

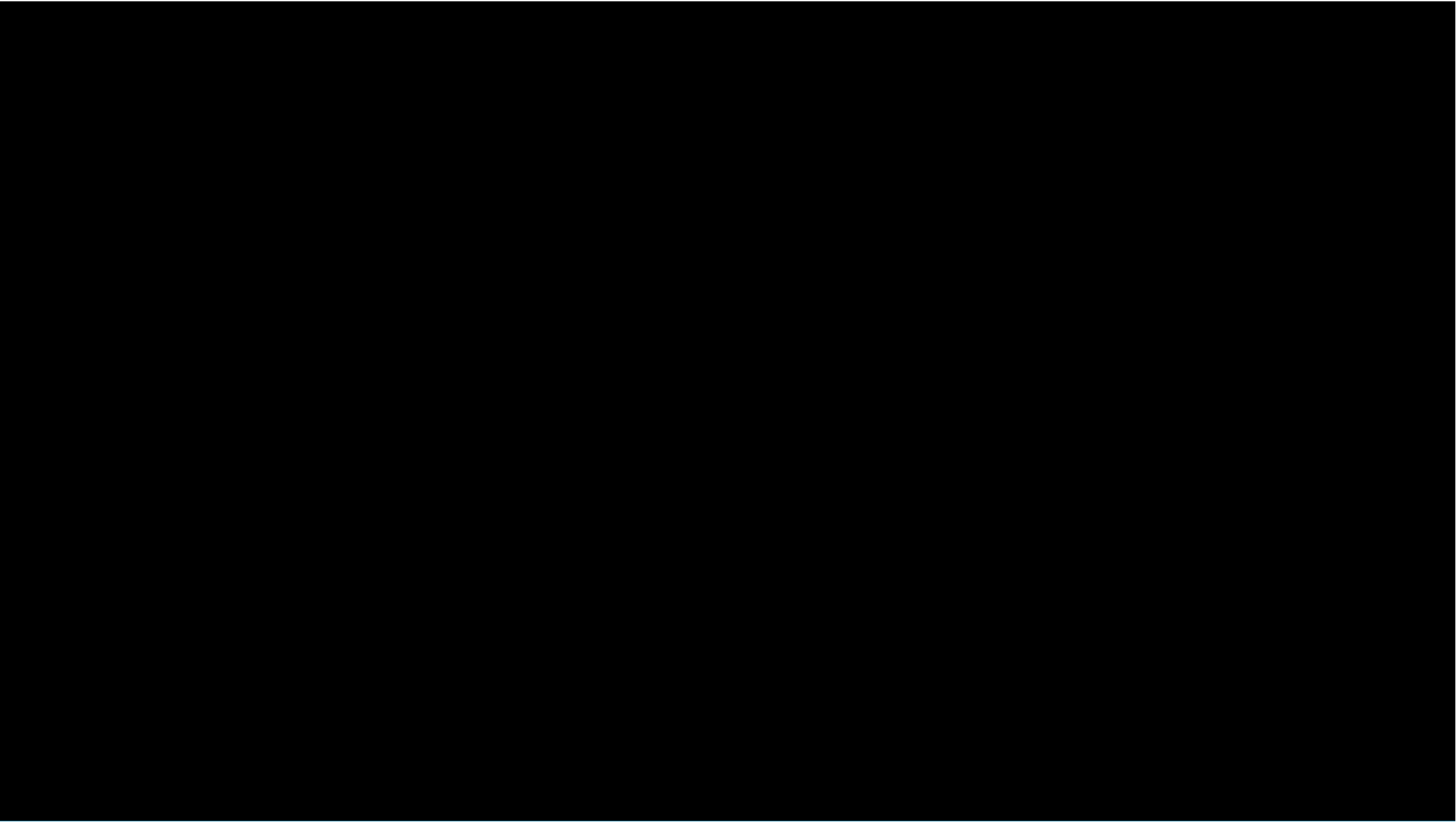
Segmentierung und Multifaktorauthentisierung

essentielle Bauteile sicherer IT-Infrastrukturen

Michael Weisgerber, CISSP
Senior Channel Systems Engineer CEUR

DON'T
PANIC







Bruteforce-Attacke ->

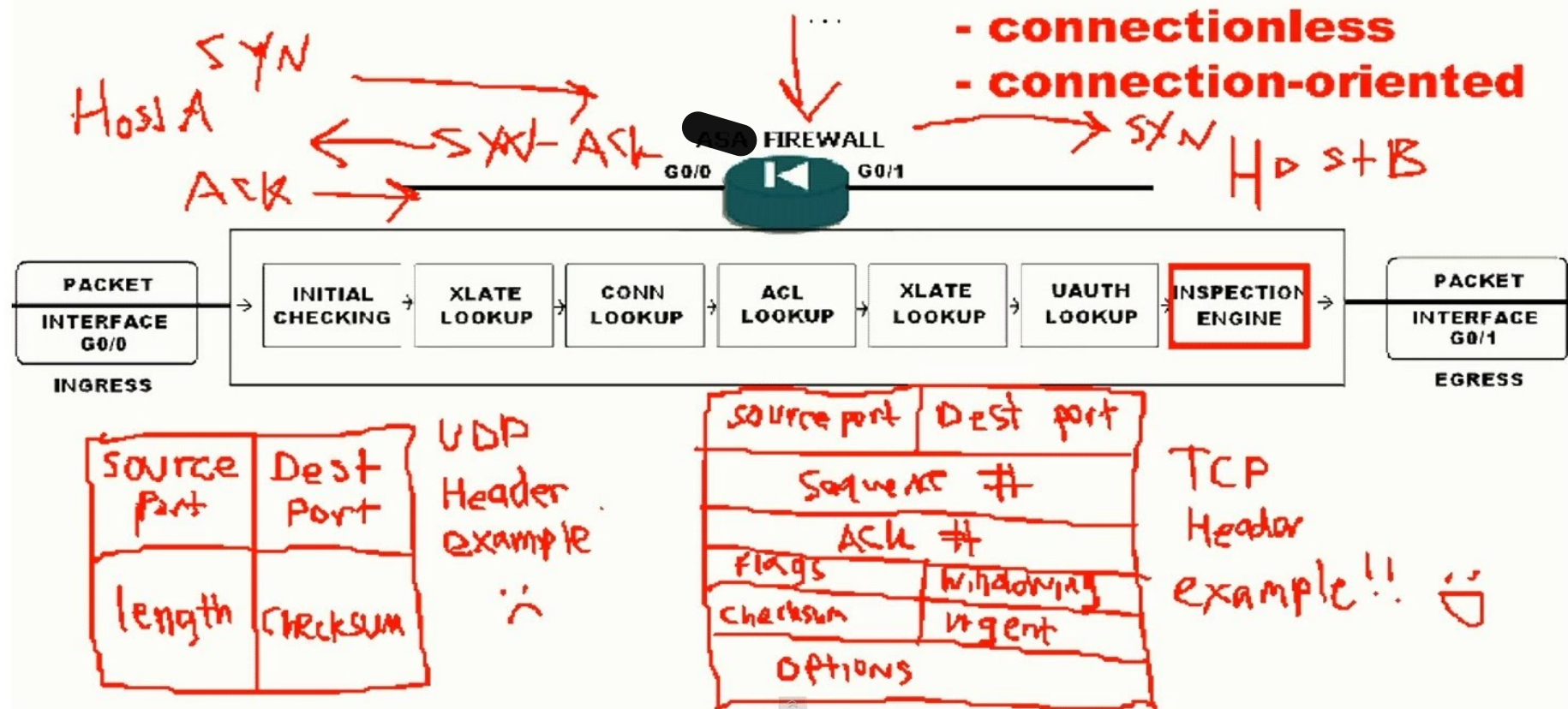
Cloud ->

Kronjuwelen ->

WELCOME

Cisco Training Videos: by Trevor Becker

Topic: Inspection Engine Phase 7 of ASA packet inspection process



“Wer braucht denn noch eine weitere Firewall?“ ;-) (2005/2007)

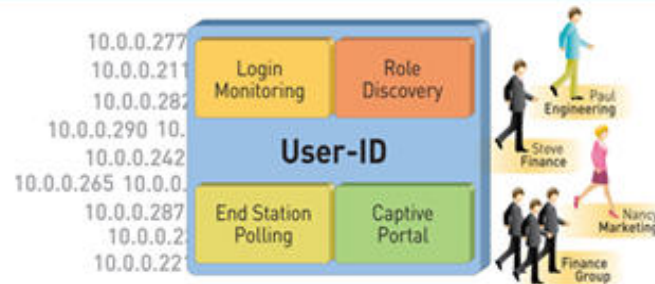
App-ID™

Identify the application



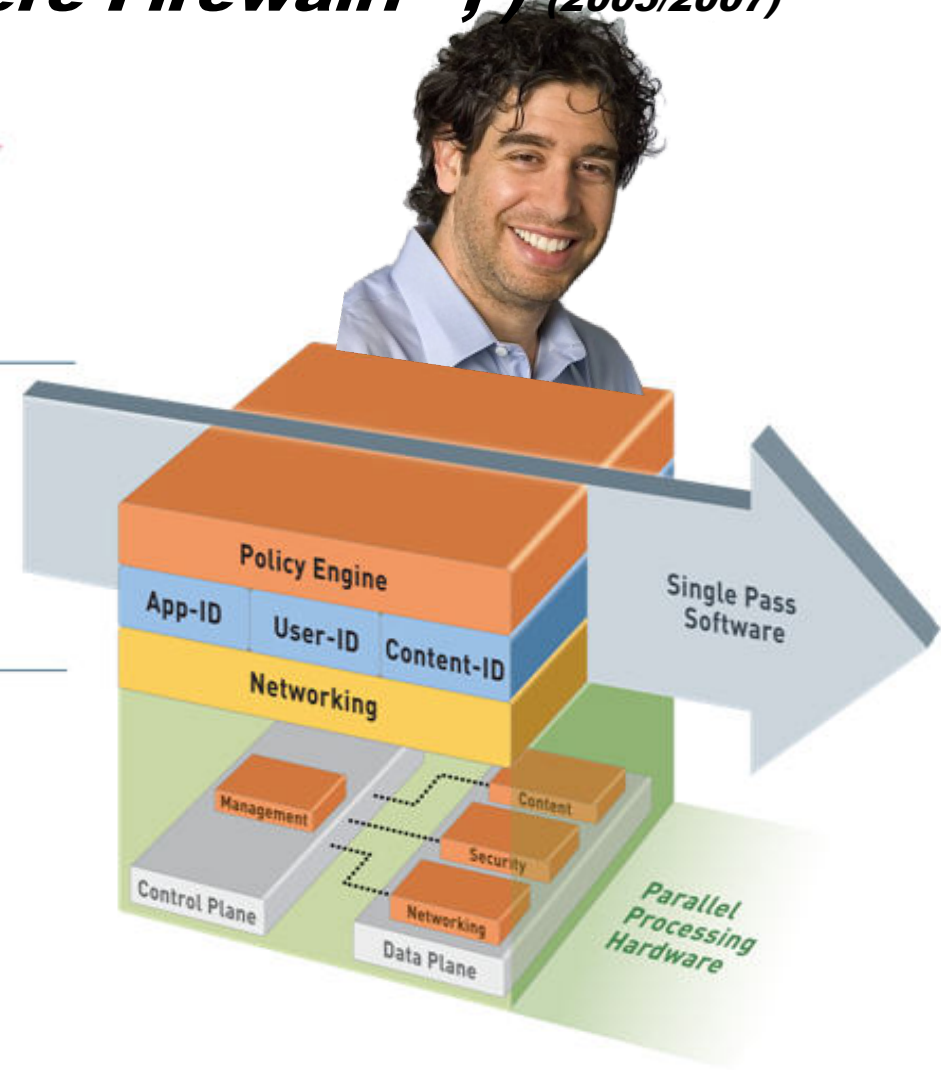
User-ID™

Identify the user

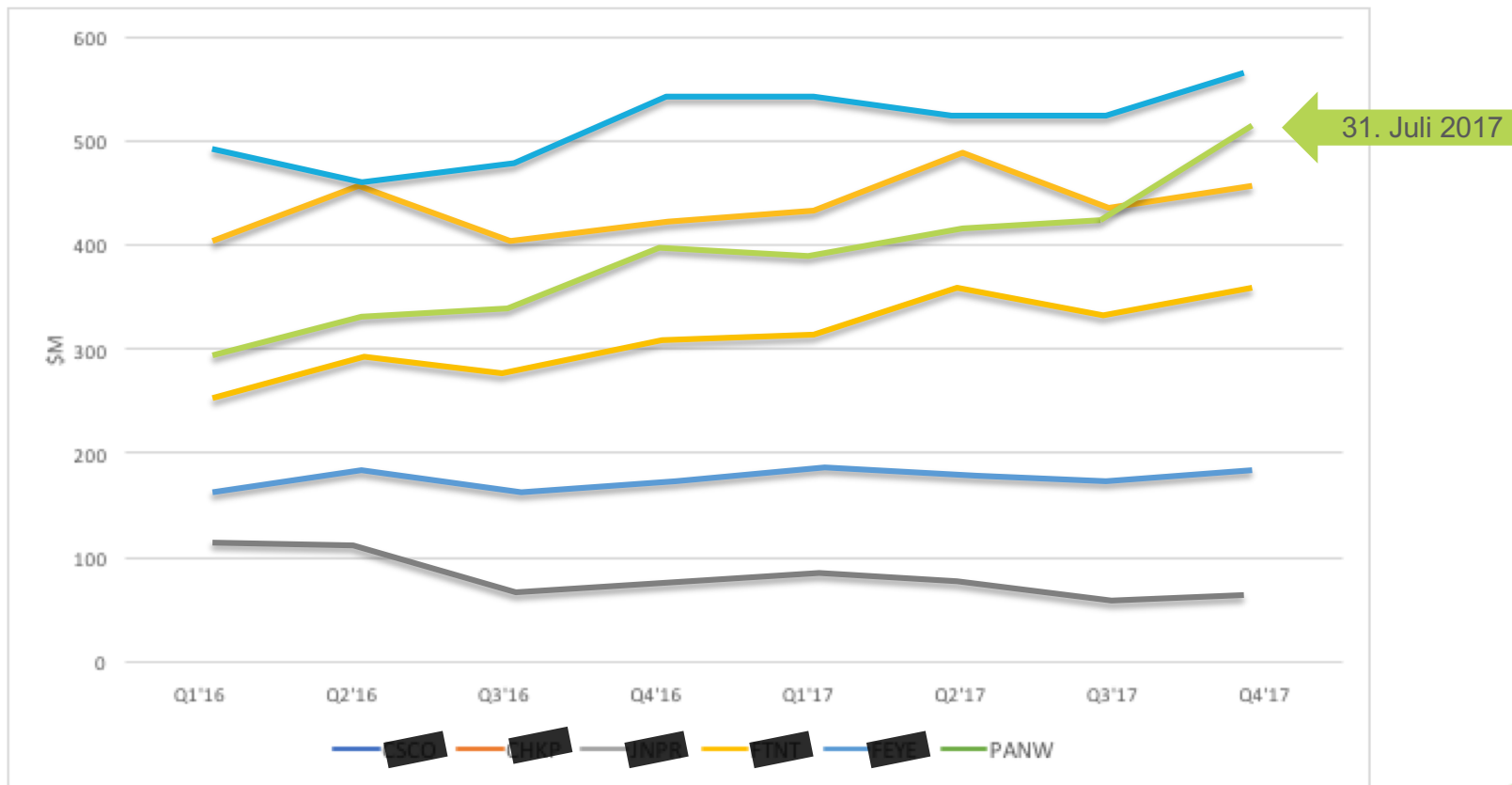


Content-ID™

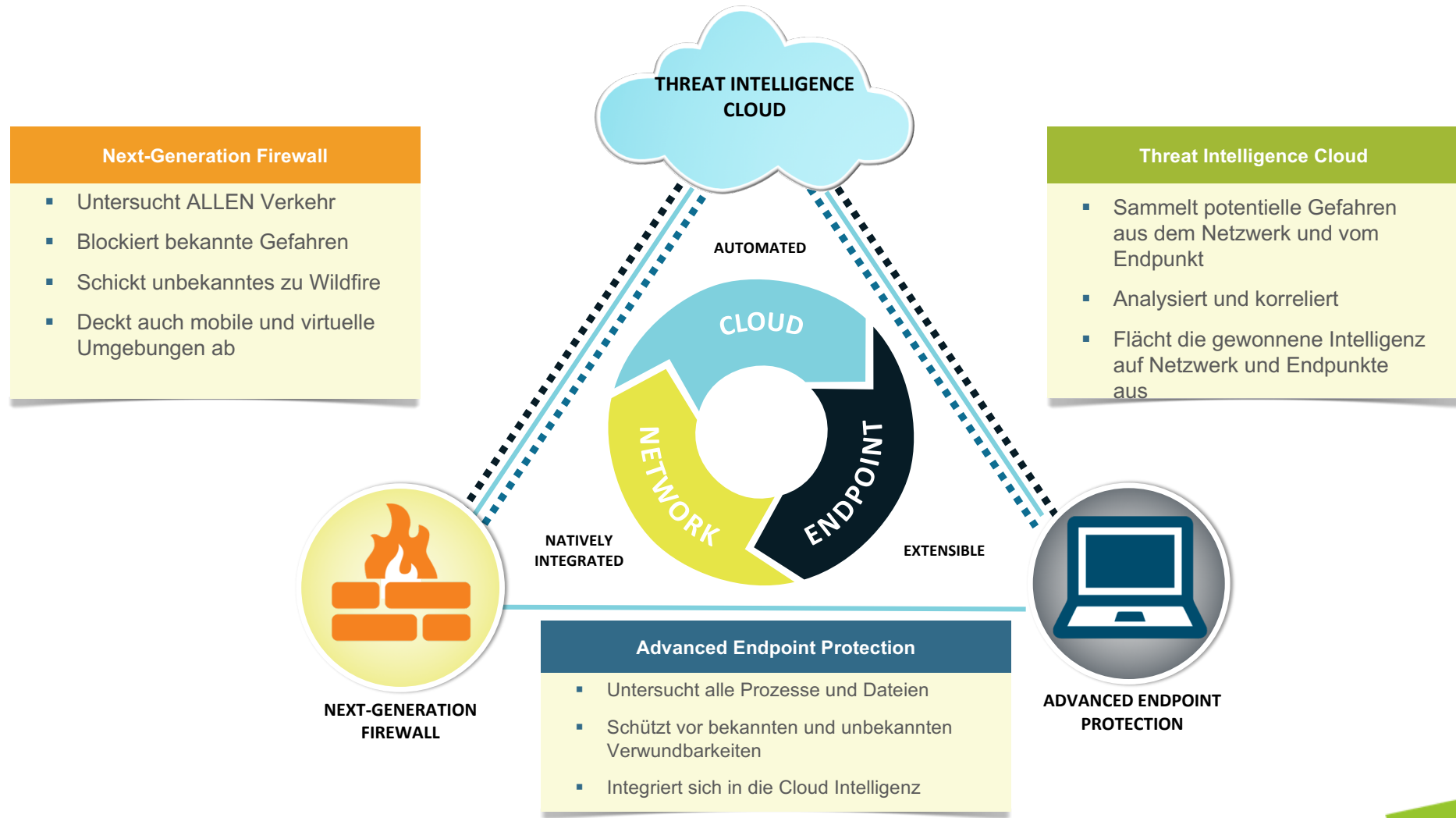
Scan the content



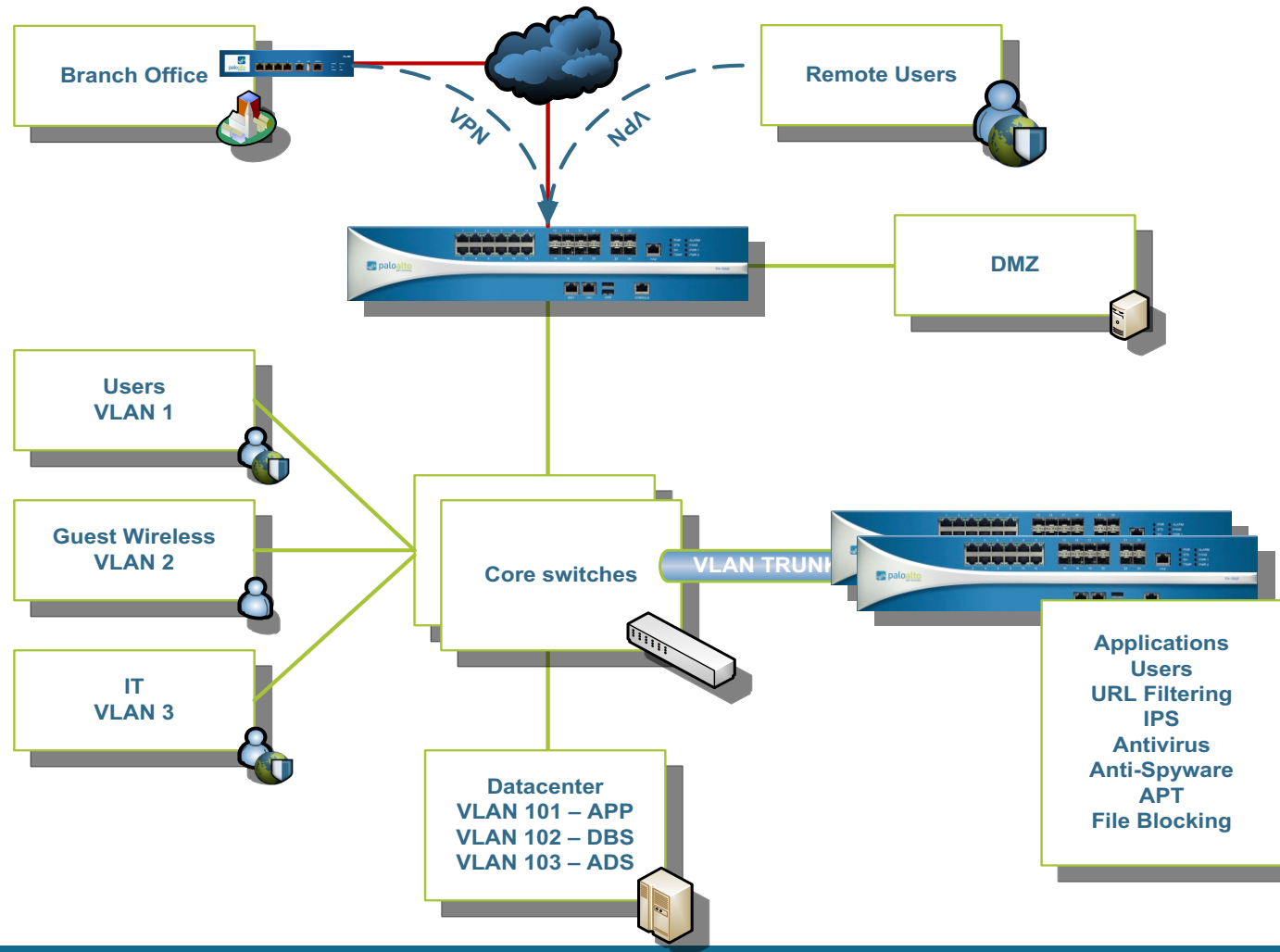
“Wer braucht denn noch eine weitere Firewall?“ ;-) (2005/2007)
Security Revenue Trend

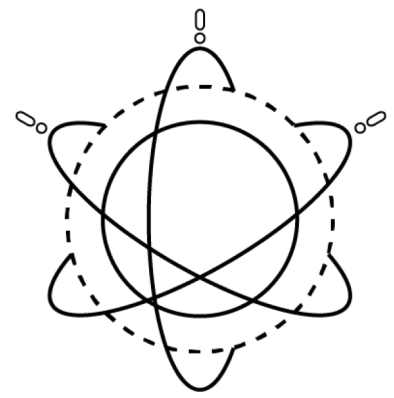
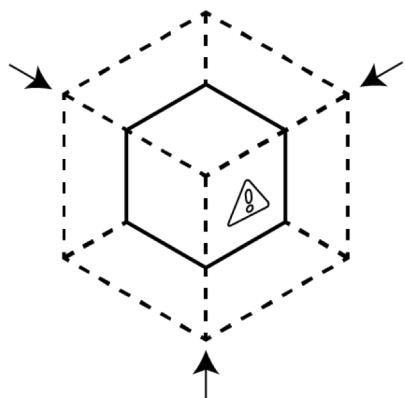
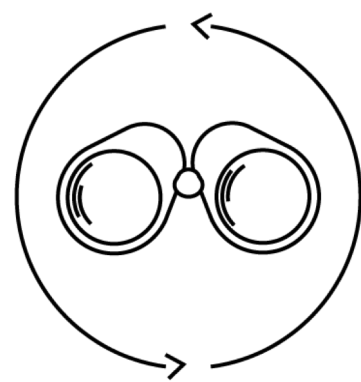


Die Palo Alto Networks Plattform



Das “Zero-Trust-Konzept” (2010)



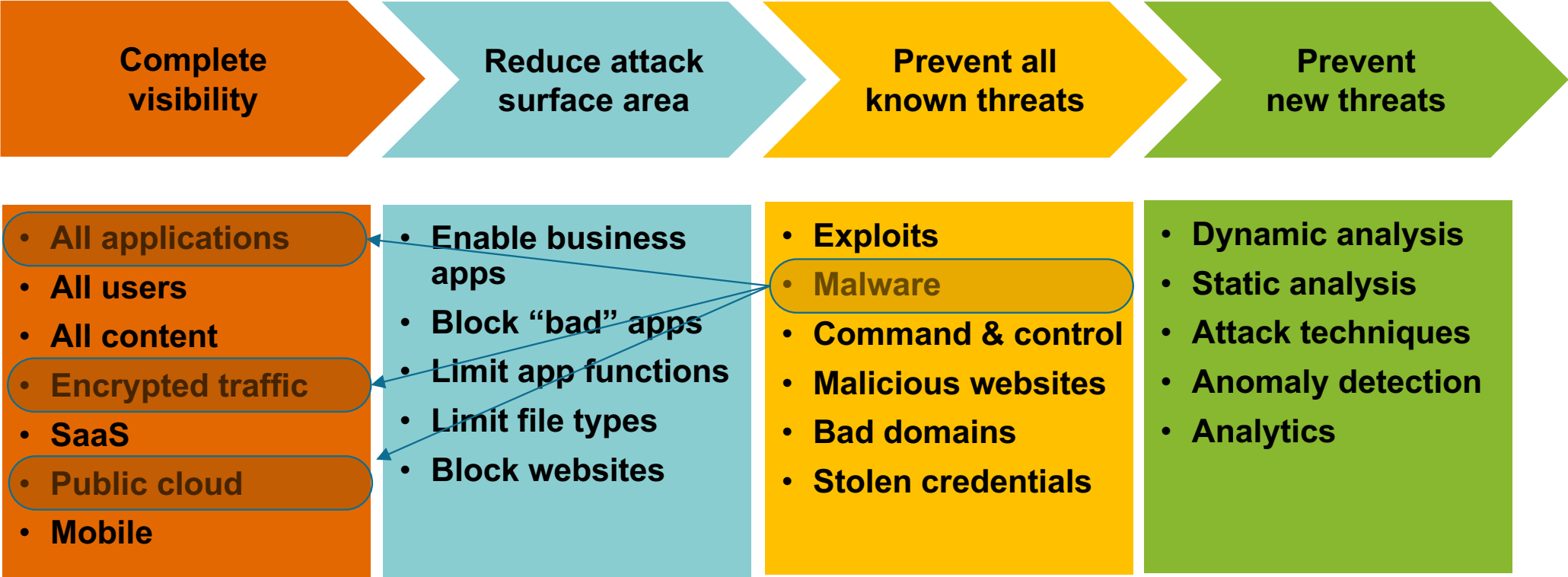


**Complete
visibility**

**Reduce attack
surface area**

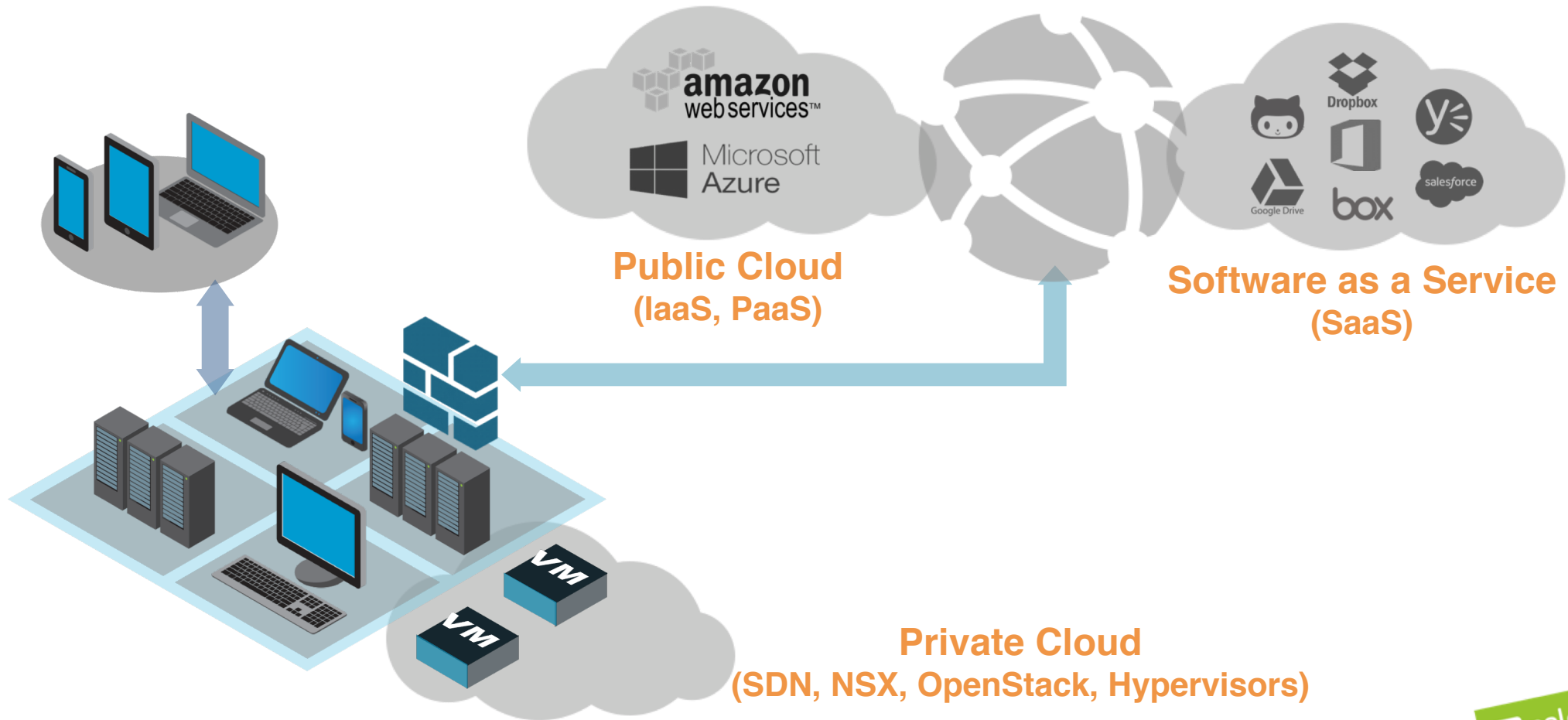
**Prevent all
known threats**

**Prevent
new threats**



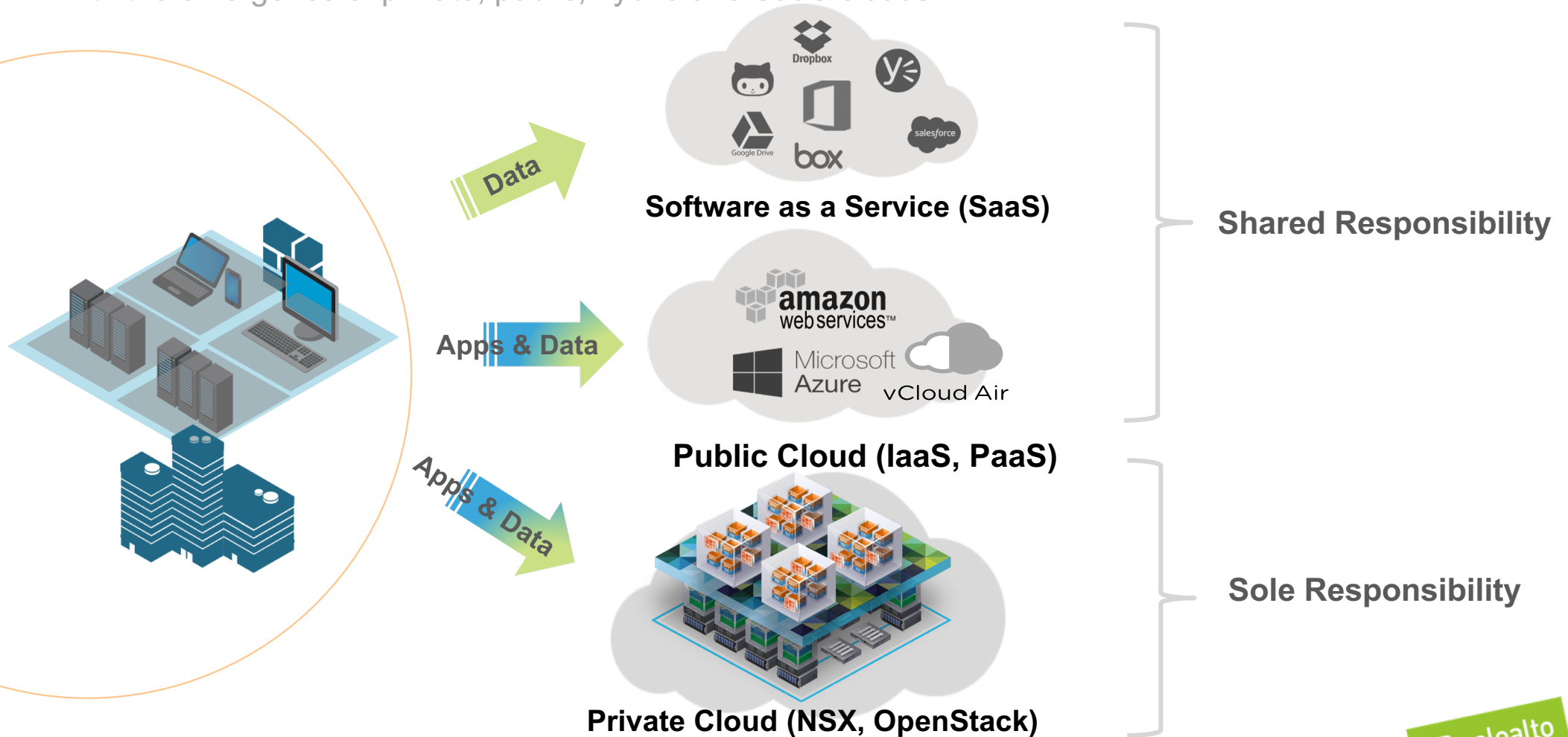
Aperture

Agility Driving Change



Managing Risk Has Become More Complex

..with the emergence of private, public, hybrid and SaaS clouds...



SAAS Risks



**MALWARE
PROPAGATION**



**ACCIDENTAL
DATA EXPOSURE**



**MALICIOUS
DATA EXFILTRATION**

A Journey For Complete SAAS Security



1

Discover and Understand SaaS Usage

2

Control SaaS Usage on any device

3

Control Exposure and Malware in the cloud

Discover And Understand SAAS Usage



I want to...

- Know all apps are being used
- Know who are using these apps
- Know what data transferred to/from these apps

SAAS Usage Reporting

1

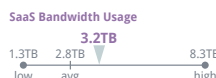
SAAS APPLICATION USAGE REPORT



KEY FINDINGS

- 80% of SaaS applications in your network are unsanctioned
- Your SaaS application usage is **more** than most Palo Alto Networks customers
- 57% of users in your network use one or many unsanctioned SaaS applications

The SaaS Application Usage Report summarizes actionable insight into SaaS application use in your organization for the 7 days captured in this report. Unsanctioned SaaS applications are SaaS Applications not approved or monitored by your security organizations. Unsanctioned applications could present a risk to your organization.

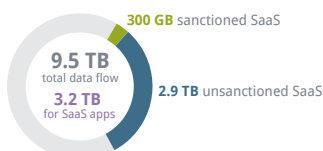


SaaS App Usage Benchmarks
Your SaaS application usage compared to other Palo Alto Networks customers.

Applications



Bandwidth



Users

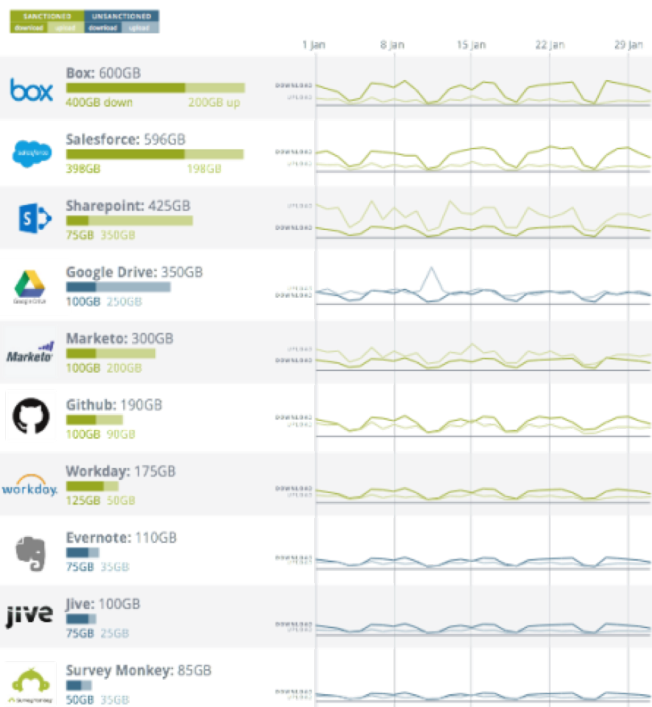


REPORT PERIOD: 7 days

SAAS APPLICATION USAGE REPORT | PALO ALTO NETWORKS 1

TOP 10 SAAS APPLICATIONS BY DATA MOVEMENT

The graph below shows top SaaS applications by the amount of data movement they generated.



REPORT PERIOD: 7 days

SAAS APPLICATION USAGE REPORT | PALO ALTO NETWORKS 5

FILE-SHARING APPLICATIONS AT A GLANCE

Top 10 file-sharing applications by data transfer (includes SaaS and non-SaaS).

APPLICATION	SANCTIONED?	SAAS?	USERS	FILES	BYTES
FTP X	yes	non-SaaS	2,047,272	2,047,272	2,047,272
Box	yes	SaaS	1,847,483	1,847,483	1,847,483
Google Drive	no	SaaS	944,253	944,253	944,253
Dropbox	no	SaaS	696,167	696,167	696,167
Zipshare	no	SaaS	683,161	683,161	683,161
4Shared	no	SaaS	607,418	607,418	607,418
iCloud	no	SaaS	523,886	523,886	523,886
Cloud Drive	no	SaaS	477,734	477,734	477,734
Photo Bucket	no	SaaS	200,026	200,026	200,026
Egnyte	no	SaaS	183,188	183,188	183,188

Top 3 File-Sharing Applications Detail

FTP	box	Google Drive
FTP Sanctioned non-SaaS 5101 users 100 files - 6TB	box.net Sanctioned SaaS 5101 users 100 files - 6TB	Google Drive Not sanctioned SaaS 5101 users 100 files - 6TB
Wildfire submissions: 22 Benign: 21 Malicious: 1	Wildfire submissions: 321 Benign: 318 Malicious: 3	Wildfire submissions: 12 Benign: 12 Malicious: 0
TOP 10 USERS BY DATA MOVEMENT	TOP 10 USERS BY DATA MOVEMENT	TOP 10 USERS BY DATA MOVEMENT
Colin Kapernick Torrey Smith Joe Skaley Al Smith Guest 1 10.3.4.55 10.45.4.33 Navarro Bowman Eric Reid Reggie Bush	Colin Kapernick Torrey Smith Joe Skaley Al Smith Guest 1 10.3.4.55 10.45.4.33 Navarro Bowman Eric Reid Reggie Bush	Colin Kapernick Torrey Smith Joe Skaley Al Smith Guest 1 10.3.4.55 10.45.4.33 Navarro Bowman Eric Reid Reggie Bush
TOP 10 BLOCKED OR ALERTED FILE TYPES	TOP 10 BLOCKED OR ALERTED FILE TYPES	TOP 10 BLOCKED OR ALERTED FILE TYPES
MP3 454 ZIP 123 EXE 99 MPEG 80 APK 43 DOC 12 BAT 6 SWF 5 RES 4 GZIP 1	MP3 454 ZIP 123 EXE 99 MPEG 80 APK 43 DOC 12 BAT 6 SWF 5 RES 4 GZIP 1	MP3 454 ZIP 123 EXE 99 MPEG 80 APK 43 DOC 12 BAT 6 SWF 5 RES 4 GZIP 1
TOP 10 THREATS	TOP 10 THREATS	TOP 10 THREATS
SSLv3 found 534 FTP login failed 123 HTTP parameters 111 Illegal parameter 12 SSLv3 found 9 FTP login failed 8 HTTP parameters 7 Illegal parameter 7 SSLv3 found 4 FTP login failed 2	SSLv3 found 534 FTP login failed 123 HTTP parameters 111 Illegal parameter 12 SSLv3 found 9 FTP login failed 8 HTTP parameters 7 Illegal parameter 7 SSLv3 found 4 FTP login failed 2	SSLv3 found 534 FTP login failed 123 HTTP parameters 111 Illegal parameter 12 SSLv3 found 9 FTP login failed 8 HTTP parameters 7 Illegal parameter 7 SSLv3 found 4 FTP login failed 2
SEVERITY	SEVERITY	SEVERITY
Critical High Medium Low Info	Critical High Medium Low Info	Critical High Medium Low Info

REPORT PERIOD: 7 days

SAAS APPLICATION USAGE REPORT | PALO ALTO NETWORKS 8



An Example

1

John uploads a PDF to OneDrive for Business

User-ID

Content-ID

App-ID

NGFW

APERTURE

Control SAAS Usage On Any Device



I want to...

- Block apps where risk is unmanageable
- Limit functions for apps that are allowed but not managed
- Enforce deep security on apps that are sanctioned

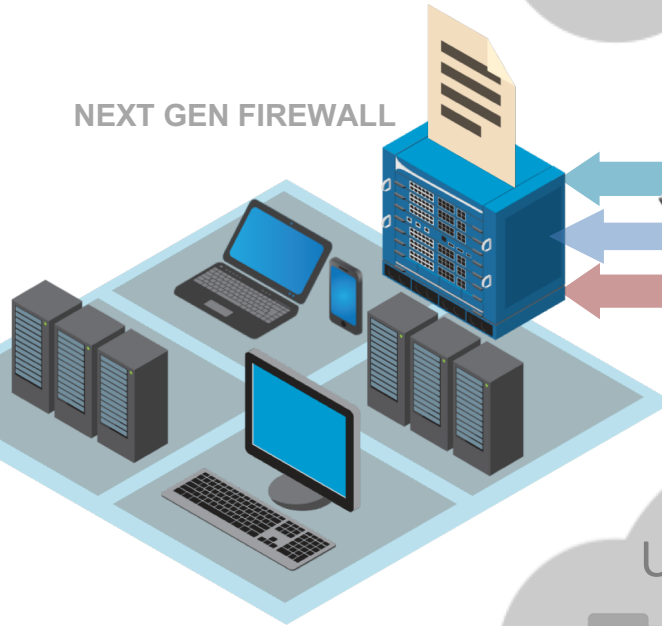
Control Usage

2

GLOBALPROTECT



NEXT GEN FIREWALL



SANCTIONED



TOLERATED



UNSANCTIONED



An Example

2

John uploads a PDF to OneDrive for Business

ALLOW

John uploads a EXE to OneDrive for Personal

BLOCK

NGFW

User-ID

Content-ID

App-ID

File Blocking

APERTURE

Control Exposure And Malware In The Cloud

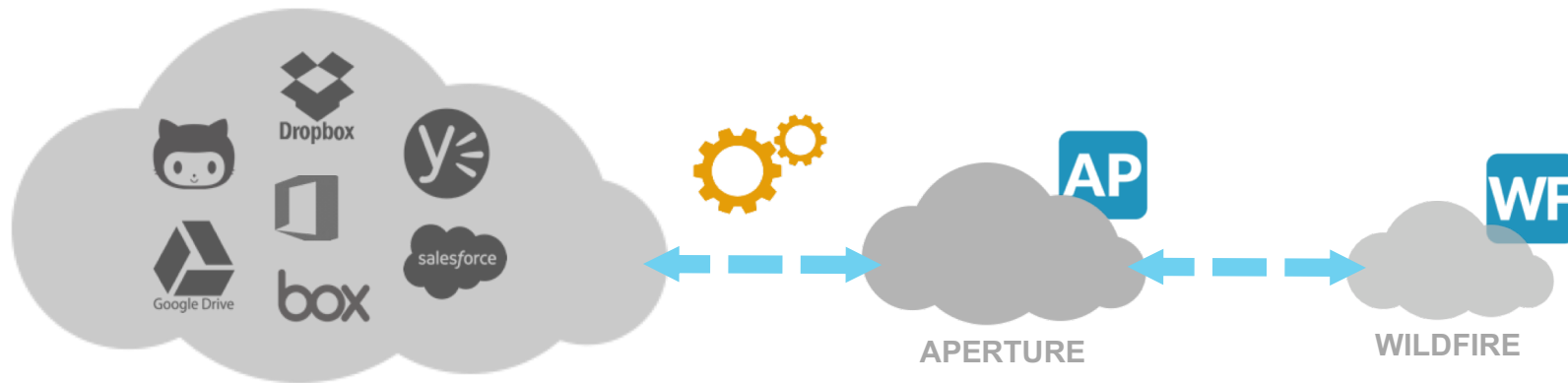


I want to...

- Block malware propagating through SaaS apps
- Prevent sharing and exposure of sensitive data
- Monitor all user and data activity in the SaaS app

Securely Enable Sanctioned Apps With Aperture

3



COMPLETE VISIBILITY & CONTROL

Prevent data exposure
and enforce compliance

PREVENT MALWARE

Known and unknown
malware

AUTOMATED REMEDIATION

Quarantine assets,
limit sharing, log and
notify users instantly

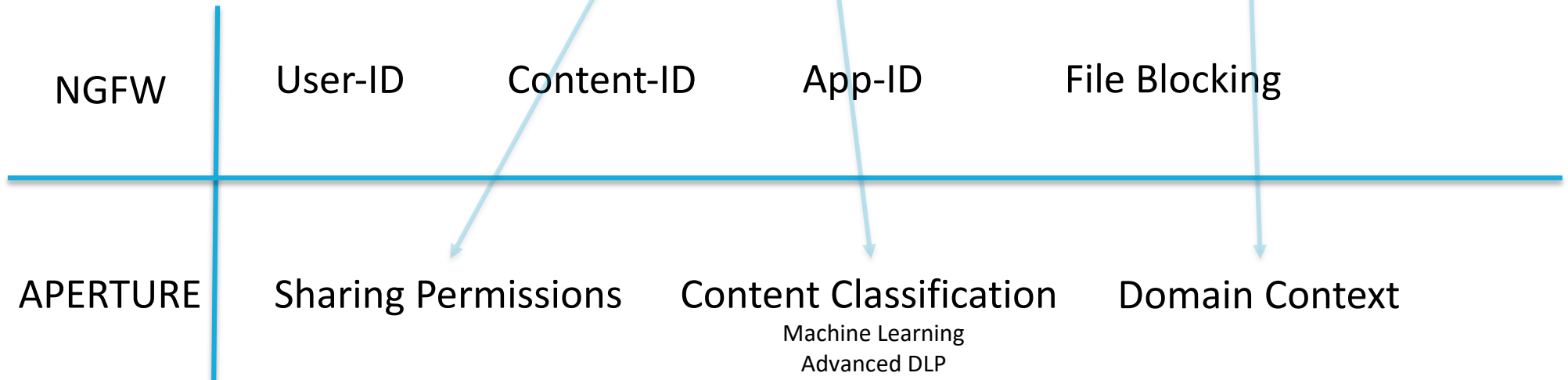
RETROACTIVE POLICY

Policy applies
to past and
future events

An Example

3

John uploads a PDF to OneDrive for Business
PDF is a sensitive legal document
John shares the PDF with his personal email



Expansion Of Aperture

SANCTIONED APPS

IMPROVED



OFFICE 365



BOX.COM



GITHUB



GOOGLE DRIVE

IMPROVED



SFDC

IMPROVED



DROPBOX



YAMMER

NEW



SLACK

NEW



SECURE DATA
SPACE



AMERICAS

NEW



EMEA

NEW

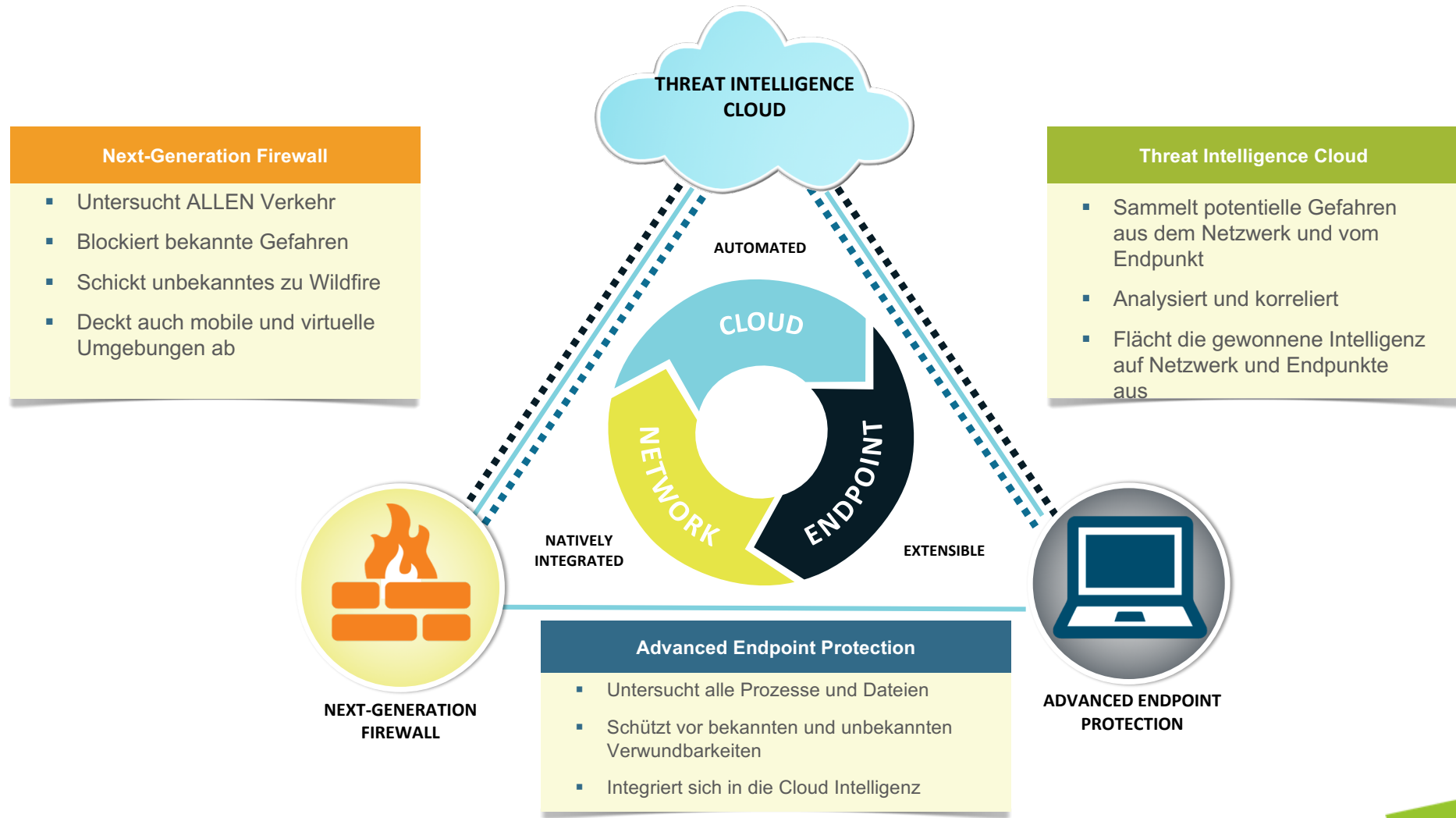


APAC

UNSANCTIONED & TOLERATED APPS

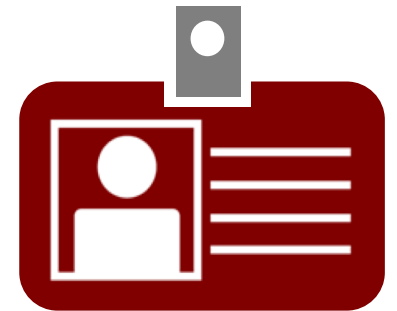
- 2300+ Apps (SaaS and Non-SaaS Apps) with App-ID
- 6 new App-ID every week
- Custom App-ID
- URL Filtering (adding 70K URLs/day)

Die Palo Alto Networks Plattform

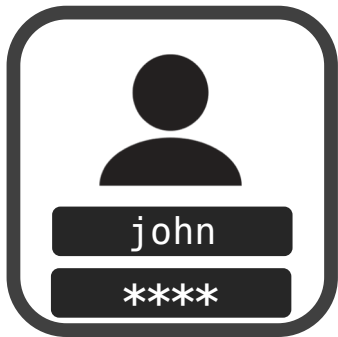


Beispiel:

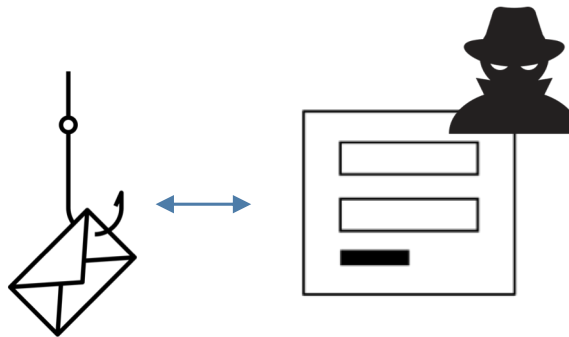
Schutz vor Diebstahl und Missbrauch von Zugangsdaten



THE PROBLEM



Password-based credentials provide an easy way to bypass the attack lifecycle

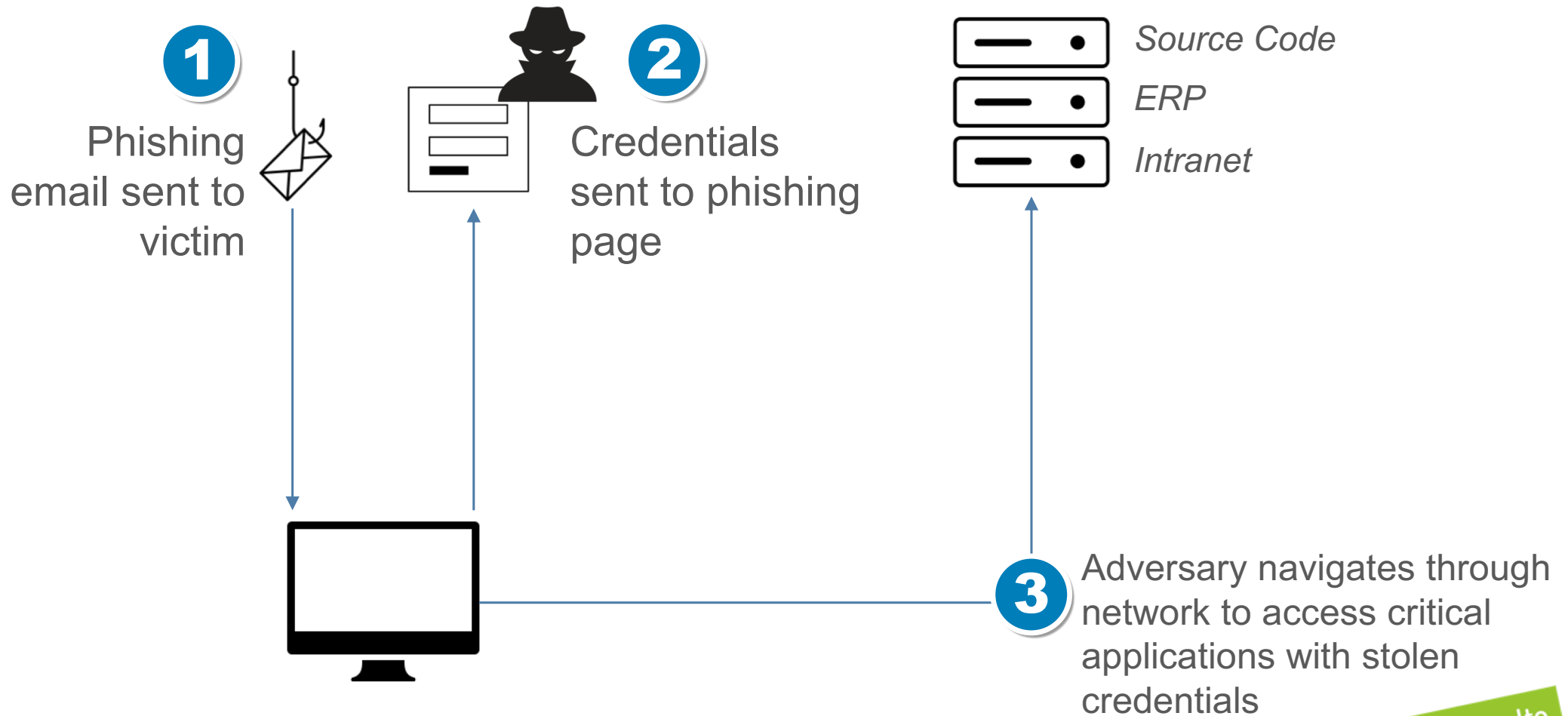


Attackers are actively using credential phishing to target organizations

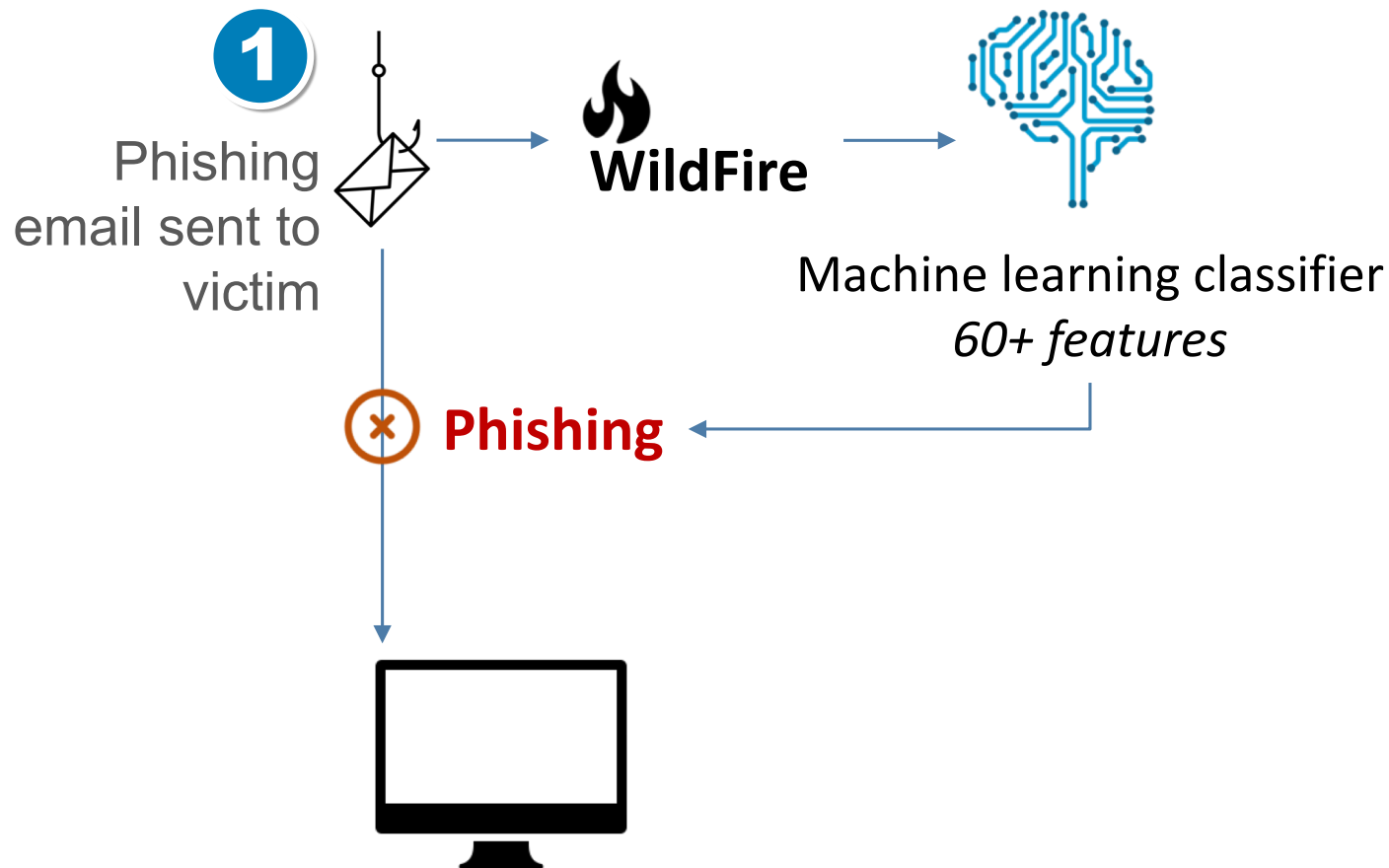


Multi-Factor Auth prevents this type of attack, but is difficult to deploy pervasively

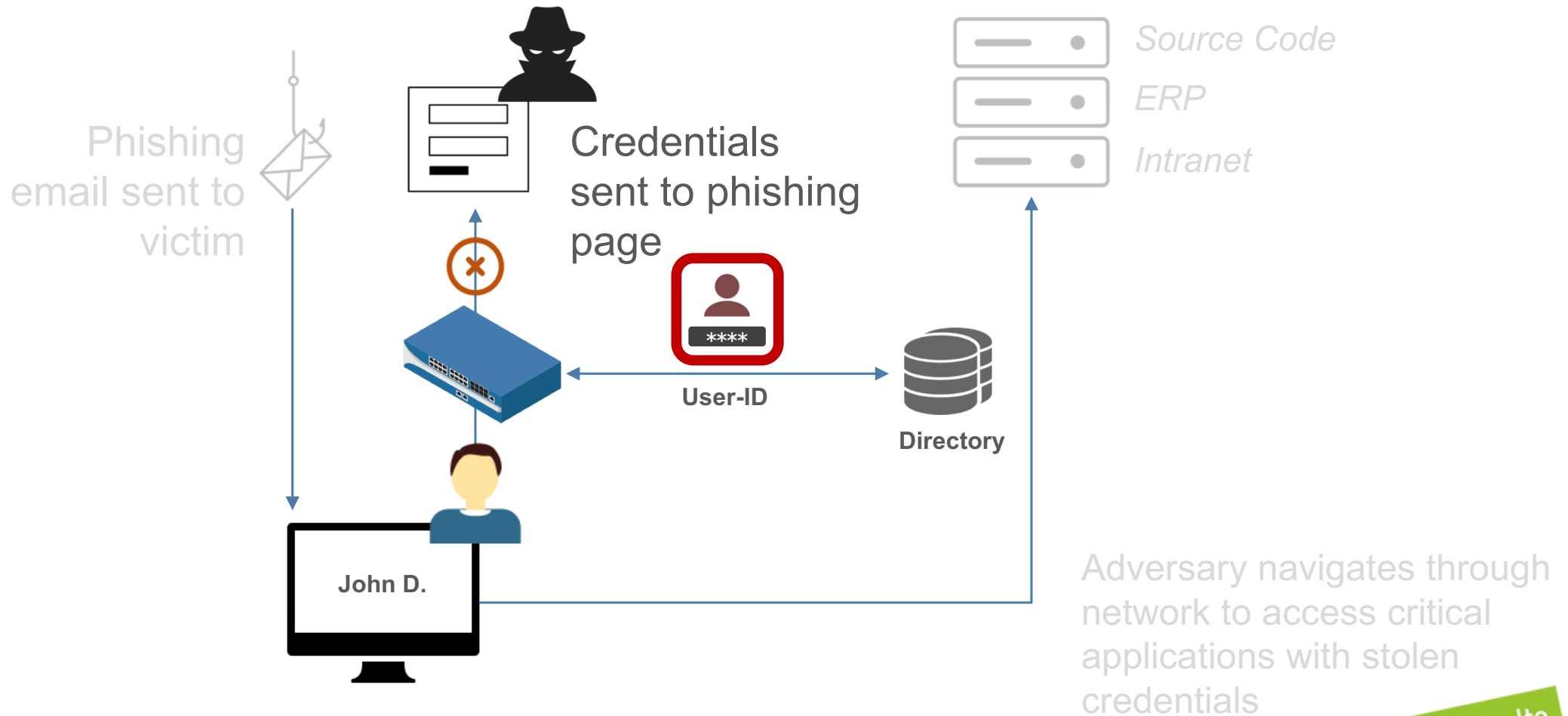
ANATOMY OF A CREDENTIAL THEFT-BASED ATTACK



Identify and block the phishing page



IDENTIFY AND BLOCK CREDENTIAL PHISHING ATTEMPTS



Credential Detection Explained

Known user names

- Detect submission of **valid users names**.
-
- Uses information retrieved from a **connected LDAP directory** to detect **uniquely created user identifiers** that don't resemble real names.

Known logged in users

- Detect submissions of user names for logged in users for **visibility** and **user education**.
-
- Uses information **available in User-ID** to detect the **known user name** for the **source IP of a session**.

Known user credentials

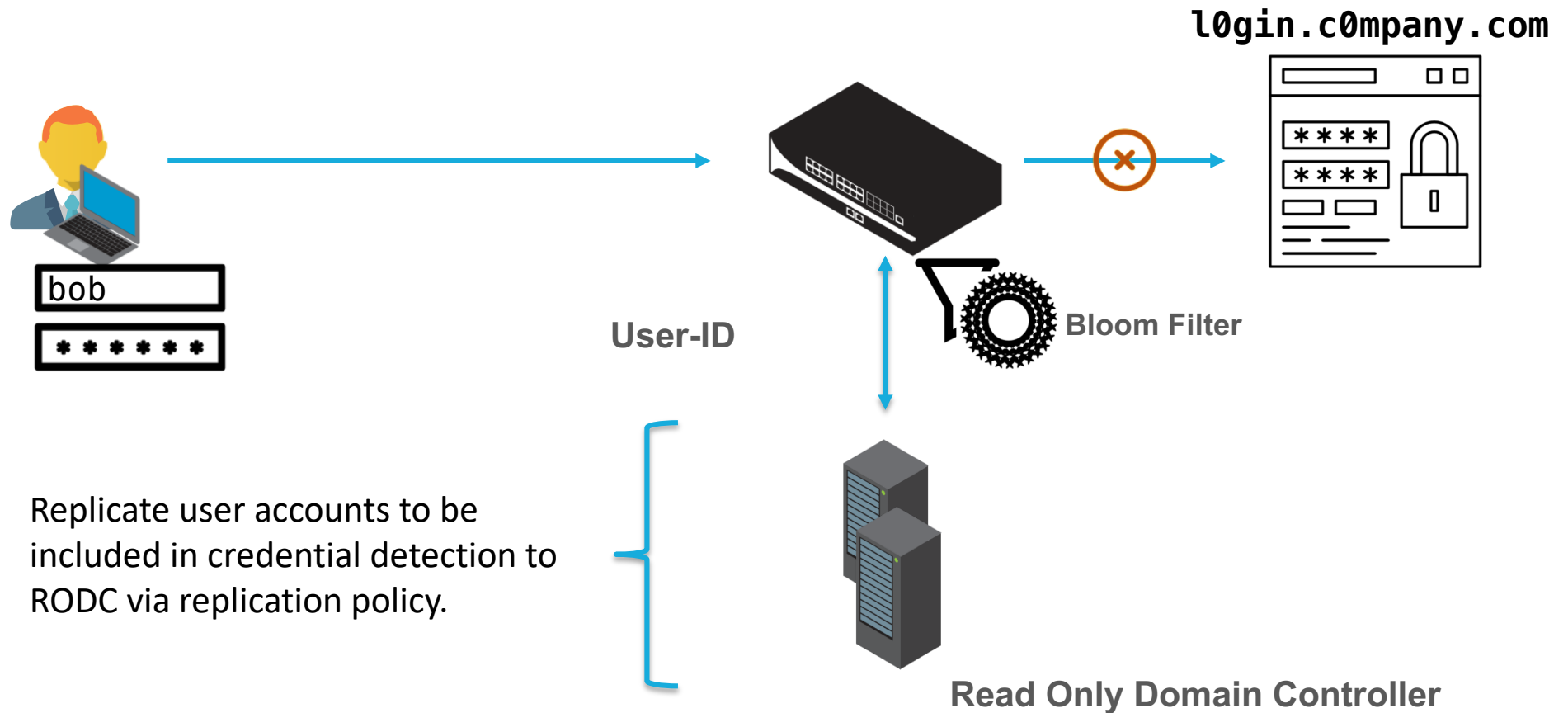
- Exact credential submission to **prevent credential leakage** with zero false negatives.
-
- Used to detect the **known user name and password** for the source of a session, by **using the User-ID Agent and the User-ID Credential Agent add-on**.

Prevent credential re-use

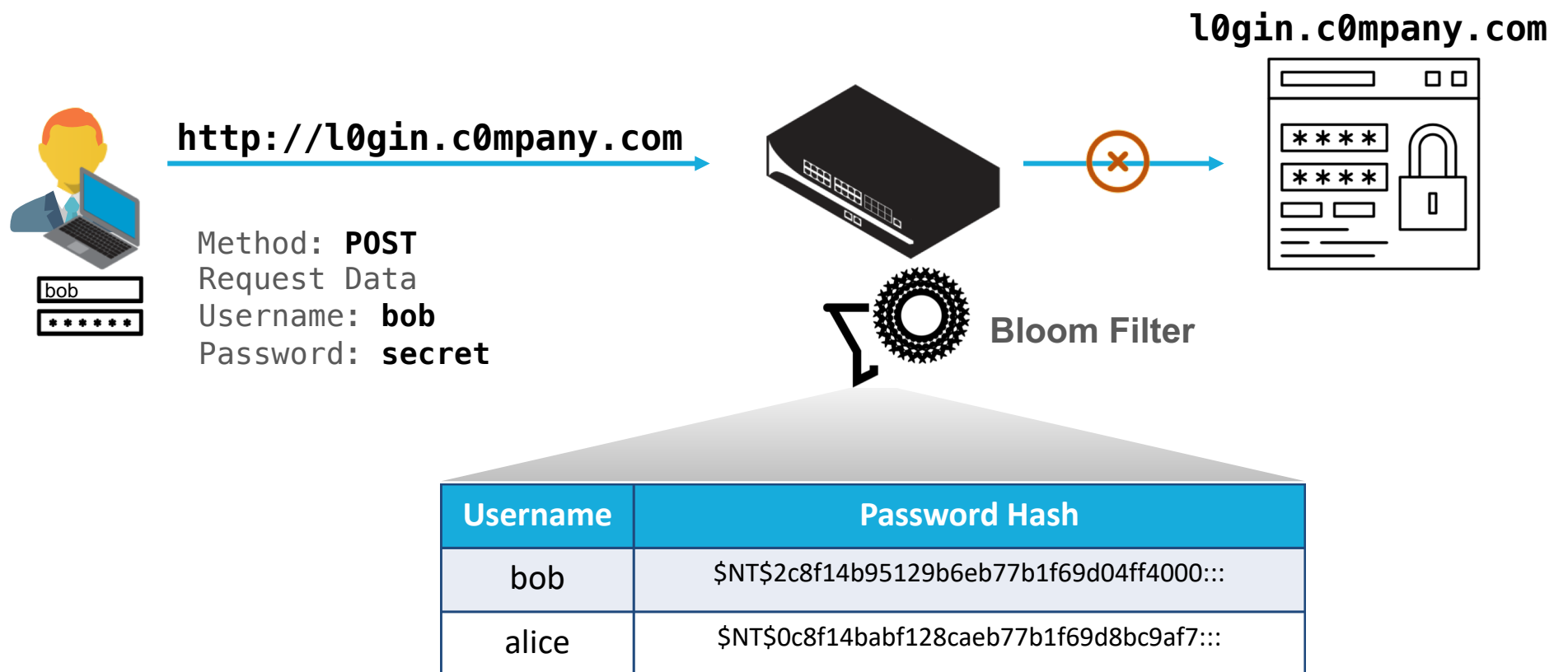


Prevent credential theft

Credential Detection - User-ID



Credential Detection - Firewall



What is a Bloom Filter?

- 1 Collect data and create a table of hashes.

P4ssw0rd!	hash	18	a0	e6	a5	be	cb	68	a3	eb	67	27	0c	f6	e9	7a	c3
P4ssw0rd	hash	69	c8	79	0e	45	9b	5e	b7	94	17	2b	f0	ce	09	46	81
p4ssw0rd	hash	f1	69	7e	66	a0	8b	79	53	2d	58	02	a5	cf	6f	fa	4c
password!	hash	09	5f	e3	fd	56	e6	d7	69	c4	23	10	64	59	c1	57	89
password	hash	28	67	55	fa	d0	48	69	ca	52	33	20	ac	ce	0d	c6	a4

- 2 Deconstruct into stream of individual de-duplicated byte groups.

18	a0	e6	a5	be	cb	68	a3	eb	67	27	0c	f6	e9	7a	c3	69	c8	79	0e	45	9b	5e			
	b7	94	17	2b	f0	ce	09	46	81	f1	7e	66	8b	53	2d	58	02	cf	6f	fa	4c	5f	e3		
		fd	56	e6	d7	c4	23	10	64	59	c1	57	89	28	55	d0	48	ca	52	33	20	ac	0d	c6	a4

- 3 Hash data and match byte groups with Bloom Filter entries.

pa55word	hash	87	a4	52	43	78	7b	42	f0	ed	a5	0e	2a	37	88	1c	84	⊘
----------	------	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	---

Credential Detection - Policy

- Credential submission policy part of URL Filtering Profile

URL Filtering Profile

Name:

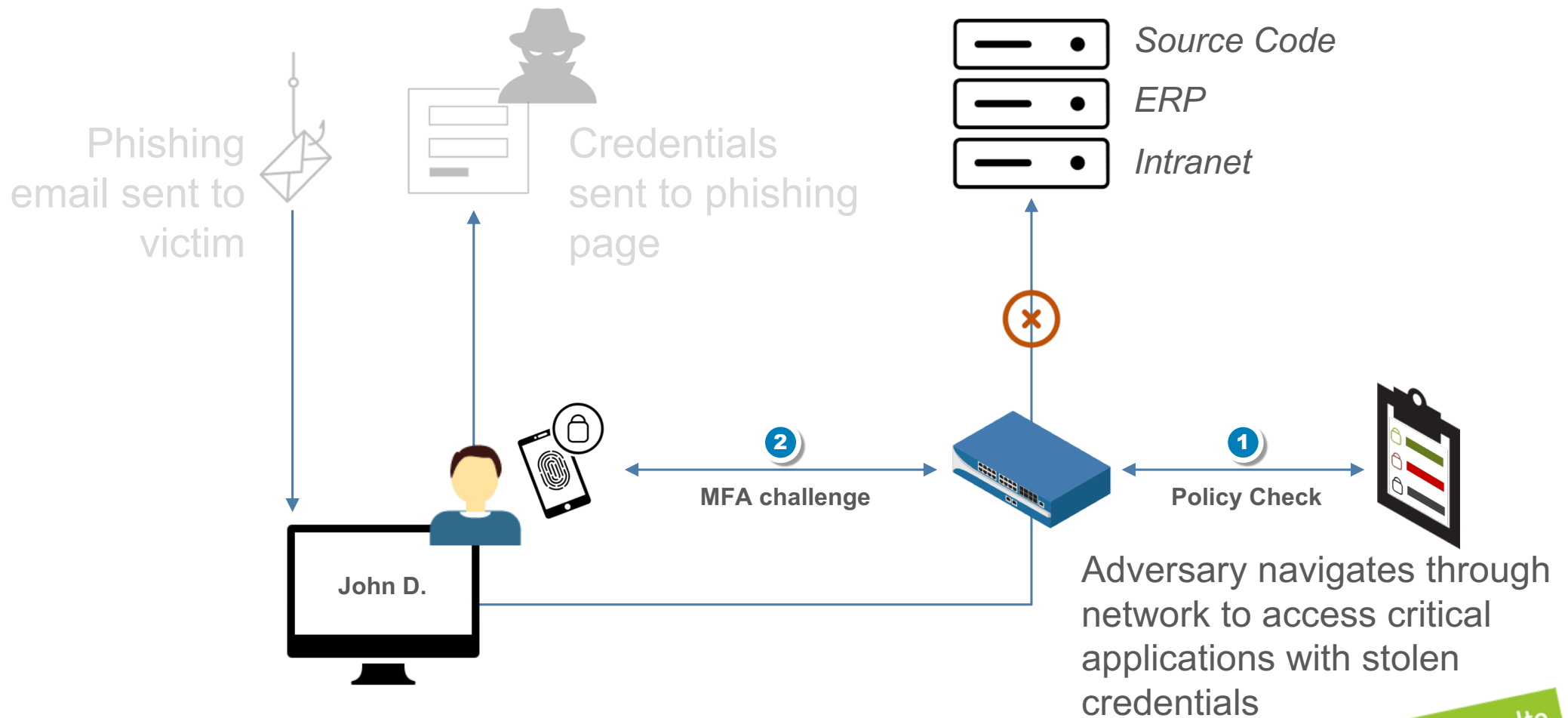
Description:

Categories | Overrides | URL Filtering Settings | User Credential Detection

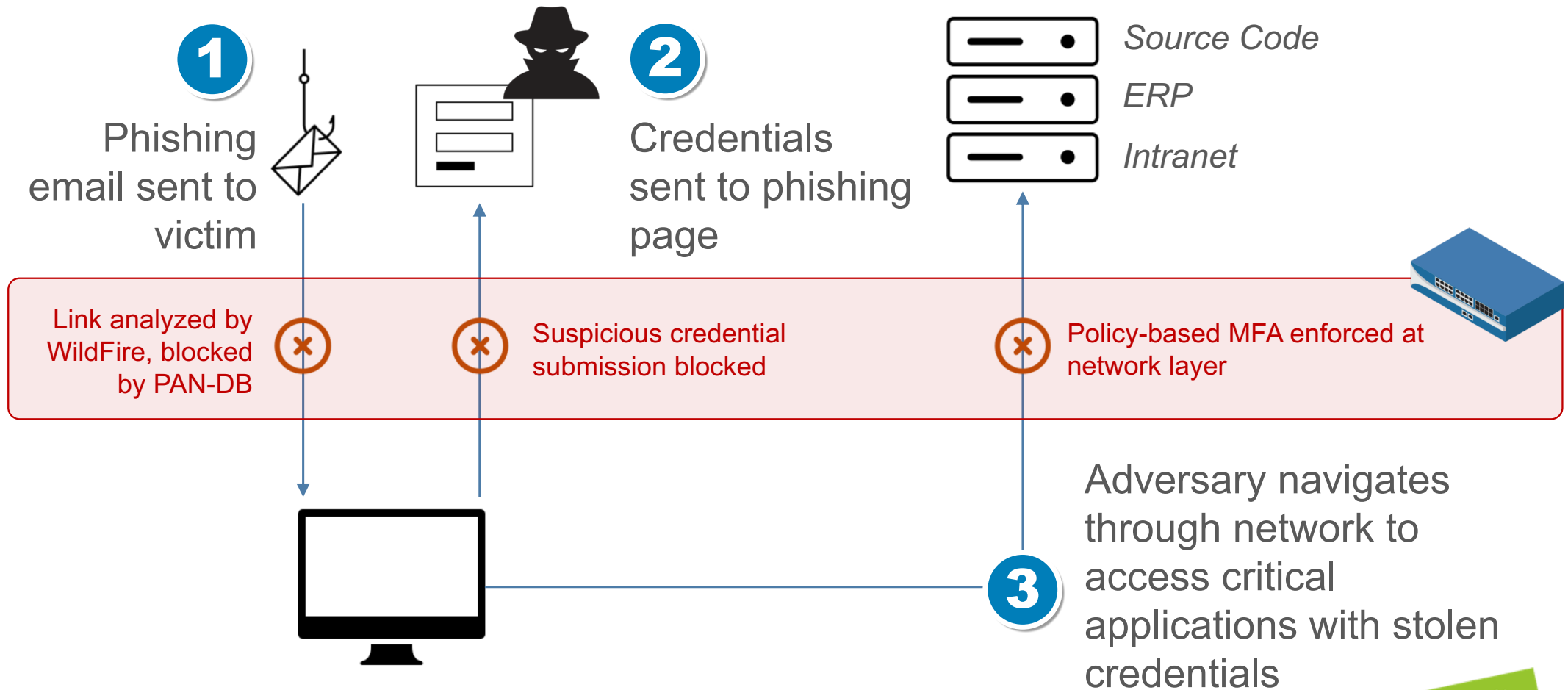
69 items

☐	Category	Site Access	User Credential Submission
☐	abortion	alert	continue
☐	abused-drugs	alert	continue
☐	adult	continue	block
☐	alcohol-and-tobacco	continue	block
☐	auctions	alert	continue
☐	business-and-economy	alert	continue

PREVENT USE OF STOLEN CREDENTIALS

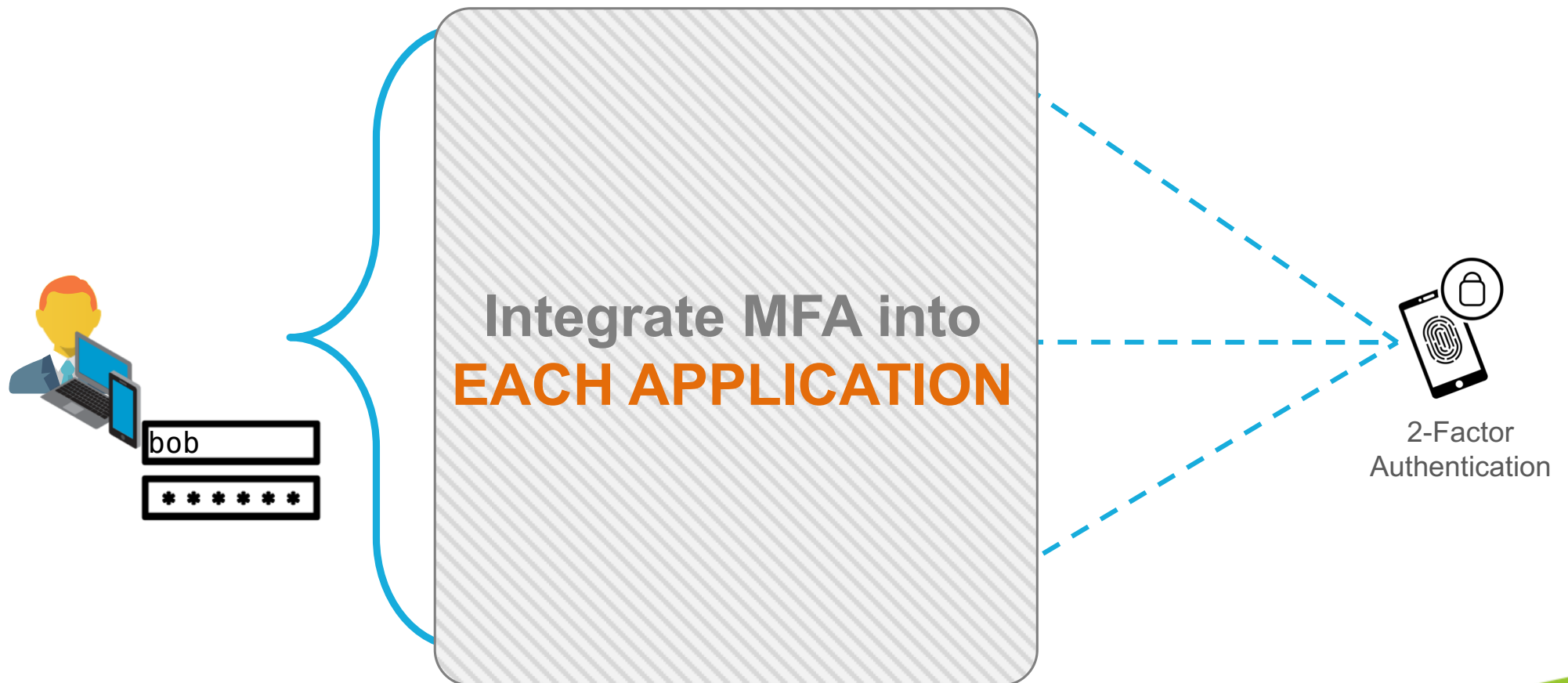


A PLATFORM APPROACH TO CREDENTIAL THEFT AND ABUSE

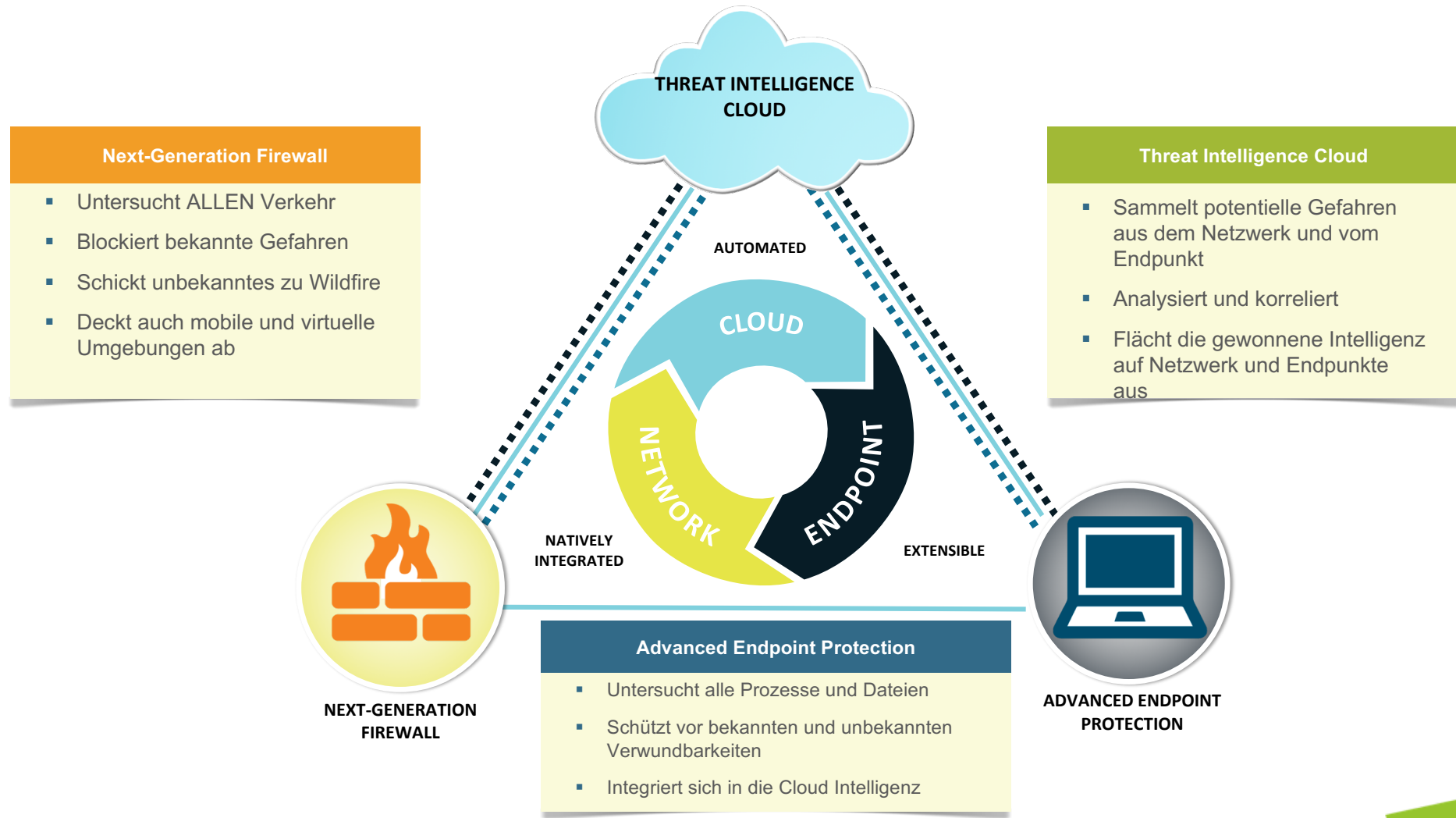


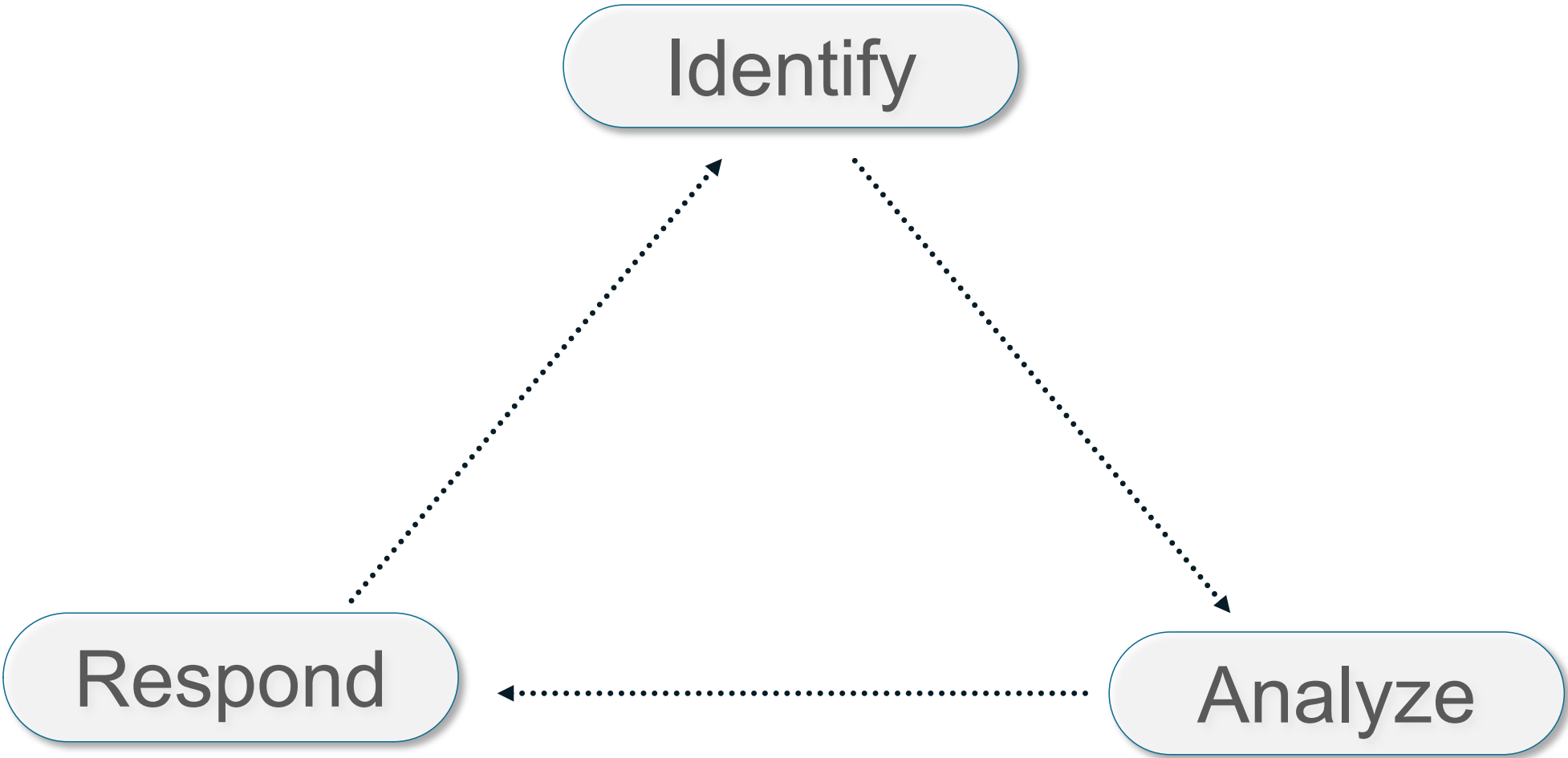
Neutralize the Value of stolen Credentials

MFA – Challenges with the current solution



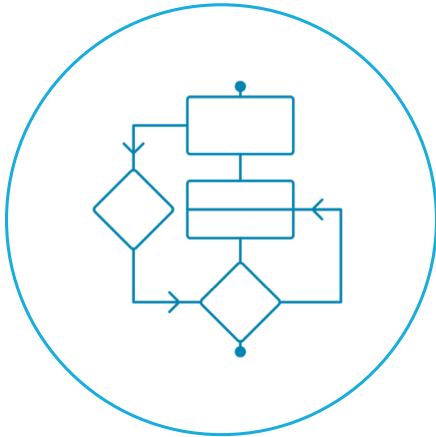
Die Palo Alto Networks Plattform







**Changing threat landscape
requires rapid deployment
of new technologies**



**Complex and manual
workflows across dozens
of security products**



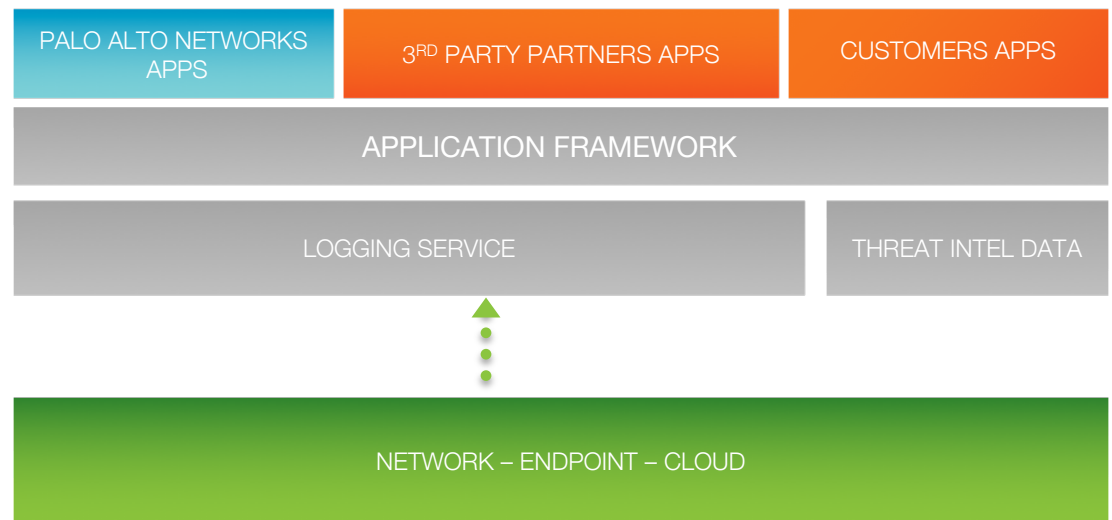
**New security product
deployments have up-
front ROI risk and cost**

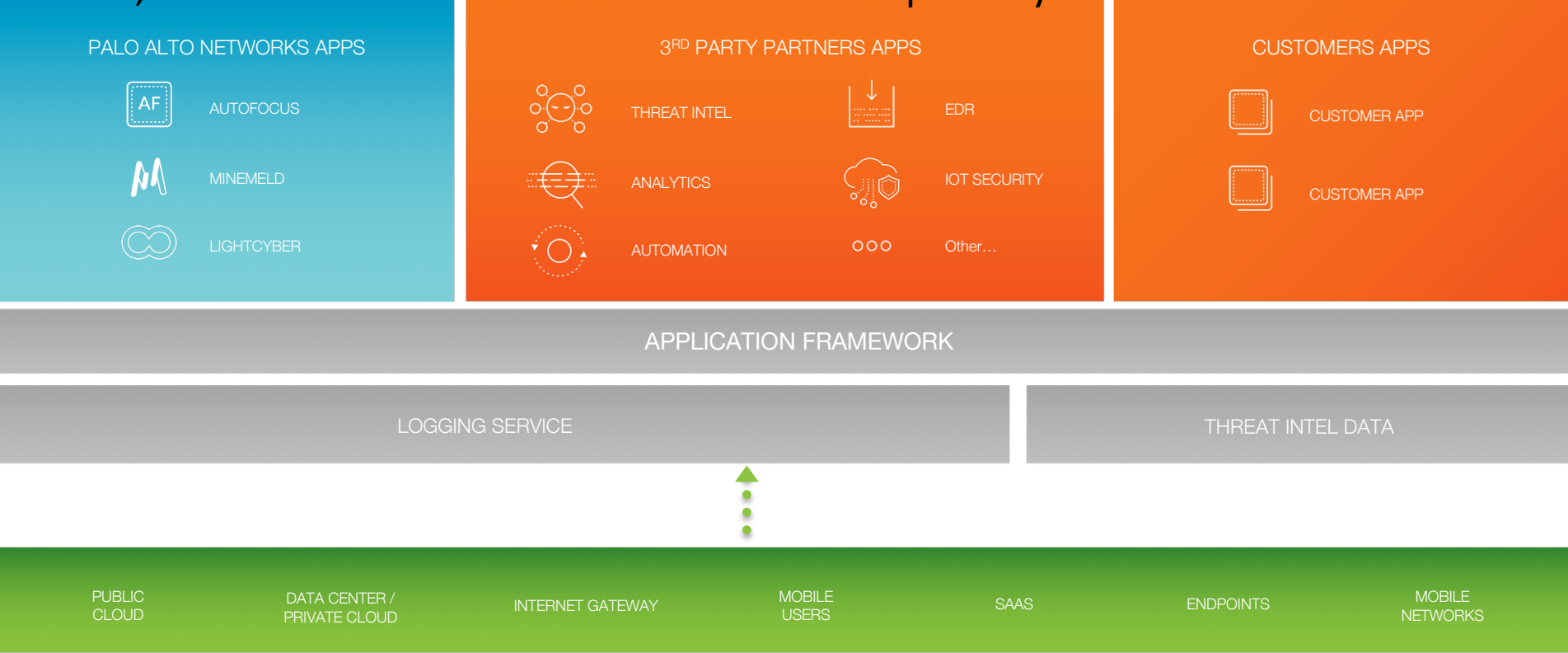
CHANGING THE CONSUMPTION MODEL OF SECURITY



44 | © 2017, Palo Alto Networks. Confidential and Proprietary.
Introducing the Application Framework

- Consume security through cloud-delivered apps from leading security providers.
- Extend the platform with innovative security capabilities with no additional infrastructure.
- Secure access to customer-specific data stores, compute, and services.
- Apps are developed by Palo Alto Networks, 3rd parties, MSSPs, and customers.





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

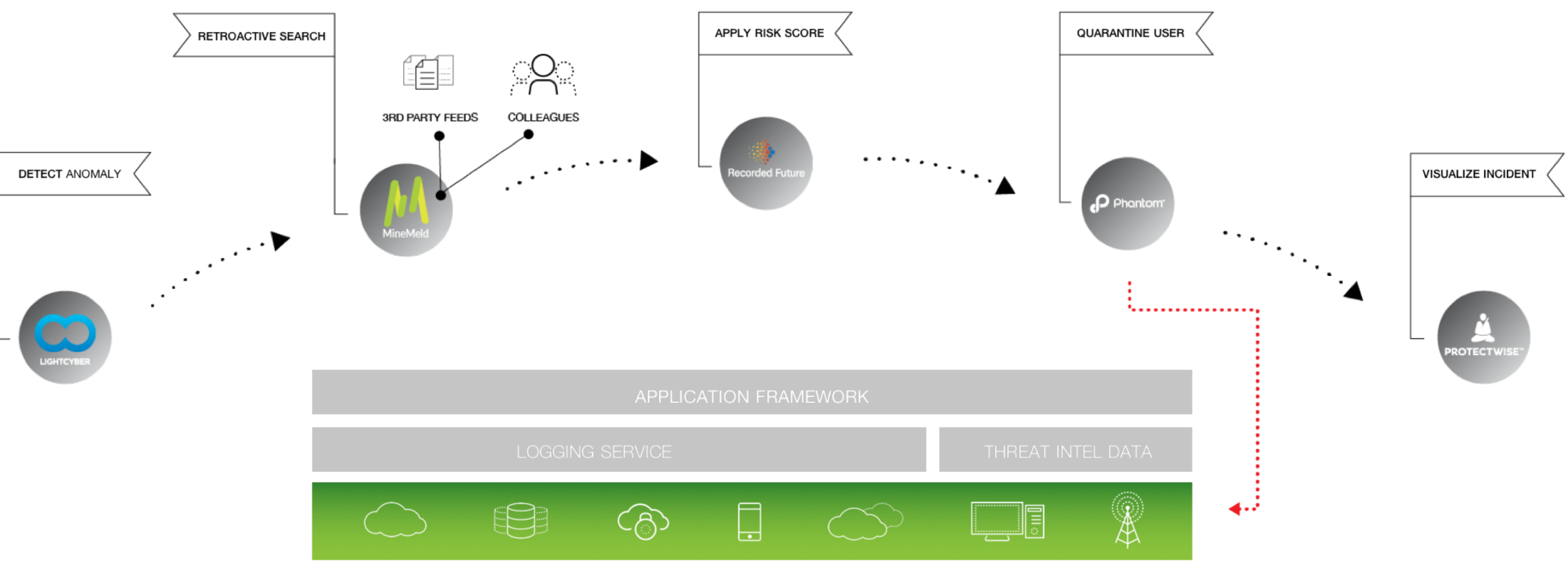
Customer-specific data store
Provides apps with rich data on a massive scale.

Apps
Apps extend the capabilities of the platform.



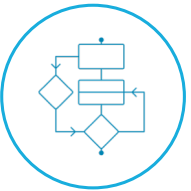




Value for customers



Superior 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.

Value for app developers



Seamless customer adoption: Reach nearly 40,000 Palo Alto Networks customers without having to develop, sell and deploy additional hardware.



Data access: Tune your machine learning, threat intelligence or other application logic with access to our customer-specific data store.



Speed to market: Accelerate the delivery of innovative apps with a unique SaaS-based consumption model.

greylockpartners.



SEQUOIA 

\$20M innovation fund

In collaboration with **Greylock Partners** and **Sequoia Capital**
Unleashing entrepreneurship for the Application Framework



- **Superior security** with high degrees of consistency by reinventing how customers rapidly **access, evaluate and adopt** the most compelling new security technologies.
- An **extension** of the Next-Generation Security Platform they **already own** and operate.
- Allows the adoption of **compelling cloud-based apps** developed by Palo Alto Networks and today's most **innovative** security providers, large and small.

