Desired security outcomes

Public Cloud Speed Boat Boot Camp

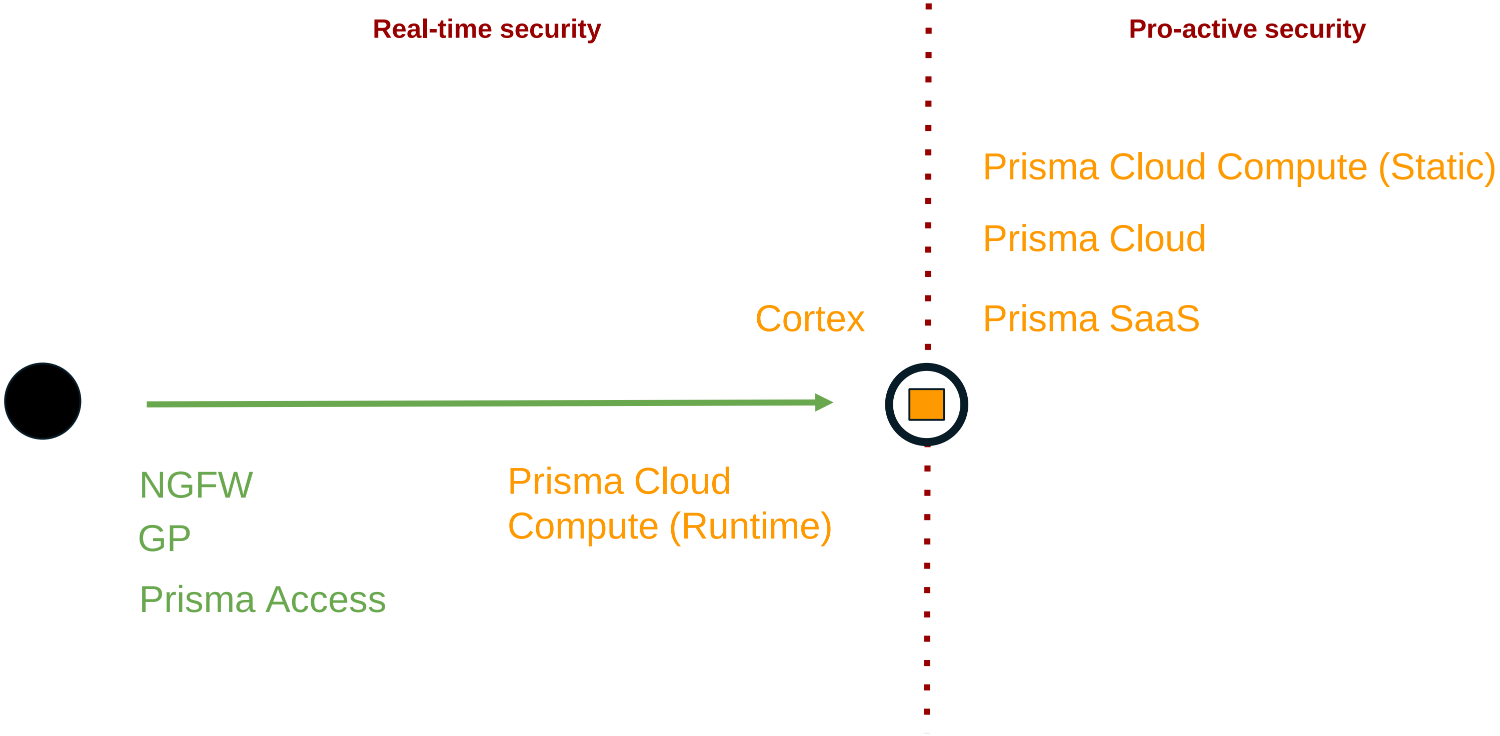
Calvin Mangubat

Learning objectives

At the end of this module, attendees will:

- Understand what Palo Alto Networks believes is the customer’s desired security outcome
- Understand what it takes to achieve this security outcome
- Be able to explain why are endpoints still being compromised
- Explain how we convert unknown threats to known threats
- Understand what the conversion of unknown-to-known means to the customer

Desired Security Outcomes



Real-time security

Pro-active security

Prisma Cloud Compute (Static)

Prisma Cloud

Prisma SaaS

Cortex

NGFW

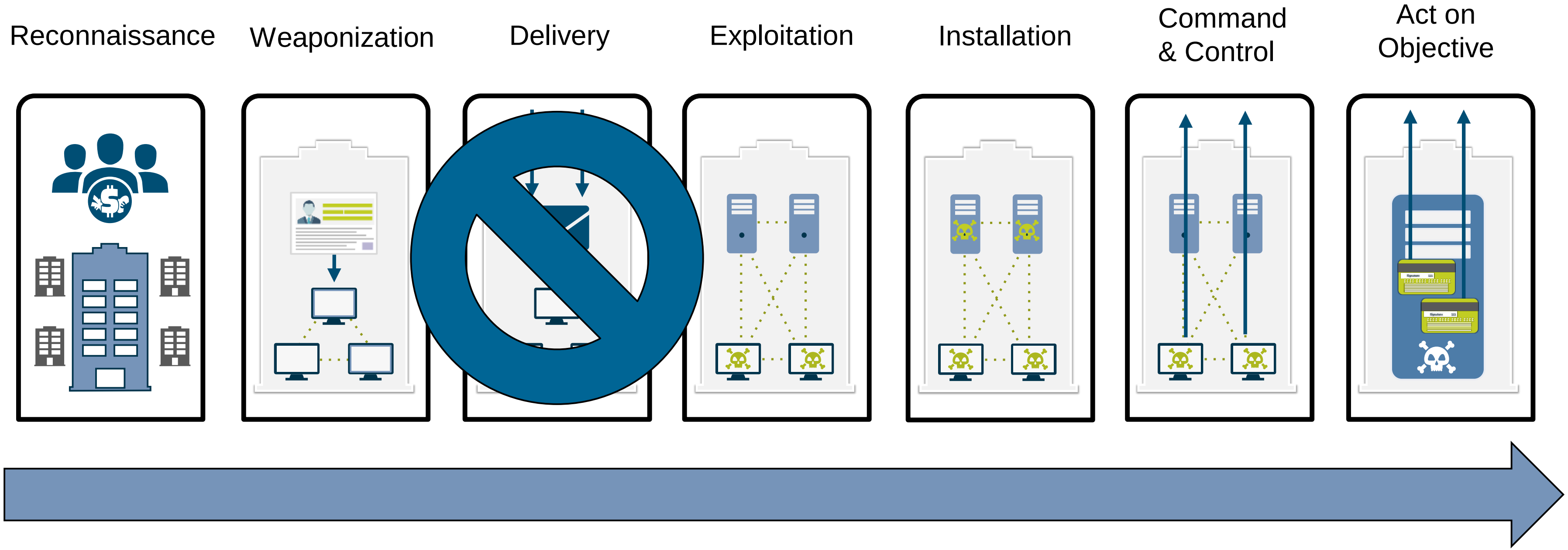
GP

Prisma Access

Prisma Cloud Compute (Runtime)

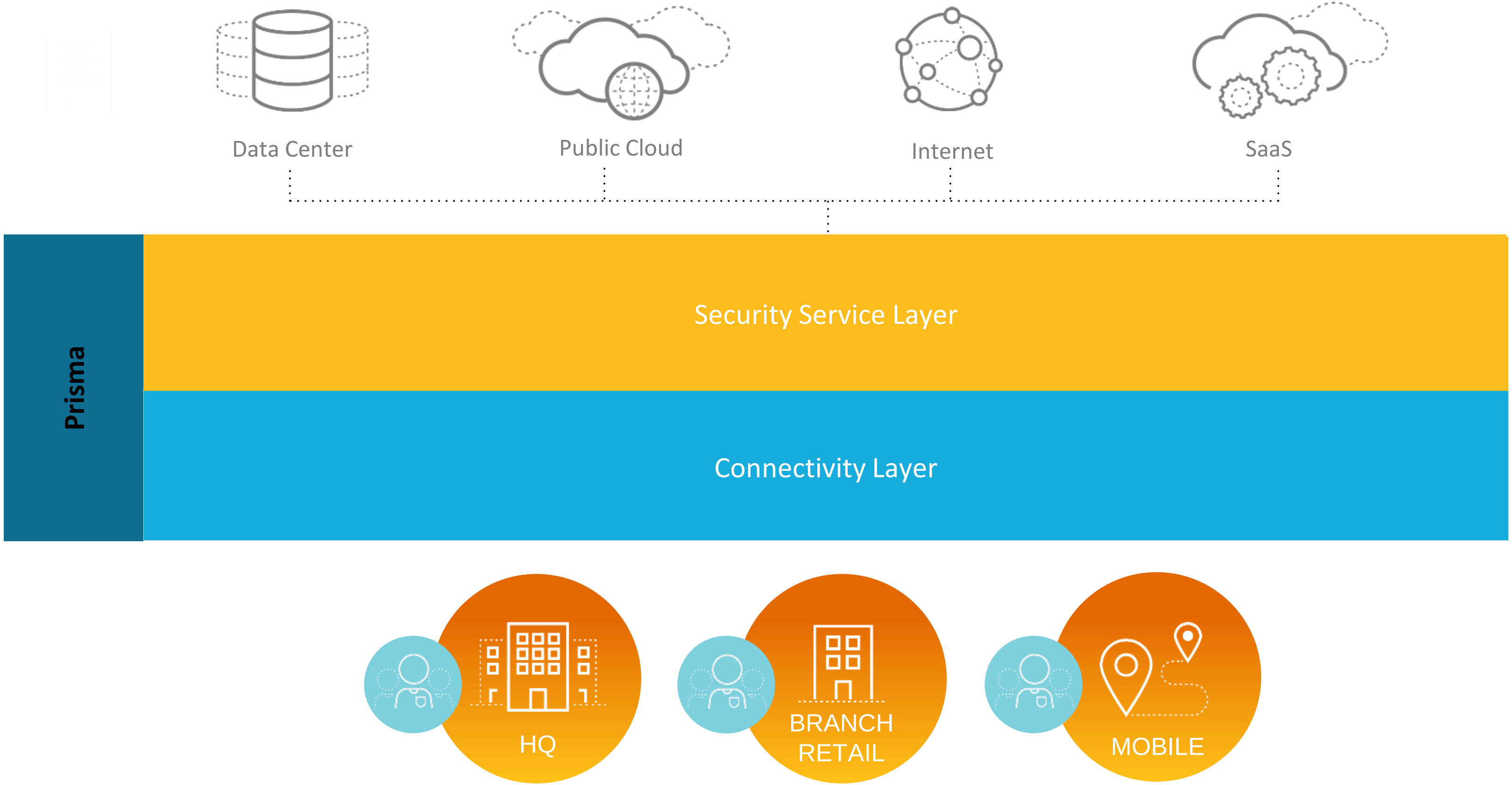
Desired Security Outcomes

Cyber Attack Lifecycle



Stop the attack at any point!

A NEW ARCHITECTURE FOR CLOUD SECURITY



Data Center

Public Cloud

Internet

SaaS

Prisma

Security Service Layer

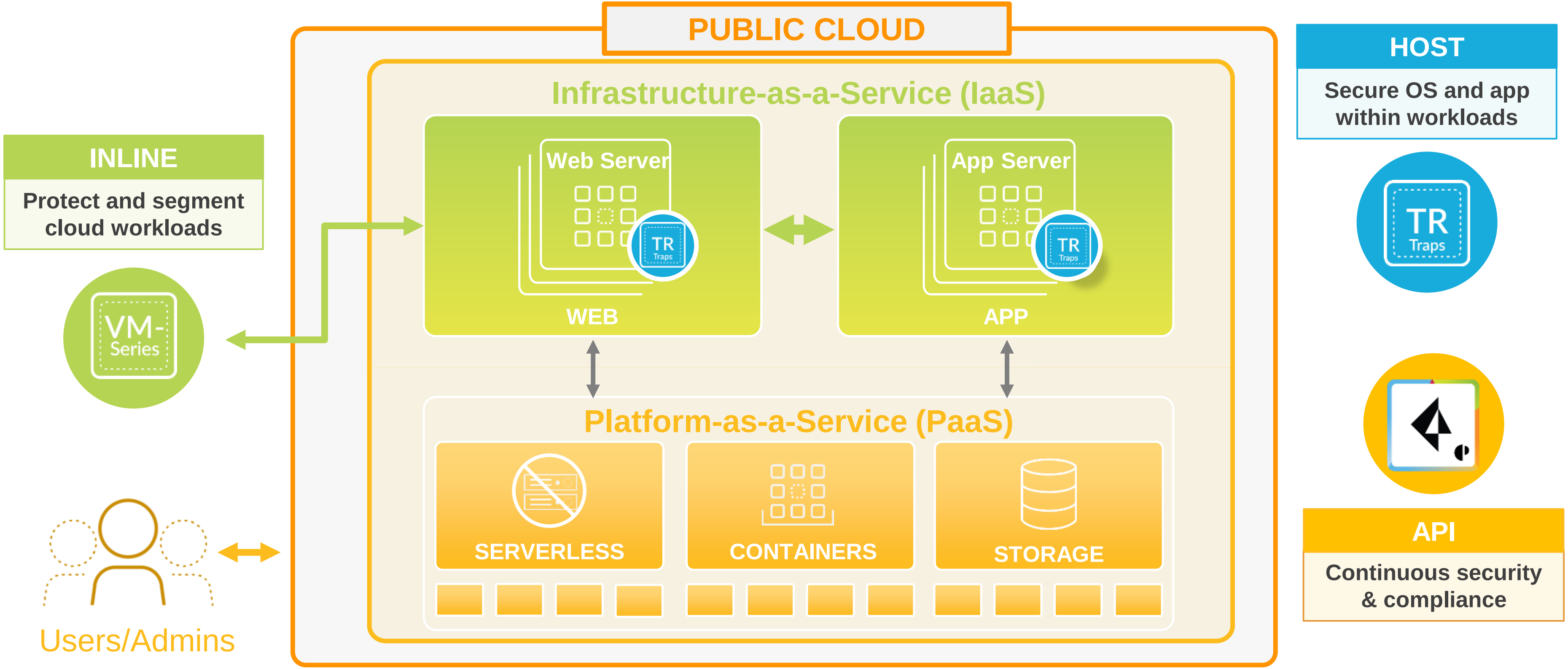
Connectivity Layer

HQ

BRANCH RETAIL

MOBILE

THE MOST COMPLETE PUBLIC CLOUD SECURITY OFFERING


PUBLIC CLOUD
Infrastructure-as-a-Service (IaaS)
Web Server
TR
Traps
WEB
App Server
TR
Traps
APP
Platform-as-a-Service (PaaS)
SERVERLESS
CONTAINERS
STORAGE
INLINE
Protect and segment cloud workloads
VM-Series
Users/Admins
HOST
Secure OS and app within workloads
TR
Traps
API
Continuous security & compliance

The Problems We Can Help You Solve

Visibility, Detection & Response

Data Security	AP DLP / Storage scanning
Hosts & Containers	TR Runtime security 🔒 Configuration monitoring (for cloud native) 🔒 Vulnerable image detection
Network Security	🔒 Network visibility and incident investigations 🔒 Suspicious/malicious traffic detection VM-Series Virtual firewall for in-line protection
Users & Credentials	🔒 Account & access key compromise detection 🔒 Anomalous insider activity detection 🔒 Privileged activity monitoring
Configurations / Control Plane	🔒 Compliance scanning (CIS, PCI, GDPR, etc.) 🔒 Storage, snapshots, & image configuration monitoring 🔒 VPC, security groups & firewall configuration monitoring 🔒 IAM configuration monitoring

Key Customer Pain Points in Public Cloud

Decentralized Administration & Lack of Visibility

- No CMDB, centralized asset inventory or network topology diagrams exist for public cloud
- Large number of privileged users with little governance

Impact

- Increased likelihood of undetected misconfigurations
- Inability to quantify risk to management and board

Complexity of Compliance Management in the Cloud

- Hundreds of unique cloud services, with more added daily
- Proving compliance to auditors challenging in dynamic environments

Impact

- Stalled or delayed digital transformation initiatives
- Increased costs in achieving compliance

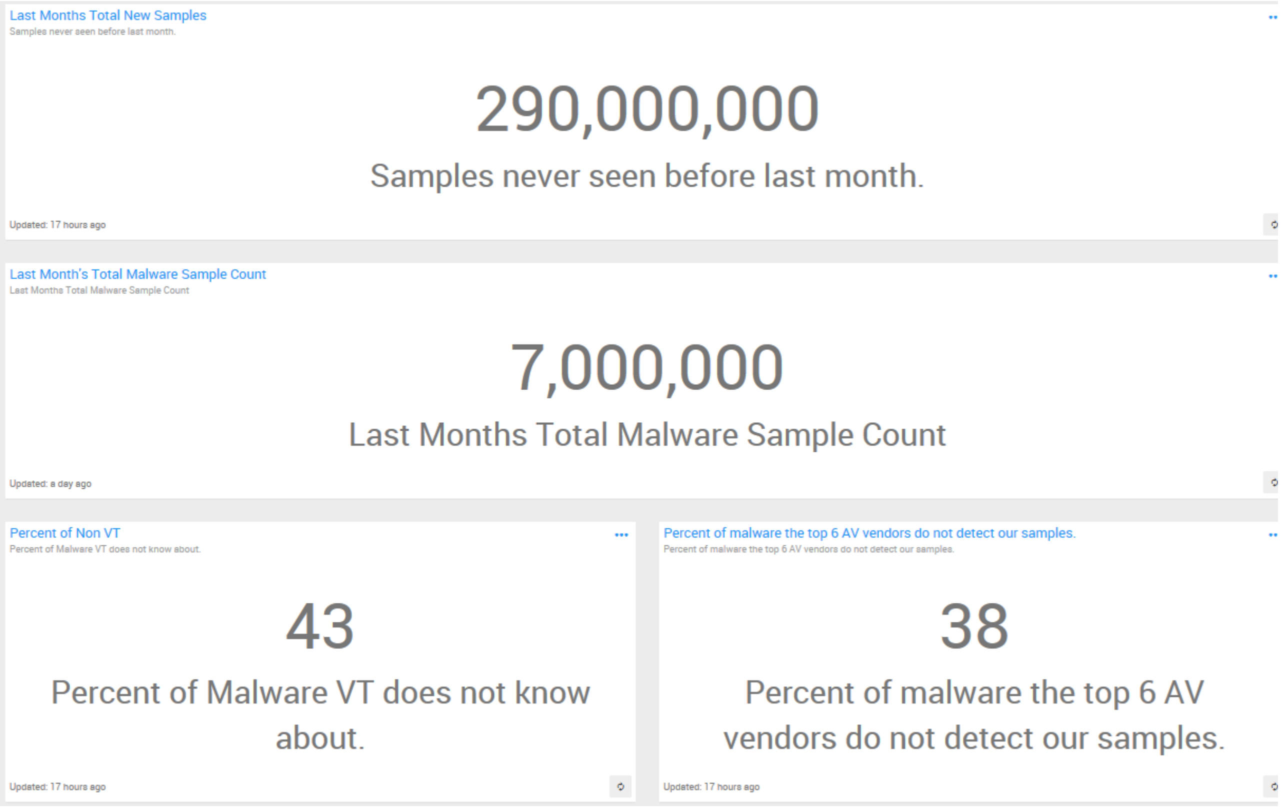
Inability to Rapidly Detect & Respond to Threats

- Traditional SIEMs do not have cloud context, and are unable to adapt to large data volumes and speed of change in public cloud

Impact

- Alert fatigue due to constant changes
- Extensive delays in investigating alerts with no context

Threat landscape



Last Months Total New Samples

Samples never seen before last month.

290,000,000

Samples never seen before last month.

Updated: 17 hours ago

Last Month's Total Malware Sample Count

Last Months Total Malware Sample Count

7,000,000

Last Months Total Malware Sample Count

Updated: a day ago

Percent of Non VT

Percent of Malware VT does not know about.

43

Percent of Malware VT does not know about.

Updated: 17 hours ago

Percent of malware the top 6 AV vendors do not detect our samples.

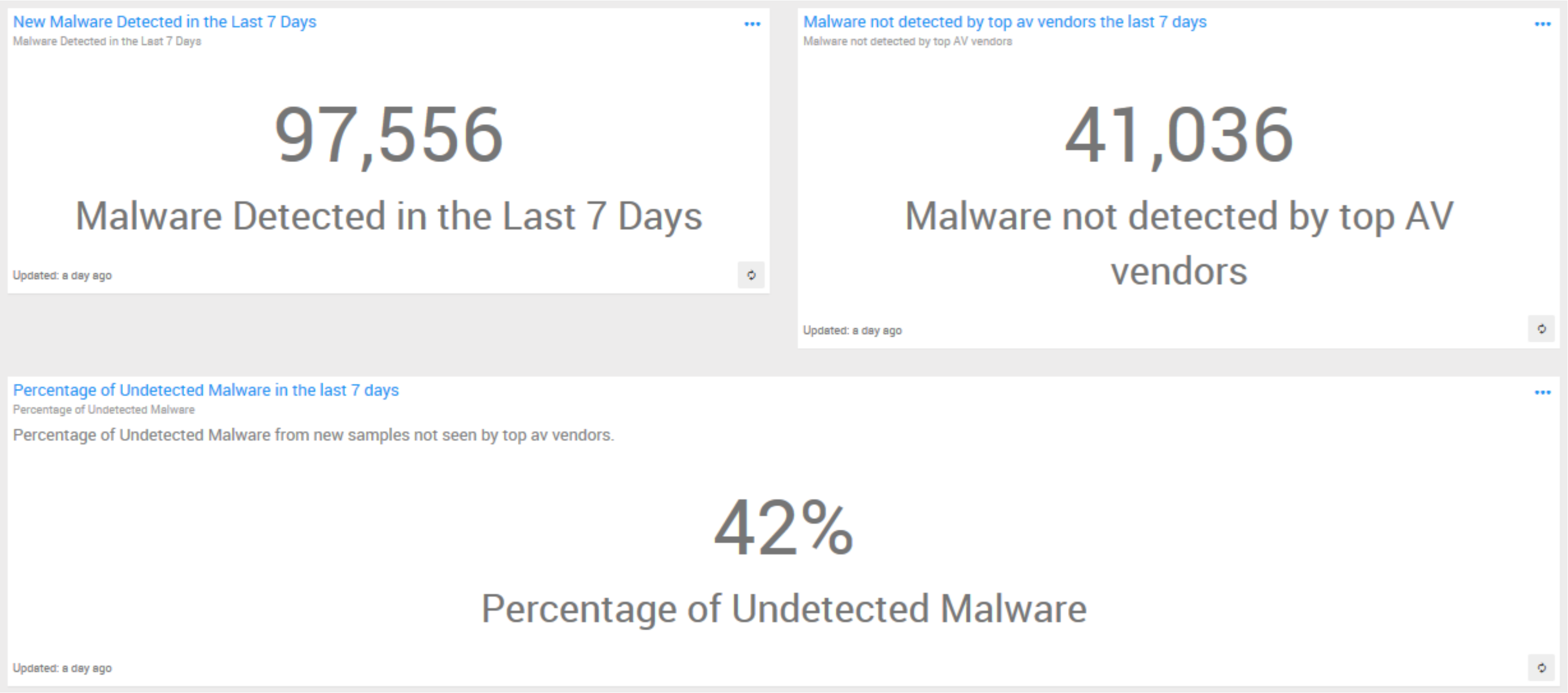
Percent of malware the top 6 AV vendors do not detect our samples.

38

Percent of malware the top 6 AV vendors do not detect our samples.

Updated: 17 hours ago

Threat landscape



New Malware Detected in the Last 7 Days

Malware Detected in the Last 7 Days

97,556

Malware Detected in the Last 7 Days

Updated: a day ago

Malware not detected by top av vendors the last 7 days

Malware not detected by top AV vendors

41,036

Malware not detected by top AV vendors

Updated: a day ago

Percentage of Undetected Malware in the last 7 days

Percentage of Undetected Malware

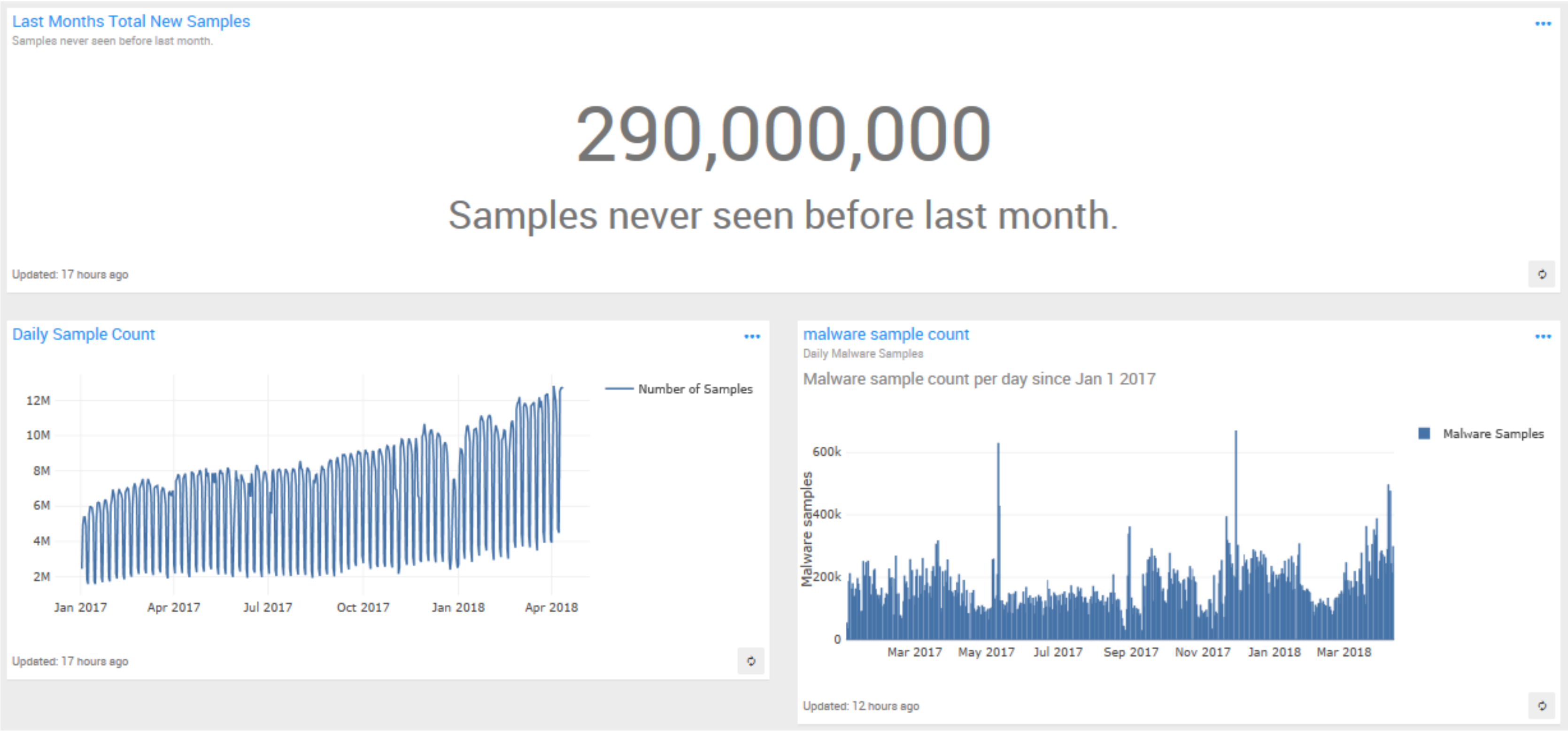
Percentage of Undetected Malware from new samples not seen by top av vendors.

42%

Percentage of Undetected Malware

Updated: a day ago

Threat landscape



Last Months Total New Samples

Samples never seen before last month.

290,000,000

Samples never seen before last month.

Updated: 17 hours ago

Daily Sample Count

Updated: 17 hours ago

malware sample count

Daily Malware Samples

Malware sample count per day since Jan 1 2017

Updated: 12 hours ago

THANK YOU

paloalto NETWORKS®