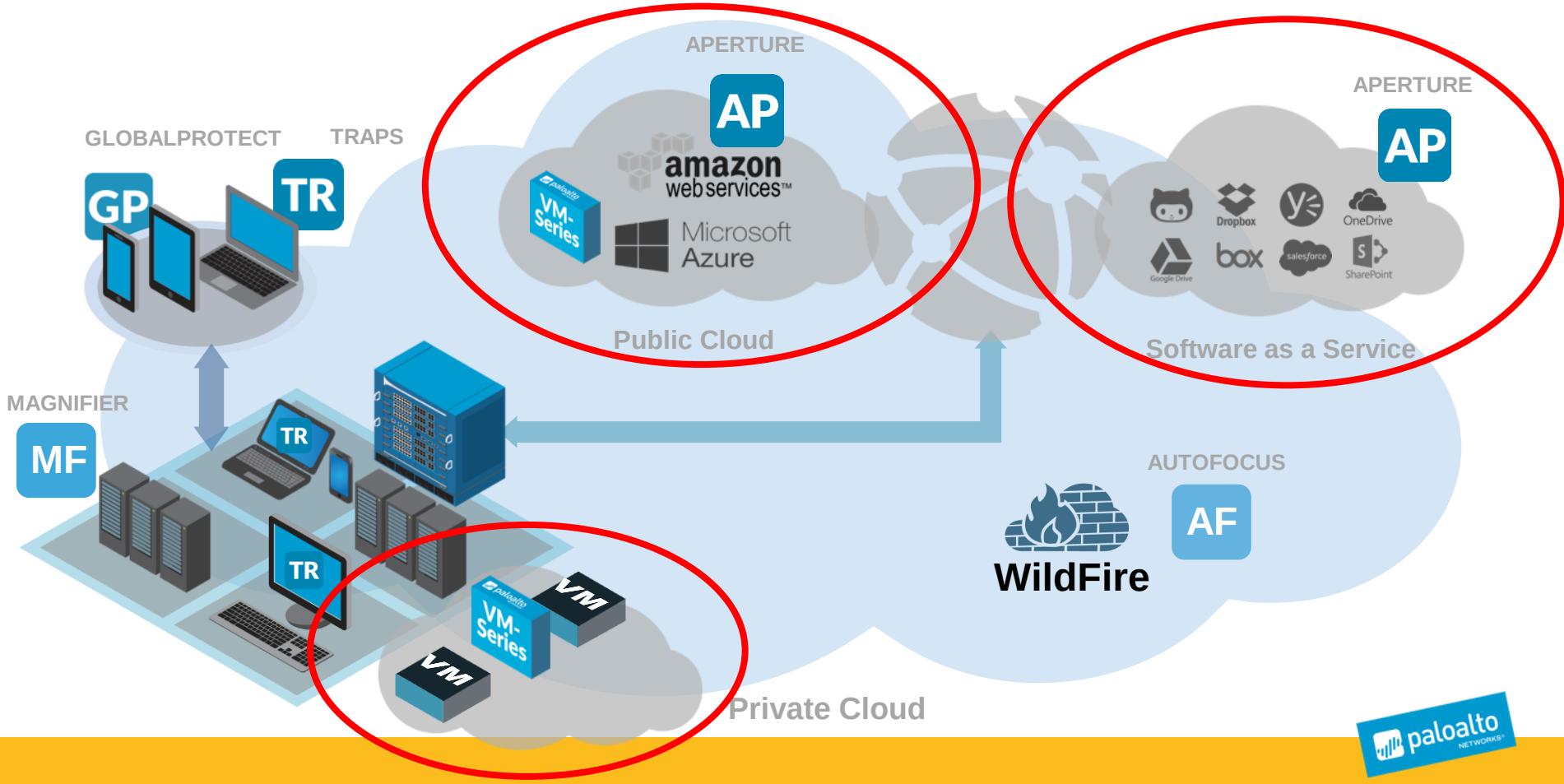
Implement Endpoint Security (Traps)



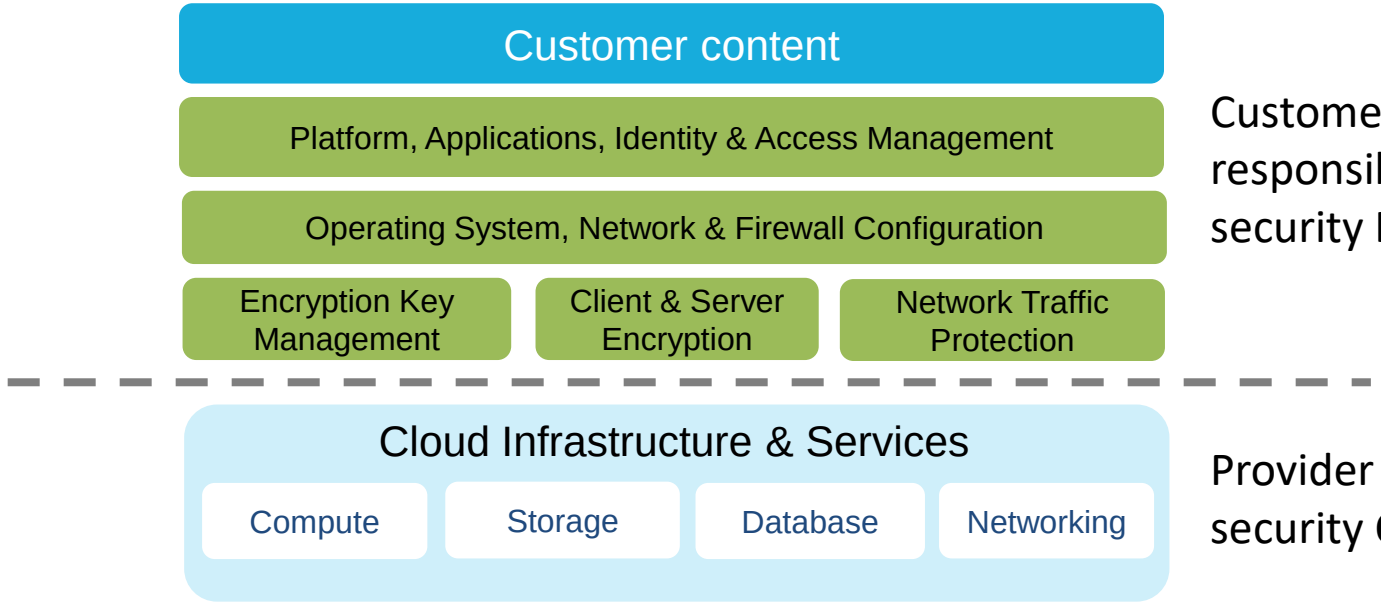
Mitigating the risks with security projects…step-by-step

- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement Network Security (NGFW)
- Implement two-factor authentication (Okta)
- Implement Endpoint Security (Traps)
- Implement Cloud Security (VM Series & Aperture)

The Next-Generation Security Platform



Security in the cloud: a shared responsibility



Customers are responsible for their security **IN** the cloud

Provider looks after security **OF** the cloud

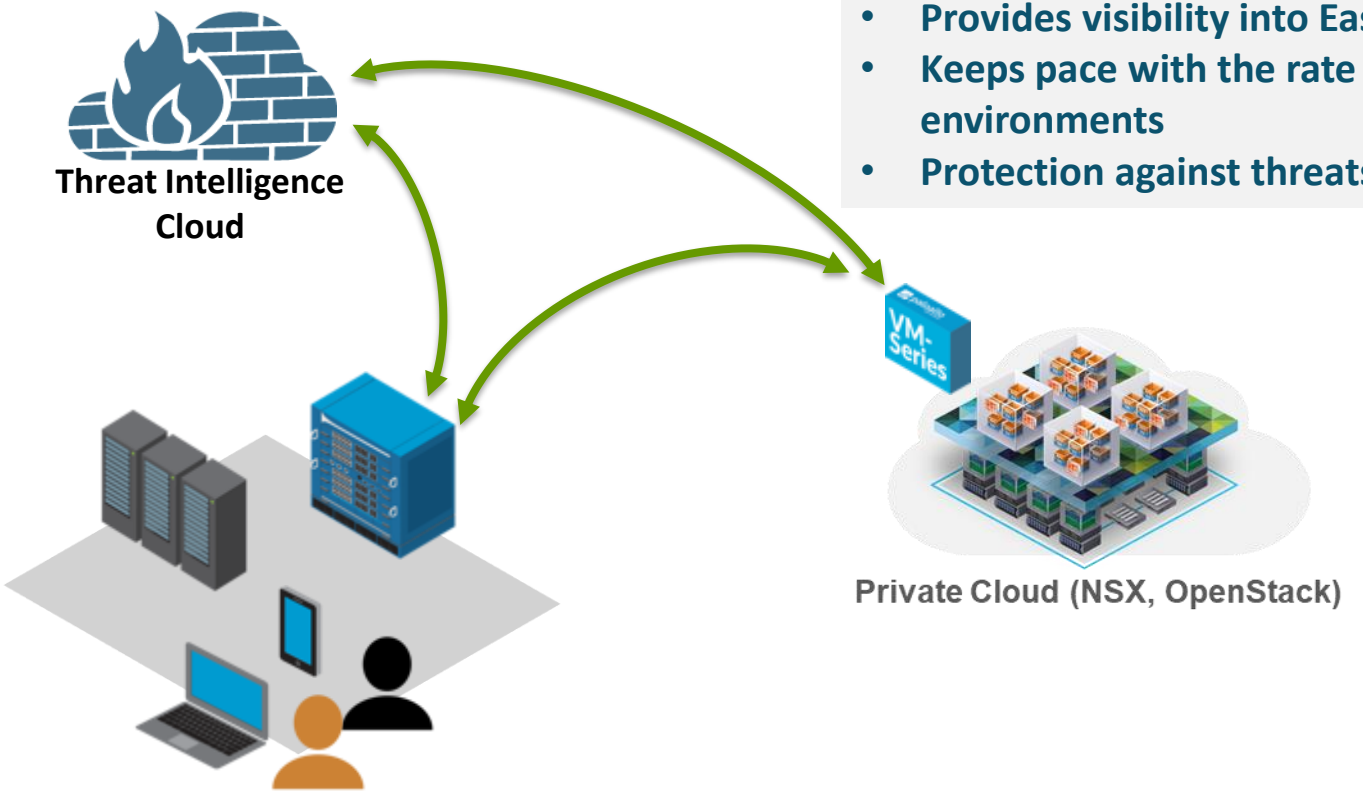
Data in the Cloud(s)

Software as a Service (SaaS)

Public Cloud (NSX, OpenStack)

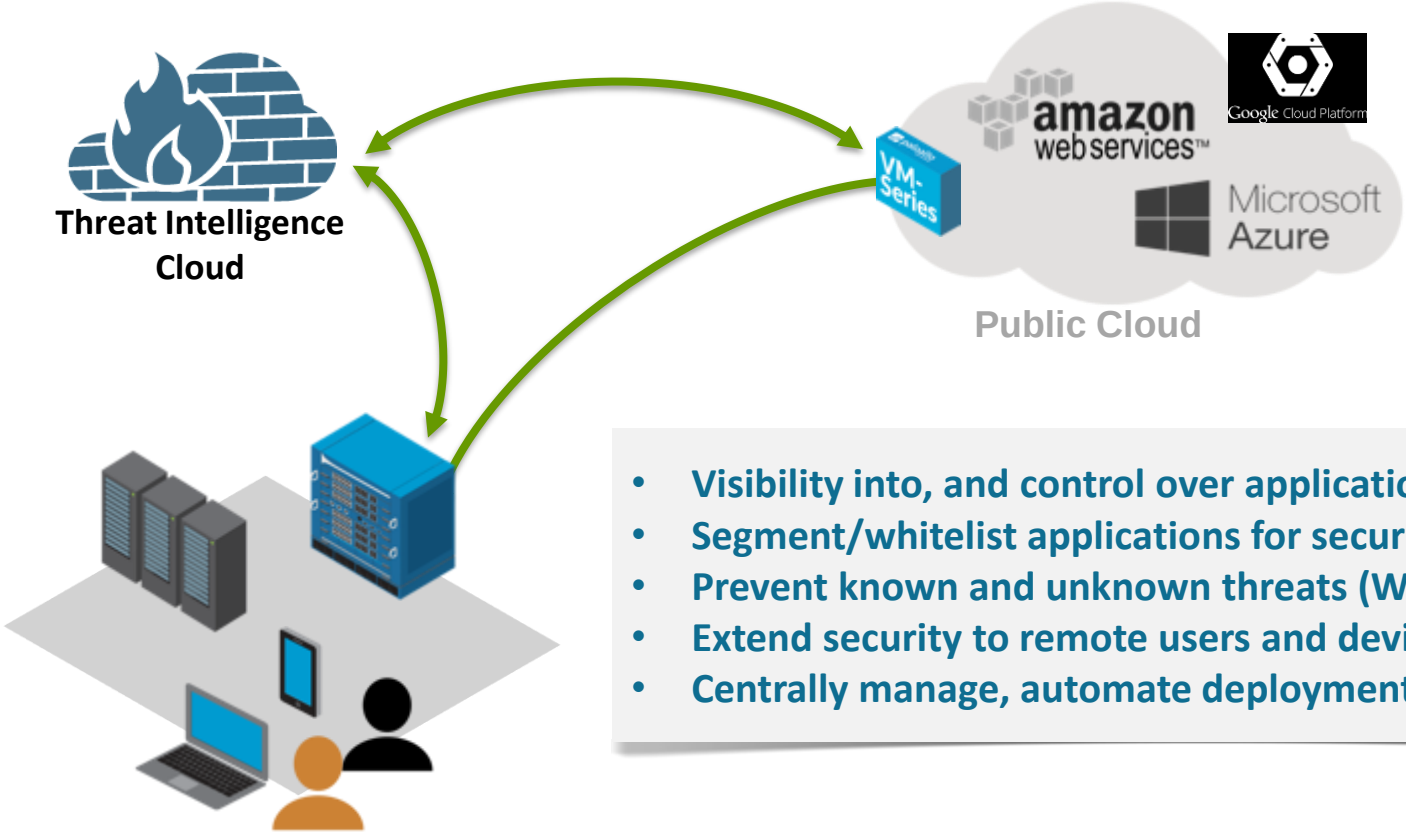
Private Cloud (NSX, OpenStack)

VM-Series for Private Cloud



- Provides visibility into East-West traffic in DC
- Keeps pace with the rate of change in virtual environments
- Protection against threats to the data center

VM-Series for Public Cloud



- Visibility into, and control over applications, not ports
- Segment/whitelist applications for security and compliance
- Prevent known and unknown threats (WildFire)
- Extend security to remote users and devices
- Centrally manage, automate deployment and policy updates

Aperture for SaaS visibility & security

EXCHANGE ONLINE

SHAREPOINT ONLINE

ONEDRIVE FOR BUSINESS

YAMMER

BOX.COM

GOOGLE DRIVE

Gmail

G SUITE

EC2 / IAM

CONFLUENCE

AMAZON S3

GITHUB

SLACK

CITRIX SHAREFILE

JIVE

SERVICENOW

SECURE DATA SPACE

SFDC

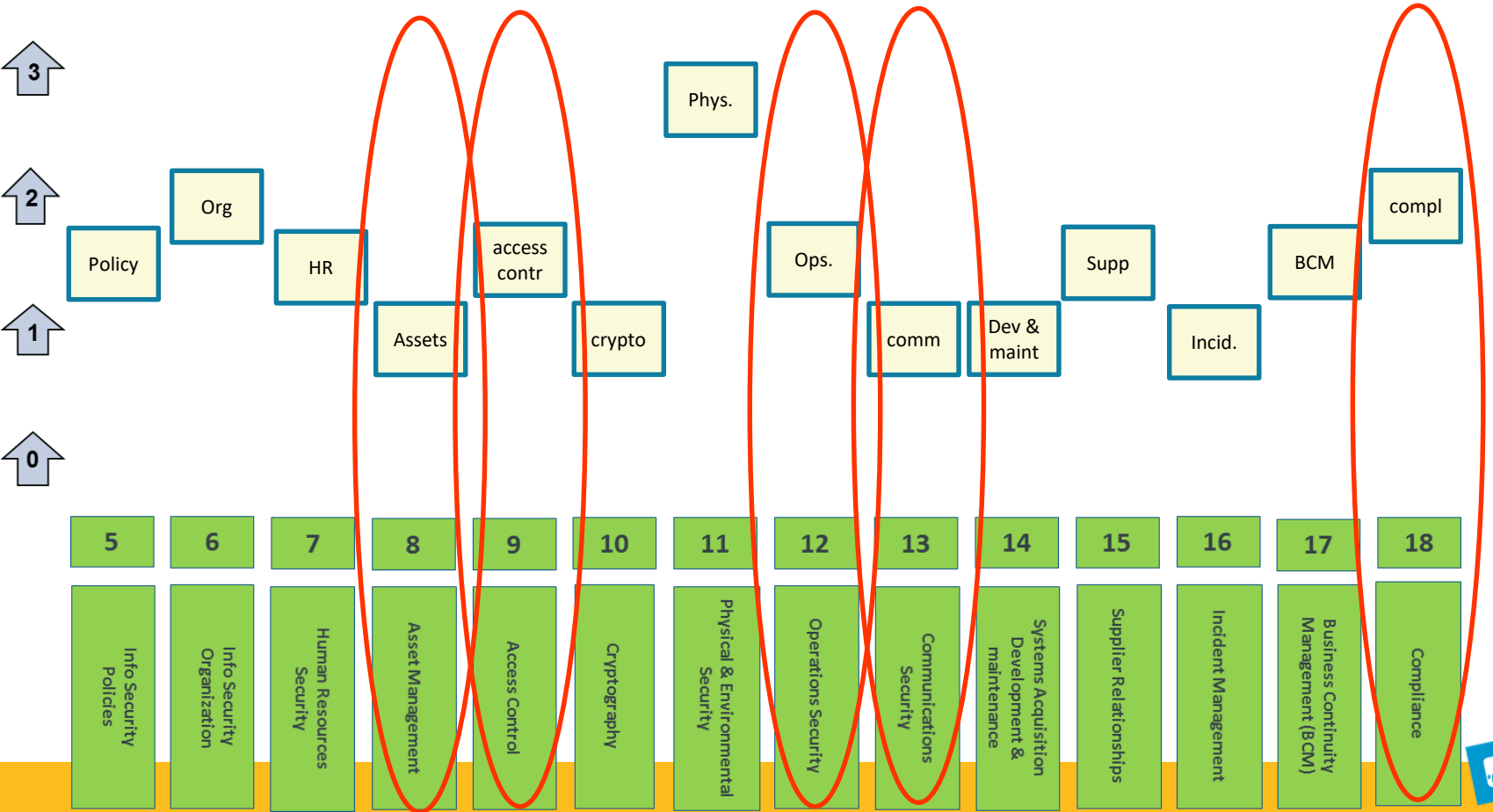
DROPBOX

AMERICAS

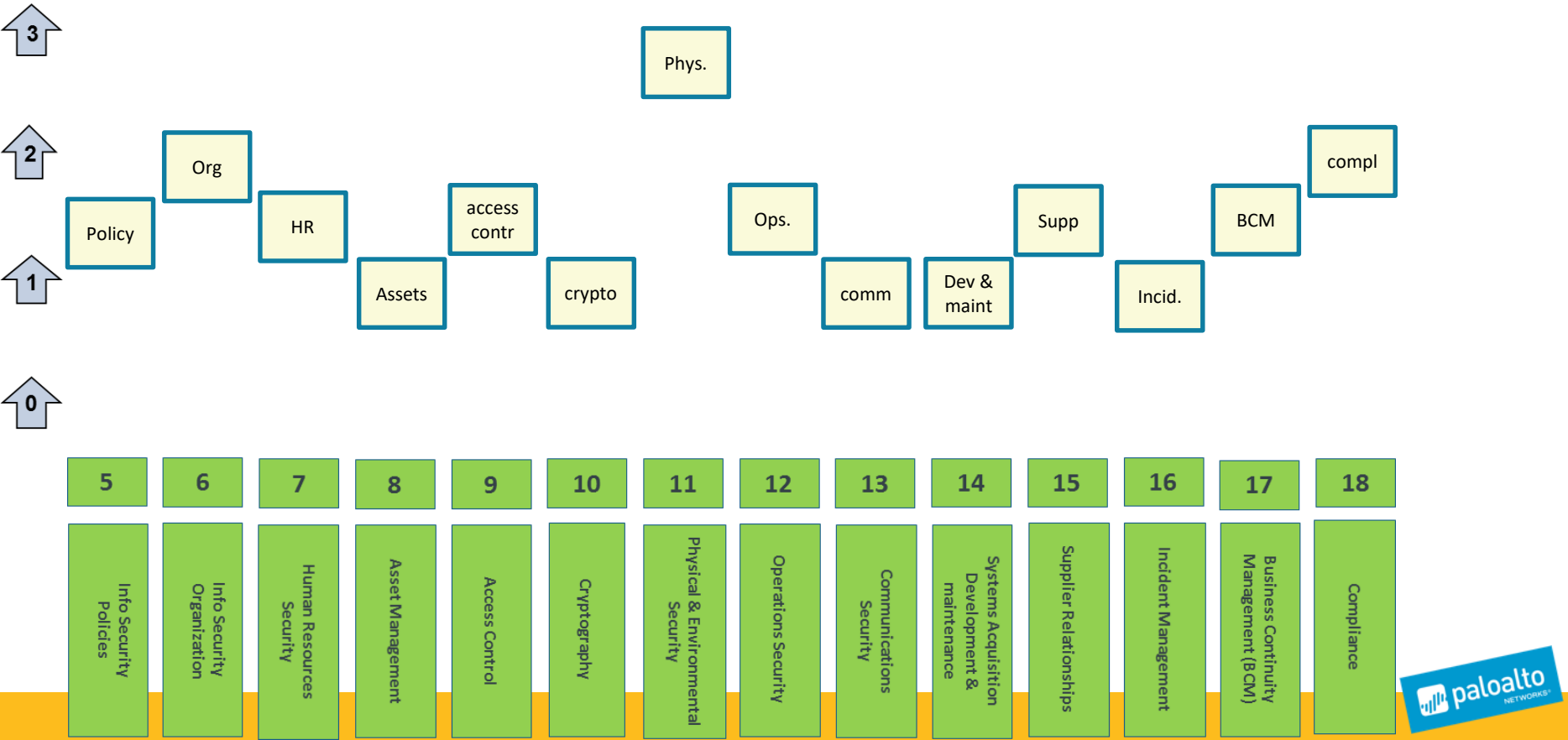
EMEA

APAC

Implement Cloud Security (VM Series & Aperture)



….so you can reach your goal !




CISO


HOLISTIC, INTEGRATED & AUTOMATED PLATFORM
USE A ‘STEP-BY-STEP’ PLAN
START WITH THE BUSINESS RISKS (ZERO TRUST)
CONCLUSION

Join us for the most game-changing cloud security event of ALL TIME!

WHO: Developers, architects, and members of cloud, network, and security teams

WHAT: A reboot of the future of cloud security, featuring:

Salim Ismail
best-selling author, futurist and technology entrepreneur

Lee Klarich
chief product officer, Palo Alto Networks

WHEN: 6 February 2018 | 5 – 6 p.m. GMT

WHERE: Watch the livestream online or join us at one of our exclusive viewing parties in:

- **Brussels**
- **Dubai**
- **Apeldoorn**
- **Istanbul**
- **Paris**

Register now

go.paloaltonetworks.com/epic-18

Ignite Europe (Amsterdam) : 8-10 October, 2018

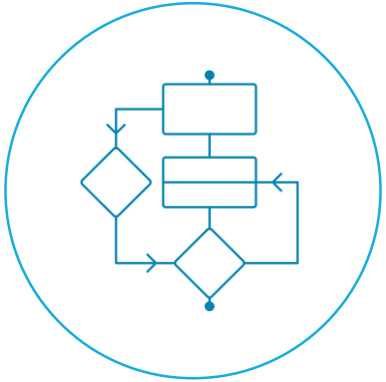
- Security Conference with more than 1500 top global security experts, peers & customers
- 65 breakout sessions representing a wide range of expertise and topic areas
- 1,000+ hands-on lab seats available (over the course of the conference)

Thank you for your attention !

Fstreefland@paloaltonetworks.com


WHAT ABOUT THE FUTURE ?

Changing threat landscape requires rapid deployment of new technologies

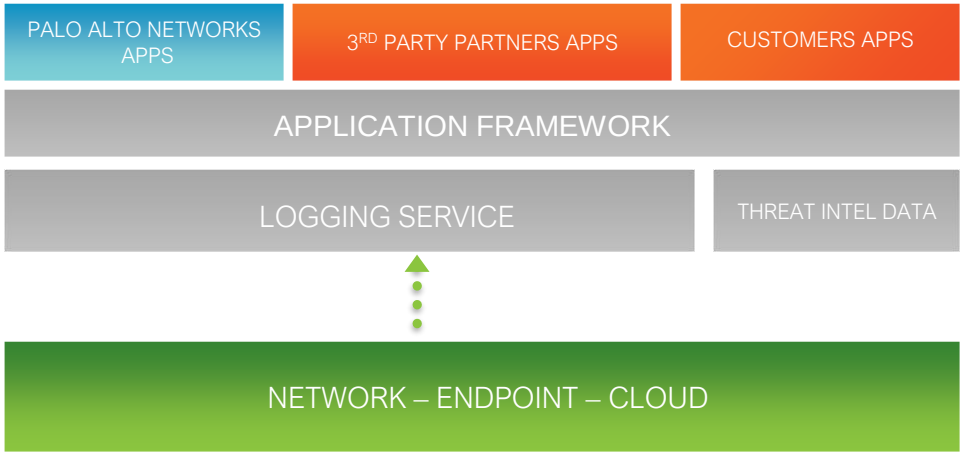


Complex and manual workflows across dozens of security products

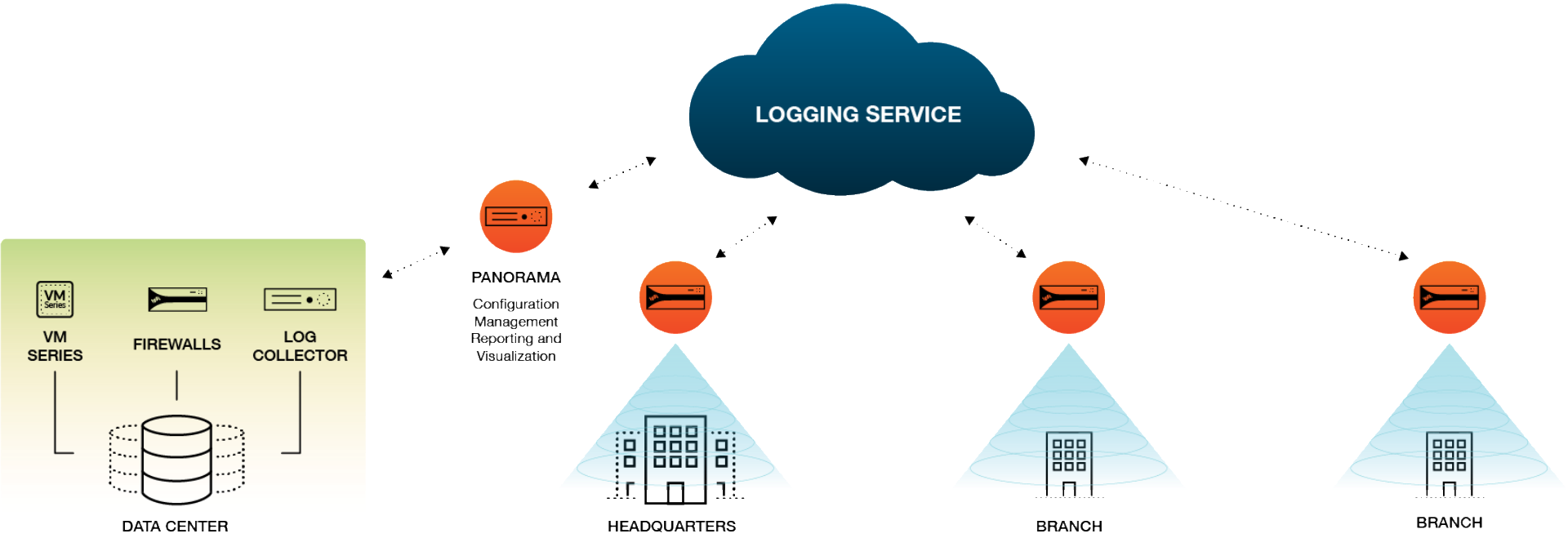
New security product deployments have up-front ROI risk and cost

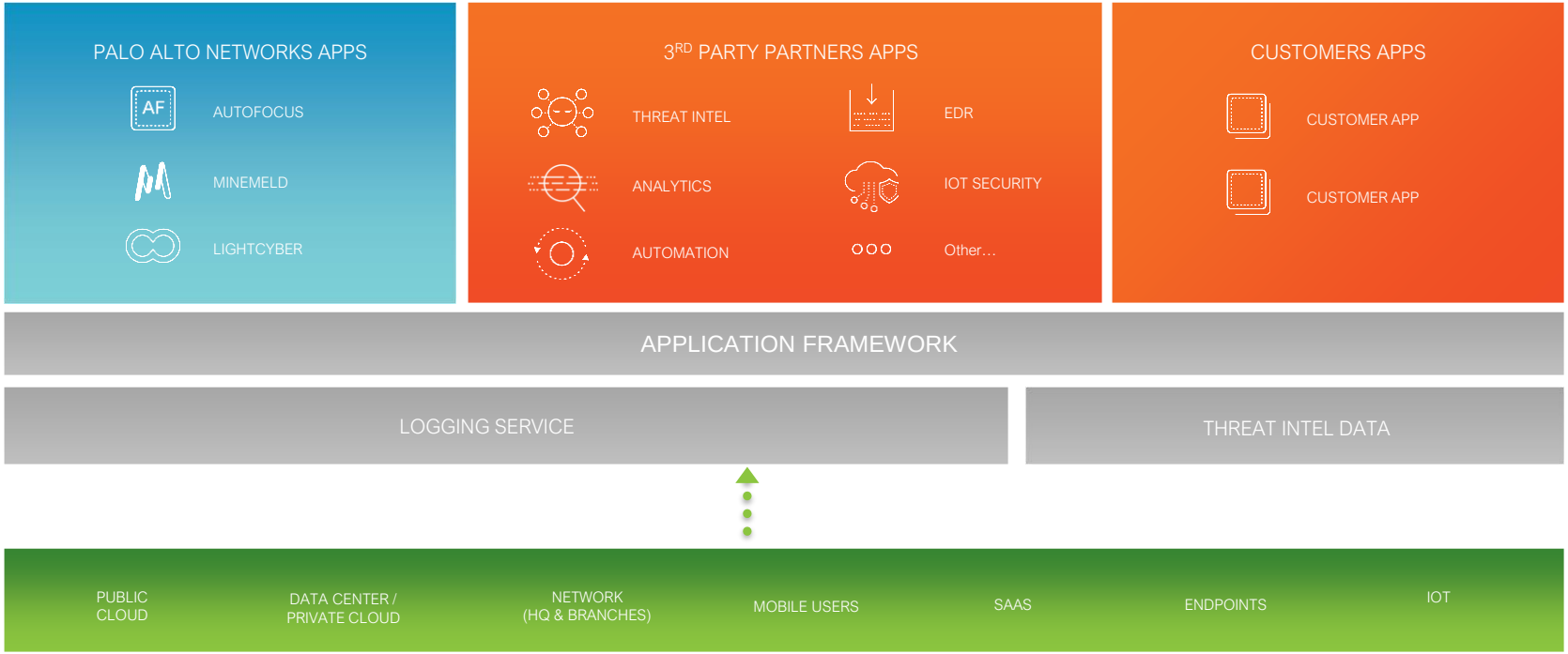
The Application Framework

- Extend the Next-Generation security platform with innovative security capabilities with no additional infrastructure.
- Consume security through cloud-delivered apps from leading security providers.
- Apps are developed by Palo Alto Networks, 3rd parties, MSSPs, and customers.



The Logging Service



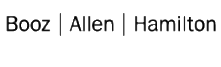


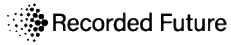
Application Framework
Rapidly build and deliver innovative, cloud-based security services.

Customer-specific data store
Provides apps with rich data on a massive scale.

Apps
Apps extend the capabilities of the platform.

Application Framework ecosystem





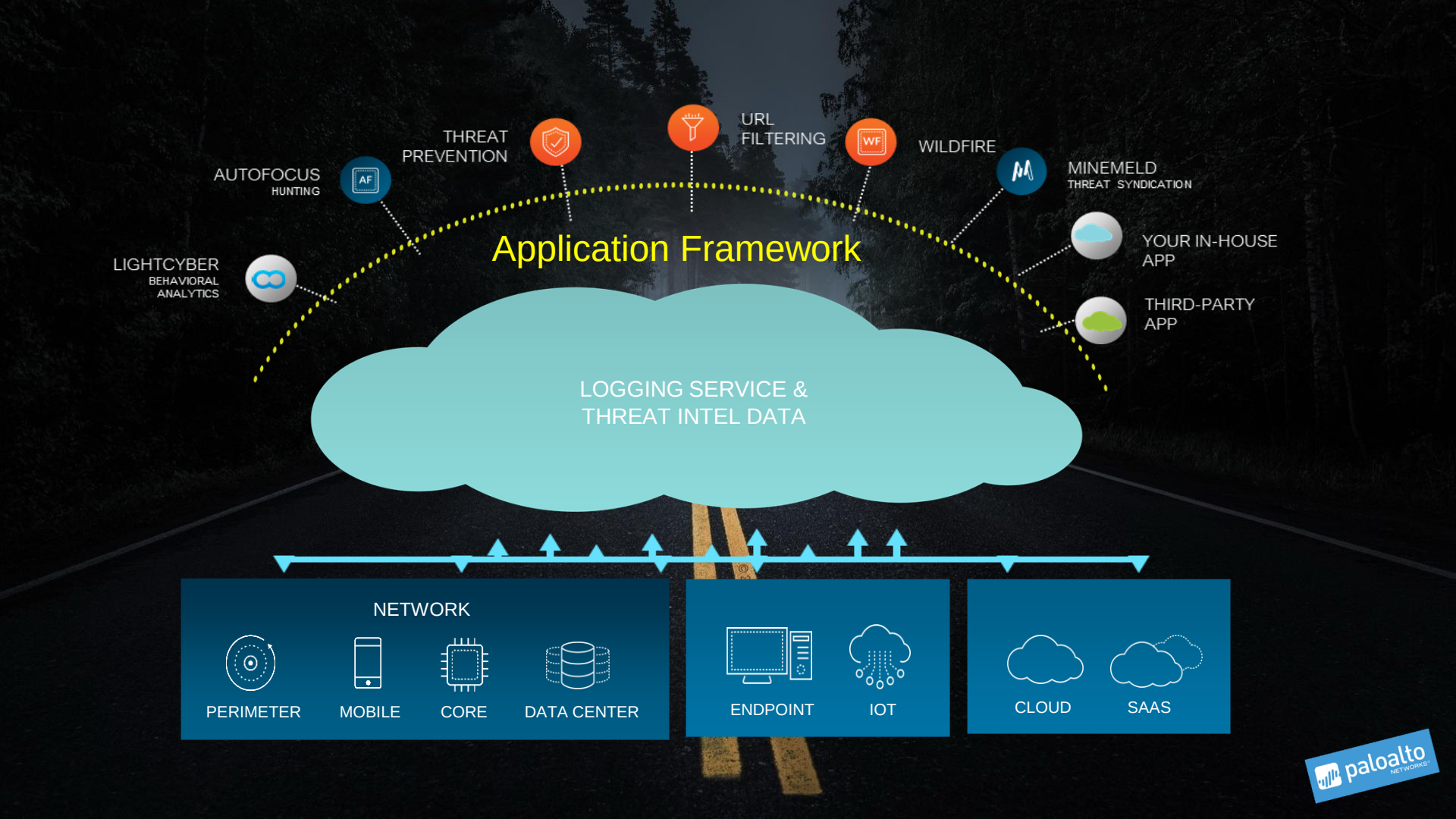
Application Framework use-case

Value for customers

Superior & agile security: Innovative new security capabilities from leading providers extend the Palo Alto Networks platform, with consistent enforcement across all users and locations.

App collaboration: Apps trigger a single workflow across different providers, including identification, analysis and response actions.

SaaS-based consumption model: Cloud-delivered apps can be consumed and updated quickly with no additional infrastructure & offer predictable OpEx.


AUTOFOCUS
HUNTING
AF
THREAT
PREVENTION
URL
FILTERING
WF
WILDFIRE
MINEMELD
THREAT SYNDICATION
LIGHTCYBER
BEHAVIORAL
ANALYTICS
Application Framework
YOUR IN-HOUSE
APP
THIRD-PARTY
APP
LOGGING SERVICE &
THREAT INTEL DATA
NETWORK
PERIMETER
MOBILE
CORE
DATA CENTER
ENDPOINT
IOT
CLOUD
SAAS
paloalto
NETWORKS