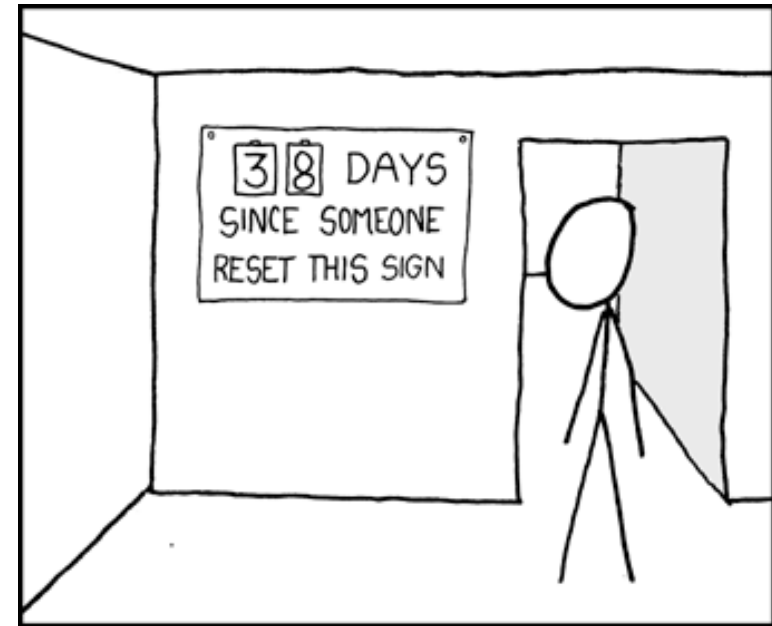


Security Metrics

for

The modern CISO

Counting on the truth



<https://xkcd.com/363/>

Metrics are the only way to
systematically improve security

Metrics hold accountable
people to account

Metrics show where to invest

Metrics extinguish politics

Metrics allow us to
demonstrate control

What's needed

Metrics require **truth**

Metrics require **automation**

Everybody is talking about metrics



The Board
Auditors
Regulators
Compliance
The Business
Technology
Customers
Ourselves

What do we need?

Point in time



Continuous

Manual



Automated

Untrusted



Baseline truth

Siloed



Business-relevant

Disparate data



Unified information

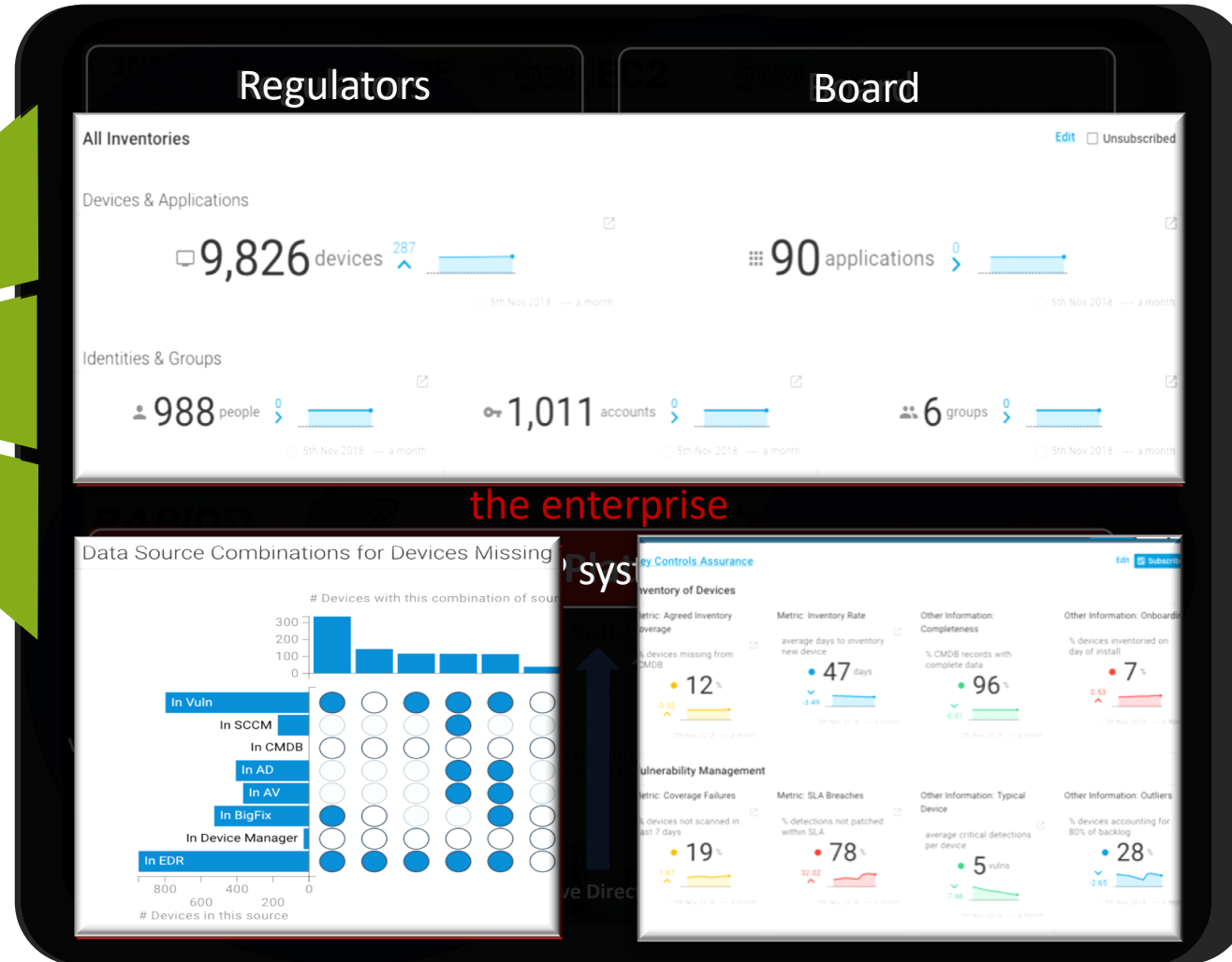
What assets are we defending?

Where are our controls deployed?

Are our controls performing within policy?

The truth is out there

Different perspectives on the same information



what do customers say?

The value delivered was:

- No more challenging of data by stakeholders
- Much more productive relationships versus toxic ones
- **Backlog of vulnerabilities reduced by 60% in 4 months**
- **Immediately identified 29% of assets not in CMDB**
- Higher quality of risk management information to board
- We can sweat the control assets we have to get much more value from the data available from them.

We needed strong data, not opinions

The ability to drill down into the data allowed us to quickly fix a device build in a particular business that was creating new detections by introducing old vulnerabilities onto the environment

Panaseer allowed us to see across 3 different IT estates with a single pane of glass for the first time

We were able to run a global campaign to track devices with end-of-life applications and measure progress across teams



Username
albert.plattner

Password
.....

[Forgot your password?](#)

Login



The Panaseer Platform.
Actionable insight, Enterprise-wide

→ 5th Nov 2018 No Filters

Key Controls Assurance

Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB



5th Nov 2018 a month

Metric: Inventory Rate

average days to inventory new device



5th Nov 2018 a month

Other Information: Completeness

% CMDB records with complete data



Vulnerability Management

Metric: Coverage Failures

% devices not scanned in last 7 days



5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA



5th Nov 2018 a month

Other Information: Typical Device

average critical detections per device



Malware Defences

AV: Coverage Failures

% endpoints not installed

AV: SLA Breaches

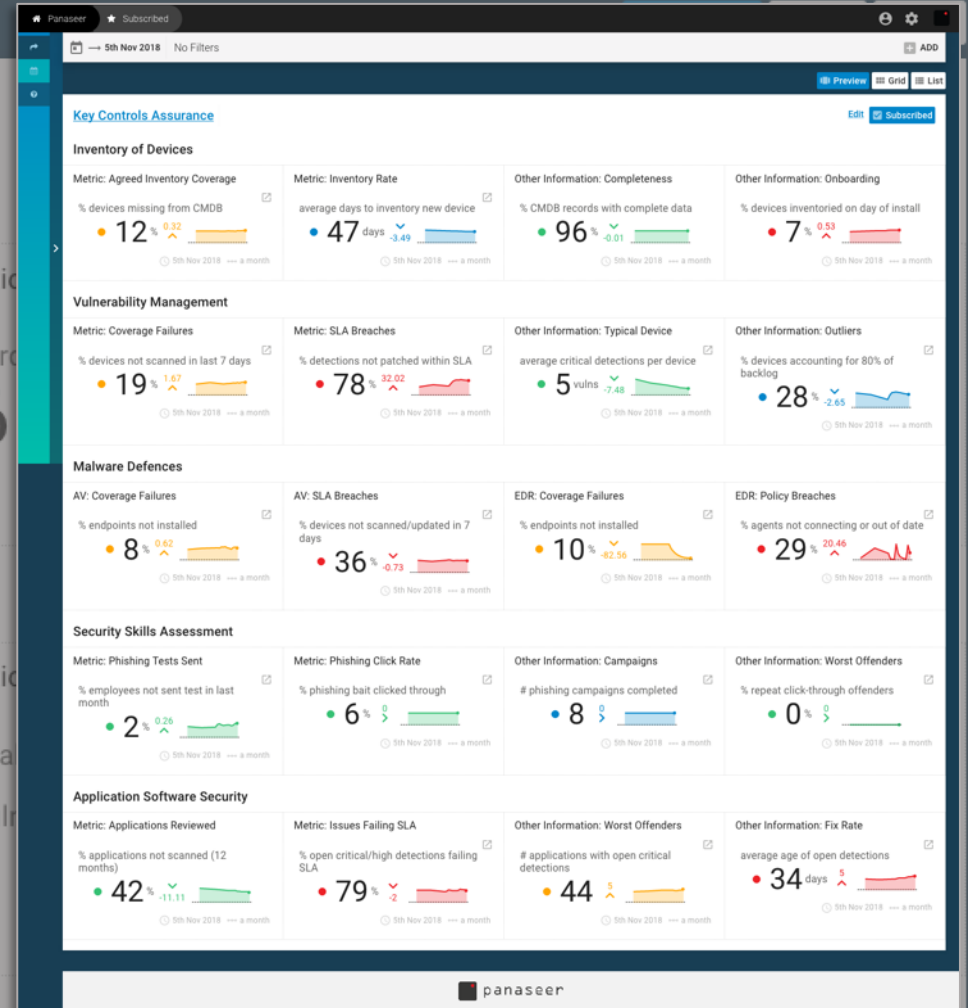
% devices not scanned/updated in 7

EDR: Coverage Failures

% endpoints not installed

EDR: Policy Breaches

% agents not connecting or out of date





Data Connector Catalogue

The Data Connector Catalogue shows our collection of data source system integrations.

Browse your organisation's active and available Data Connectors or talk to us about your specific data needs.

More filters

[Request Data Connector support](#)



Application Scanner

VERACODE

Application Security

Veracode

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Activate](#)

Available

CONTRAST SECURITY

Contrast Security

Contrast

Last Active: **Never**

Registered: 5 months ago

[Details](#)

SailPoint

Identity IQ

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Network Traffic Logs

5 months

Available

Proxy

Palisade

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Patch Manager

BIGFIX

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

BigFix

IBM

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Phishing Test Services

FreshLine

Installed

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Email Protection

PhishLine

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

Threat Intelligence

NVD

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

National Vulnerability Database

NIST

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Vendor Security Rating

BITSIGHT

Available

Security Ratings

Bitsight

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Vulnerability Scanner

RAPID7

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Nexpose

Parasit

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

ServiceNow

Configuration Management Database

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Cloud Instance Manager

Elastic Compute Cloud

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

Endpoint Configuration Management

jamf

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Device Management

System Center Configuration Manager

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

Systems Manager

Microsoft

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

Endpoint Security

SOPHOS

Available

Endpoint Protection

Symantec

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

Falcon

CrowdStrike

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Event Logs

ASA

Available

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

CloudWatch

Amazon Web Services

Available

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Other name

[Details](#) [Data Profile](#) [Configure](#)

Command Log

UNIX

Available

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Event Log

Windows

Available

Last Active: **Never**

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Short

Other

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

SailPoint

Identity IQ

Installed

Last Active: 5 months ago

Registered: 5 months ago

[Details](#) [Data Profile](#) [Configure](#)

Security Insights Dashboards

- ★ Subscribed
- 🕒 Recent
- 👤 Shared With You
- 📁 NIST Controls Assurance
- 📁 All Dashboards

+ All

Inventories

Search for any entity

Search

- 📁 All Inventories

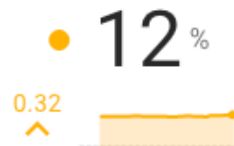
→ 5th Nov 2018 No Filters

Key Controls Assurance

Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB



5th Nov 2018 a month

Metric: Inventory Rate

average days to inventory new device

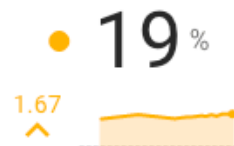


5th Nov 2018 a month

Vulnerability Management

Metric: Coverage Failures

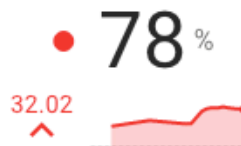
% devices not scanned in last 7 days



5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA



5th Nov 2018 a month

Key Controls Assurance

Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB



5th Nov 2018 a month

Metric: Inventory Rate

average days to inventory new device



5th Nov 2018 a month

Other Information: Completeness

% CMDB records with complete data



5th Nov 2018 a month

Other Information: Onboarding

% devices inventoried on day of install



5th Nov 2018 a month

Vulnerability Management

Metric: Coverage Failures

% devices not scanned in last 7 days



5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA



5th Nov 2018 a month

Other Information: Typical Device

average critical detections per device



5th Nov 2018 a month

Other Information: Outliers

% devices accounting for 80% of backlog



5th Nov 2018 a month

Malware Defences

AV: Coverage Failures

% endpoints not installed



5th Nov 2018 a month

AV: SLA Breaches

% devices not scanned/updated in 7 days



5th Nov 2018 a month

EDR: Coverage Failures

% endpoints not installed



5th Nov 2018 a month

EDR: Policy Breaches

% agents not connecting or out of date



5th Nov 2018 a month

Security Skills Assessment

Metric: Phishing Tests Sent

% employees not sent test in last month



5th Nov 2018 a month

Metric: Phishing Click Rate

% phishing bait clicked through



5th Nov 2018 a month

Other Information: Campaigns

phishing campaigns completed



5th Nov 2018 a month

Other Information: Worst Offenders

% repeat click-through offenders



5th Nov 2018 a month

Application Software Security

Metric: Applications Reviewed

% applications not scanned (12 months)



5th Nov 2018 a month

Metric: Issues Failing SLA

% open critical/high detections failing SLA



5th Nov 2018 a month

Other Information: Worst Offenders

applications with open critical detections



5th Nov 2018 a month

Other Information: Fix Rate

average age of open detections



5th Nov 2018 a month

📅 → 5th Nov 2018 No Filters

+ ADD

Inventories Overview Available

All Inventories

[Edit](#) ☐ Unsubscribed

Devices & Applications

🖥️ 9,826 devices ²⁸⁷ ⬆️



🕒 5th Nov 2018 ↔ a month

📱 90 applications ⁰ ⬆️



🕒 5th Nov 2018 ↔ a month

Identities & Groups

👤 988 people ⁰ ⬆️



🕒 5th Nov 2018 ↔ a month

🔑 1,011 accounts ⁰ ⬆️




🕒 5th Nov 2018 ↔ a month

👥 6 groups ⁰ ⬆️



🕒 5th Nov 2018 ↔ a month

 → 5th Nov 2018 No Filters ADD Inventories

Overview


Available

All Inventories

[Edit](#) ☐ Unsubscribed

Devices & Applicati

Timestamp 2018-11-05 02:00

 **9** devices

9,826

source records **52,390**

 **90** applications

Identities & Groups

 **988** people **1,011** accounts **6** groups

5th Nov 2018

No Filters

Devices

Overview

Available

Device Inventory

Overview of Devices

Devices in Panaseer Smart Inventory

		Americas			AsiaPac			UK		
Investment Management	Network	392	▼ -6		153	▲ 4		197	▲ 1	
	Server	1,364	▲ 45		792	▲ 61		953	▲ 72	
	User Device	773	▶ 0		377	▲ 8		475	▼ 1	
Wealth Management	Network	293	▼ -11		108	▲ 4		198	▼ 4	
	Server	941	▲ 26		546	▲ 33		956	▲ 55	
	User Device	561	▲ 2		265	▲ 2		482	▼ 6	

Device Inventory

Edit Unsubscribed

Overview of Devices

Devices in Panaseer Smart Inventory

		Americas			AsiaPac			UK		
Investment Management	Network	392	▼ -6		153	▲ 4		197	▲ 1	
	Server	1,364	▲ 45		792	▲ 61		953	▲ 72	
	User Device	773	▶ 0		377	▲ 8		475	▼ 1	
Wealth Management	Network	293	▼ -11		108	▲ 4		198	▼ 4	
	Server	941	▲ 26		546	▲ 33		956	▲ 55	
	User Device	561	▲ 2		265	▲ 2		482	▼ 6	

5th Nov 2018 → a month

Device List

Entity ID	Host	IP Address	Device Type	Device Subtype	Region	Country	City	Business Unit	OS Type	Last Connection
View 004814	sin-29220.asiapac.mycompany.com	10.0.76.96	Server	Web application	AsiaPac	Singapore	Singapore	Investment Management	Linux	2018-11-04 23:59
View 000319	box-10793.americas.mycompany.com	10.0.4.29	Server	Web application	Americas	US	Boston	Wealth Management	Linux	2018-11-04 23:59
View 001558	can-15464.asiapac.mycompany.com	10.0.22.110	Server	Web application	AsiaPac	Australia	Canberra	Investment Management	Linux	2018-11-04 23:58
View 002748	lde-20059.uk.mycompany.com	10.0.40.115	Server	Web application	UK	UK	Leeds	Investment Management	Linux	2018-11-04 23:58
View 00275E	lde-20078.uk.mycompany.com	10.0.40.134	Server	Web application	UK	UK	Leeds	Wealth Management	Linux	2018-11-04 23:58
View 00274C	lde-20060.uk.mycompany.com	10.0.40.116	Server	Web application	UK	UK	Leeds	Wealth Management	Linux	2018-11-04 23:58
View 00480E	sin-29214.asiapac.mycompany.com	10.0.76.90	Server	Web application	AsiaPac	Singapore	Singapore	Wealth Management	Linux	2018-11-04 23:58
View 00263A	lde-19786.uk.mycompany.com	10.0.39.97	Server	Web application	UK	UK	Leeds	Wealth Management	Linux	2018-11-04 23:58
View 000326	box-10806.americas.mycompany.com	10.0.4.42	Server	Web application	Americas	US	Boston	Investment Management	Linux	2018-11-04 23:57
View 0049CC	sin-28892.asiapac.mycompany.com	10.0.75.23	Server	Web application	AsiaPac	Singapore	Singapore	Wealth Management	Linux	2018-11-04 23:56

Previous 1/983 Next

5th Nov 2018

Wealth Management

Server

941 ²⁶ 546 ³³ 956 ⁵⁵ 

User Device

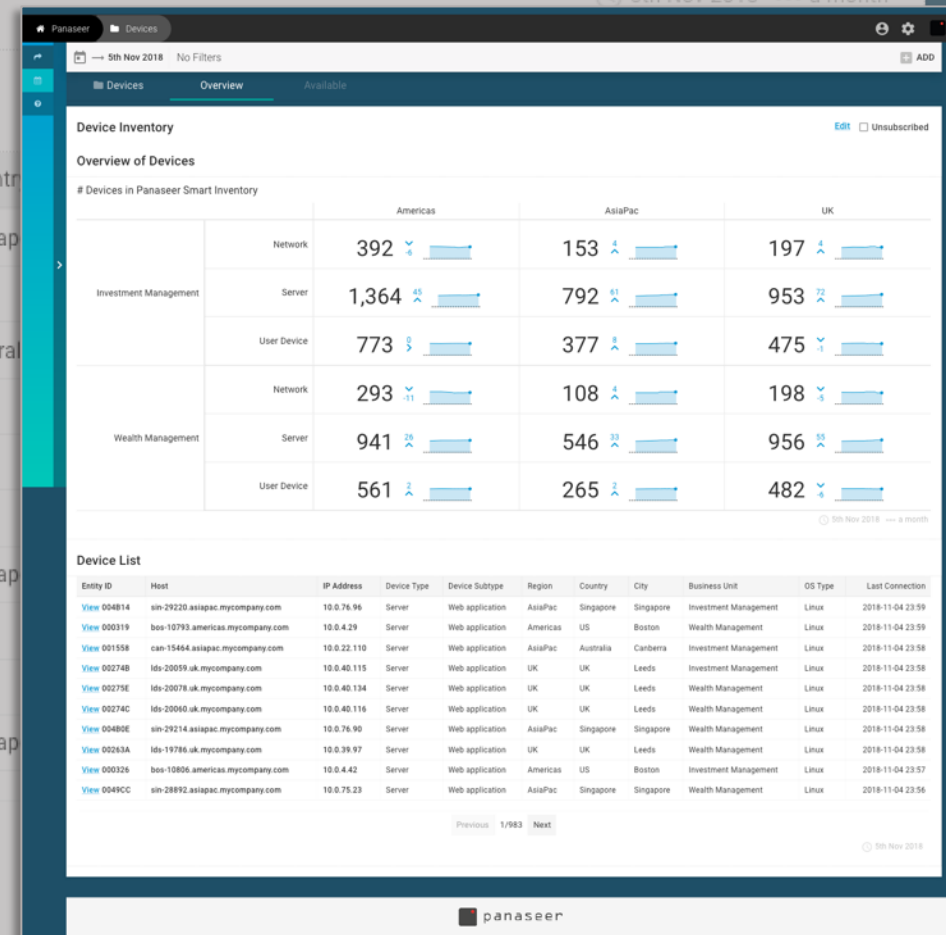
561 ² 265 ² 482 ⁻⁶ 

5th Nov 2018 → a month

Device List

Entity ID	Host	IP Address	Device Type	Device Subtype	Region	Country
View 004B14	sin-29220.asiapac.mycompany.com	10.0.76.96	Server	Web application	AsiaPac	Singap
View 000319	bos-10793.americas.mycompany.com	10.0.4.29	Server	Web application	Americas	US
View 001558	can-15464.asiapac.mycompany.com	10.0.22.110	Server	Web application	AsiaPac	Austral
View 00274B	lds-20059.uk.mycompany.com	10.0.40.115	Server	Web application	UK	UK
View 00275E	lds-20078.uk.mycompany.com	10.0.40.134	Server	Web application	UK	UK
View 00274C	lds-20060.uk.mycompany.com	10.0.40.116	Server	Web application	UK	UK
View 004B0E	sin-29214.asiapac.mycompany.com	10.0.76.90	Server	Web application	AsiaPac	Singap
View 00263A	lds-19786.uk.mycompany.com	10.0.39.97	Server	Web application	UK	UK
View 000326	bos-10806.americas.mycompany.com	10.0.4.42	Server	Web application	Americas	US
View 0049CC	sin-28892.asiapac.mycompany.com	10.0.75.23	Server	Web application	AsiaPac	Singap

Previous 1/983 Next



[< Back to "Devices" Folder](#)**FTW-18899**

Serial Number List: ASST28899U

 Edit**Device Identifiers**

Serial Number List	ASST28899U
Host List	FTW-18899
DNS List	ftw-18899.americas.mycompany.com
MAC Address List	ab:cd:ef:63:bc:64
IP Address List	10.0.35.230
Netbios List	FTW-18899




Device Context

Device Type	User Device
Device Subtype	Laptop
OS	Windows 7 Enterprise Edition

Network Context

Environment Type	Production
Network Location	Internal
Domain	AMERICAS.MYCOMPANY.COM
Distinguished Name	CN=FTW-18899,OU=Investment Management,DC=Americas,DC=MyCompany,DC=

Business Context

Criticality	Moderate
Region	Americas
Country	US
Business Unit	Investment Management
Division	-
Functional Role	Unknown
Owner	 Fidela Fridaye
Manager	 Frazer Leadbeatter
Assignee	 Fidela Fridaye

Data Source Coverage

Active Directory	2018-10-31 17:30
McAfee Foundstone	2018-10-31 03:51
SCCM	2018-11-03 06:55
ServiceNow	2018-11-03 06:55
Symantec	2018-11-04 23:52

 5th Nov 2018**Vulnerabilities**

Number of Detections

3

-5

 5th Nov 2018 --- a month**Hosted Applications**

Number of Hosted Applications

0

Applications

 5th Nov 2018**Endpoint Protection**

Last AV Scan	2018-10-21 17:01
Last AV Update	2018-11-04 06:48

 5th Nov 2018

[< Back to "Devices" Folder](#)**Fidela Fridaye**

Functional Title: Developer III

Edit

Person Identifiers

Employee ID	351
Display Name	Fidela Fridaye
First Name	Fidela
Last Name	Fridaye
Email	fidela.fridaye@mycompany.com

Person Context

Job Title	Developer III
Employment Type	Contractor
Employment Start Date	2018-09-07 01:28
Employment End Date	-

Business Context

Functional Title	Developer III
Manager (Line Manager)	Ellswerth Ablott
Manager (Department Head)	Lyndsie Klimsch
Business Unit	Investment Management
Department	Product
Division	Product
Region	Americas
Country	US

Owned and Managed Devices

Owned Devices	22
Assigned Devices	22

5th Nov 2018

Owned and Managed Applications**Owned Accounts**

Owned Accounts	1
----------------	---

- Security Insights Dashboards
- ★ Subscribed
 - 🕒 Recent
 - 📁 Shared With You
 - 📁 NIST Controls Assurance
 - 📁 All Dashboards
 - 📊 Business Overview
 - 📊 Business Unit Vulnerabilities
 - 📊 Cross-Source Coverage
 - 📊 Key Controls Assurance
 - 📊 Vulnerability Key Insights and Actions

Inventories

Search

> 📁 All Inventories

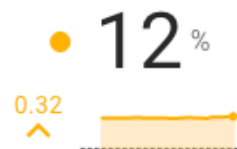
📅 → 5th Nov 2018 No Filters

Key Controls Assurance

Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB



🕒 5th Nov 2018 → a month

Metric: Inventory Rate

average days to inventory new device



🕒 5th Nov 2018 → a month

Vulnerability Management

Metric: Coverage Failures

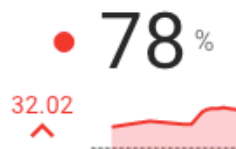
% devices not scanned in last 7 days



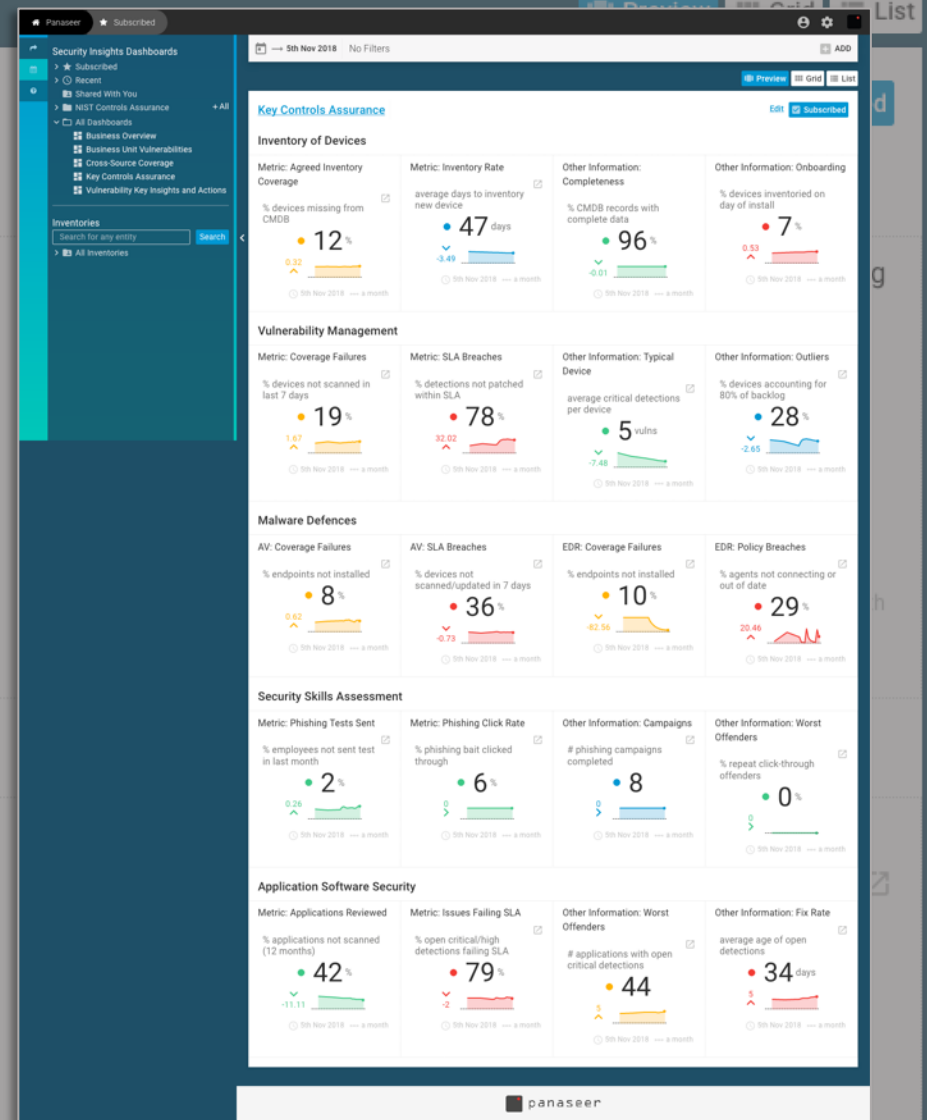
🕒 5th Nov 2018 → a month

Metric: SLA Breaches

% detections not patched within SLA



🕒 5th Nov 2018 → a month



📅 → 5th Nov 2018 No Filters

+ ADD

Cross-Source Coverage

[Edit](#) ☐ Unsubscribed

Proportion of Devices Missing from Sources

% Devices missing from source

● < 10% devices missing from source ● Between 10% and 20% devices missing from source ● > 20% devices missing from source

CMDB

● 12

0.29



AV

● 9

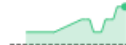
0.39



AD

● 0

0.19



Vuln

● 19

1.69



SCCM

● 14

0.2



BigFix

● 20

1.6



Device Manager

● 97

0.3



EDR

● 10

-82.5



🕒 5th Nov 2018 ↔ a month

5th Nov 2018

Expected in CMDB + true X

In CMDB + false X

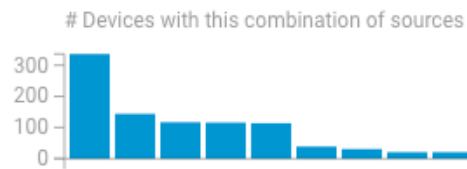
Source Coverage Detail

Regional Coverage Breakdown

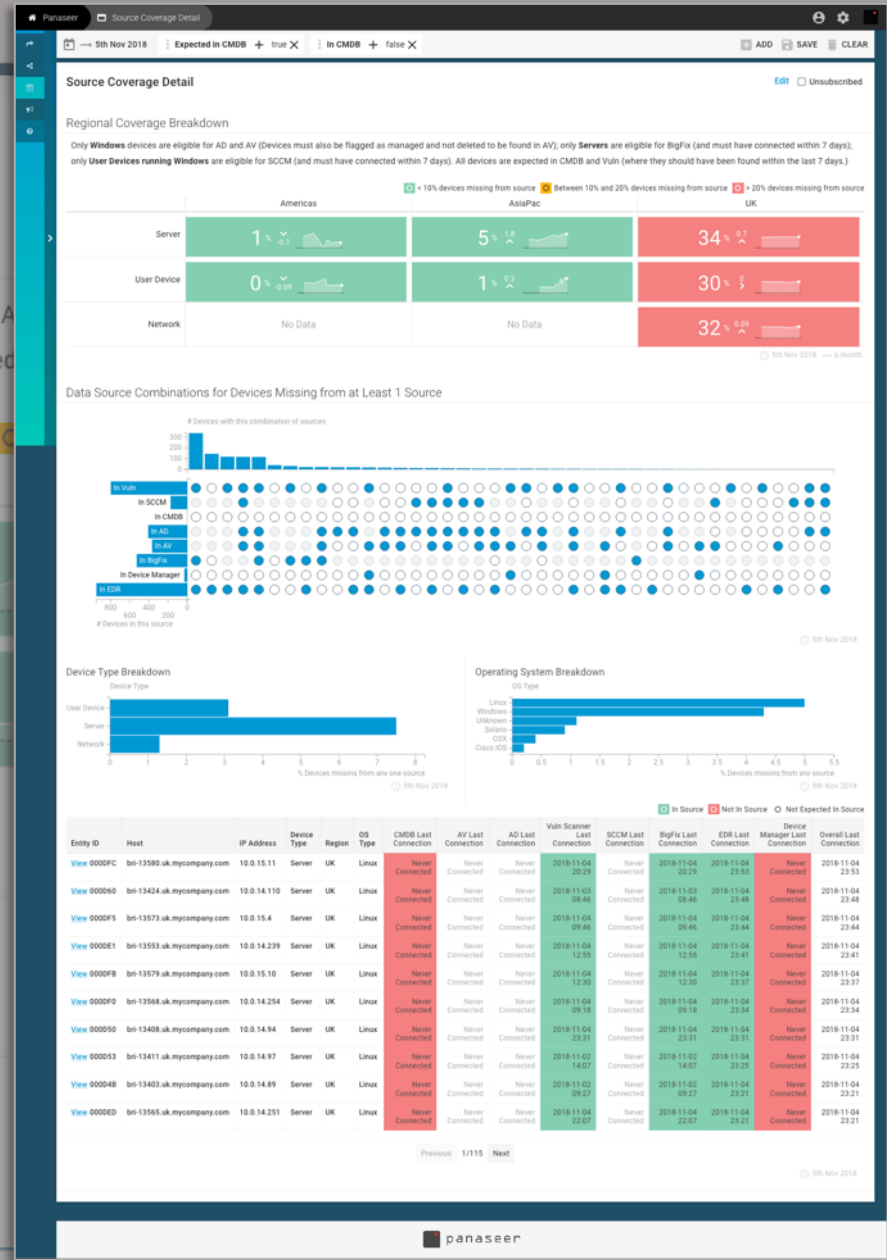
Only **Windows** devices are eligible for AD and AV (Devices must also be flagged as managed and not deleted to be found in AV); only **Servers** are eligible for BigFix (and must have connected within 7 days); only **User Devices running Windows** are eligible for SCCM (and must have connected within 7 days). All devices are expected



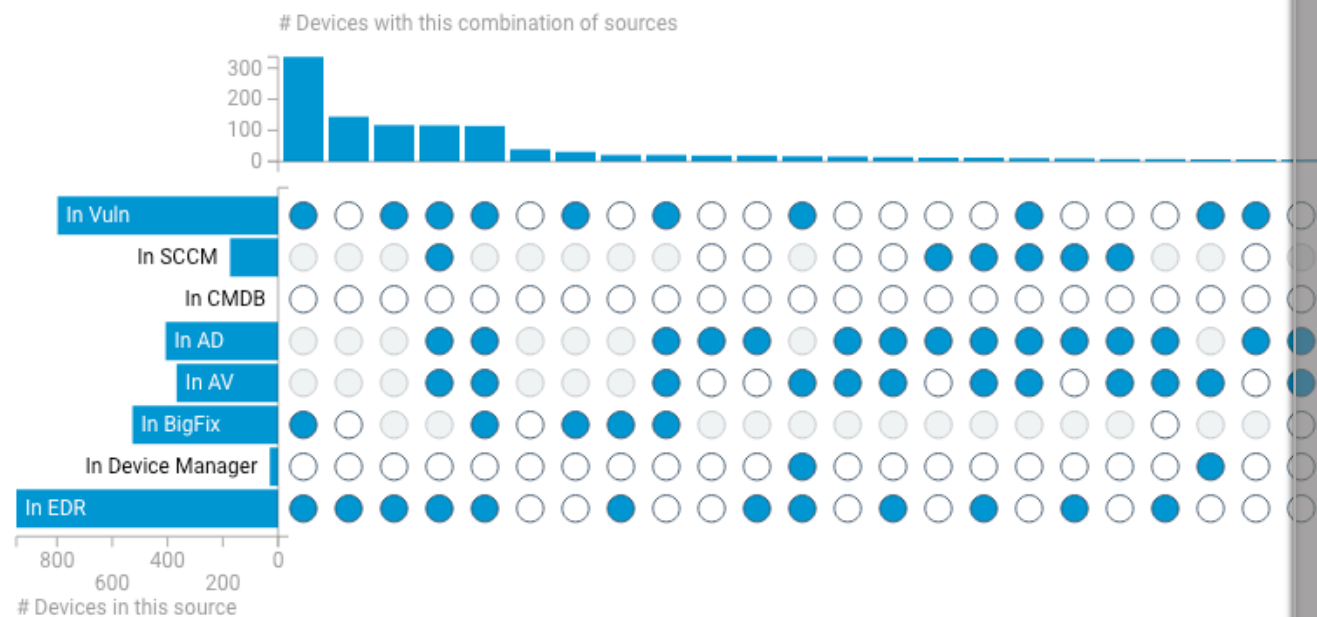
Data Source Combinations for Devices Missing from at Least 1 Source



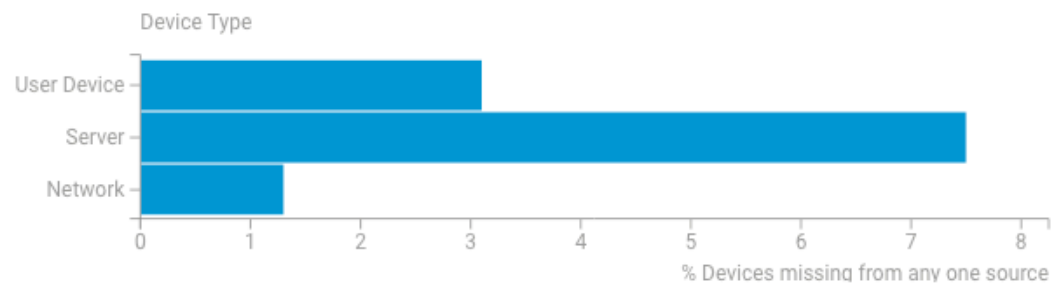
In Vuln



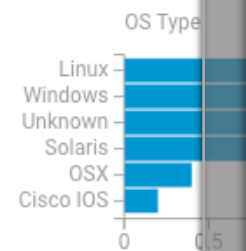
Data Source Combinations for Devices Missing from at Least 1 Source



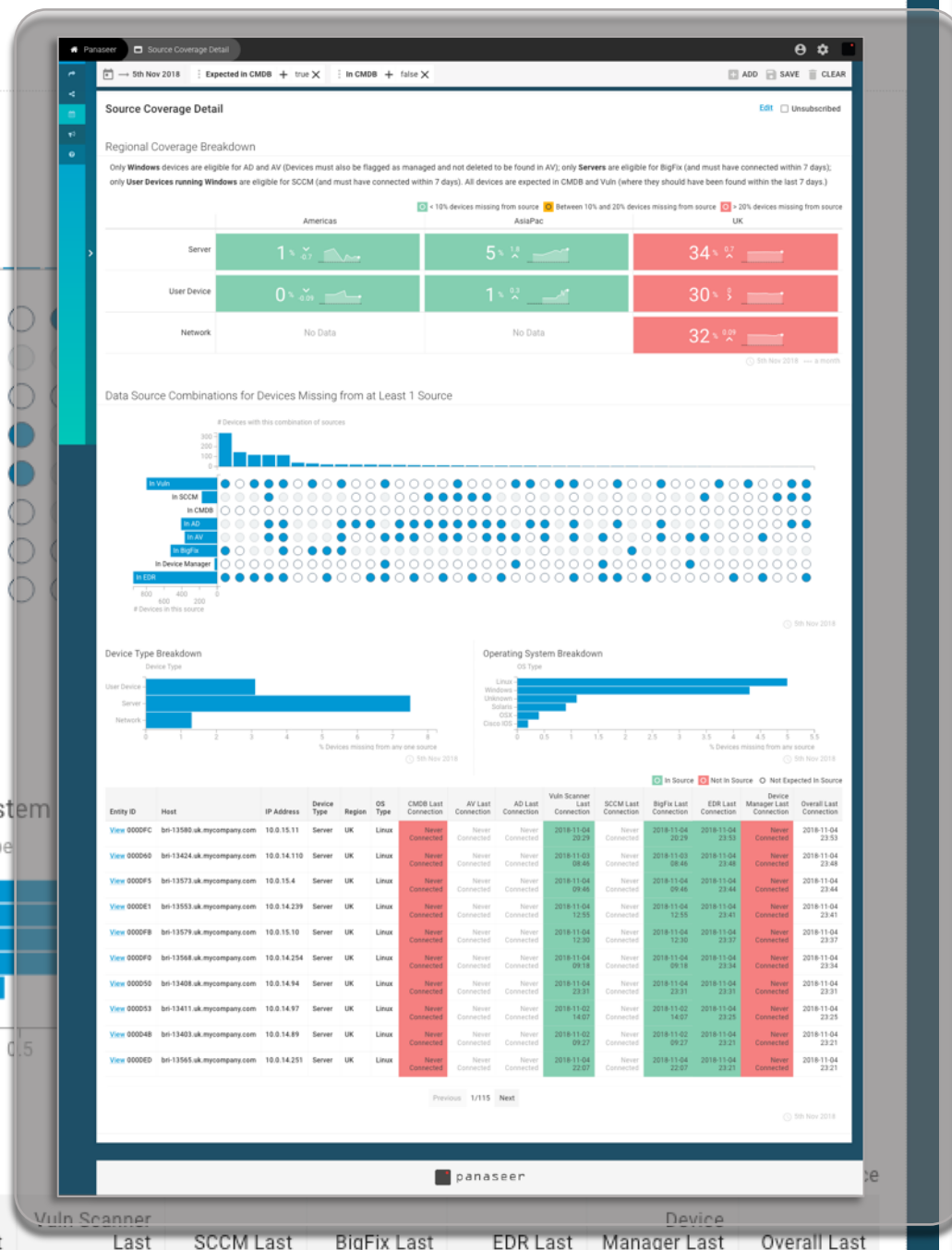
Device Type Breakdown



Operating System

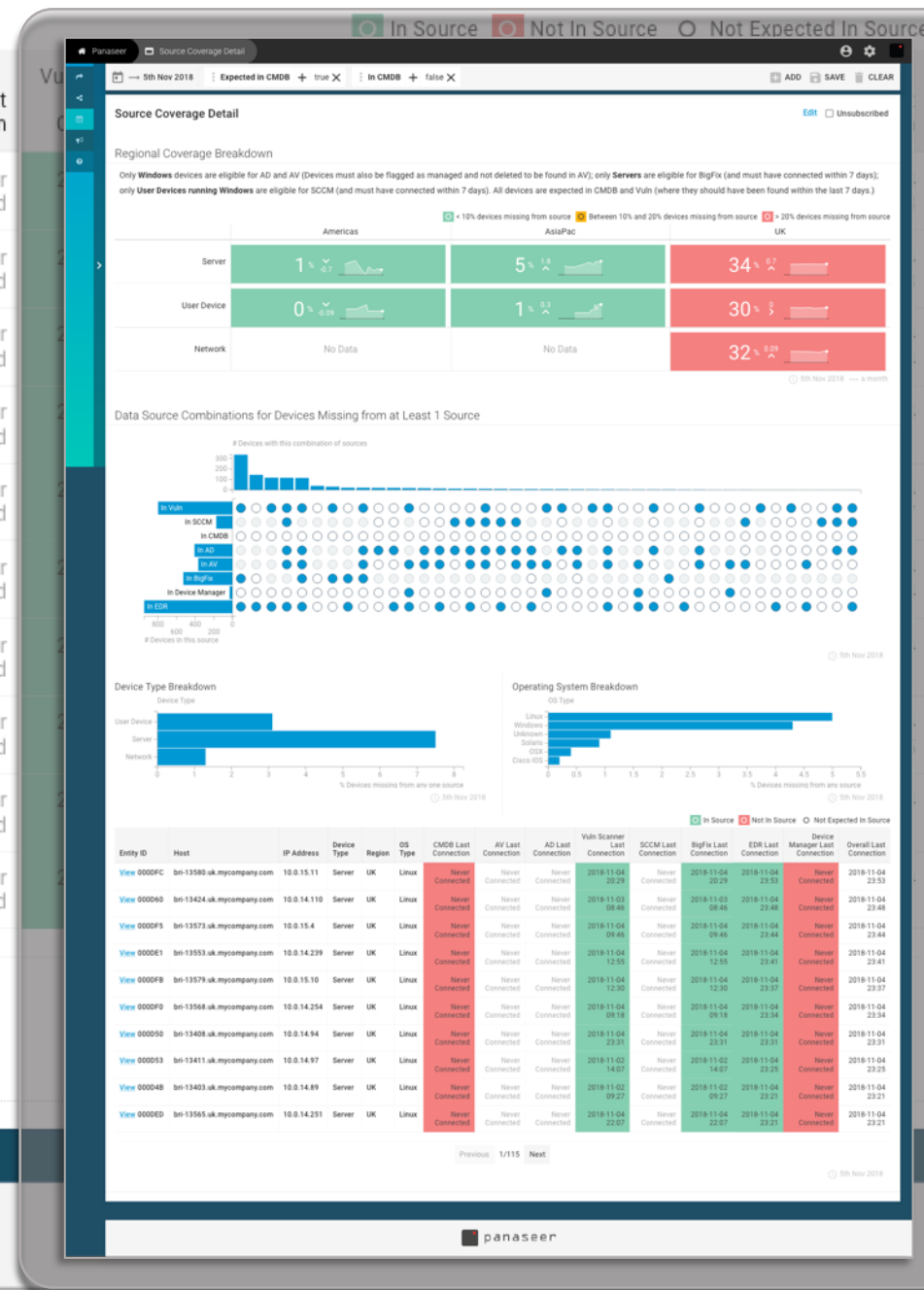


5th Nov 2018

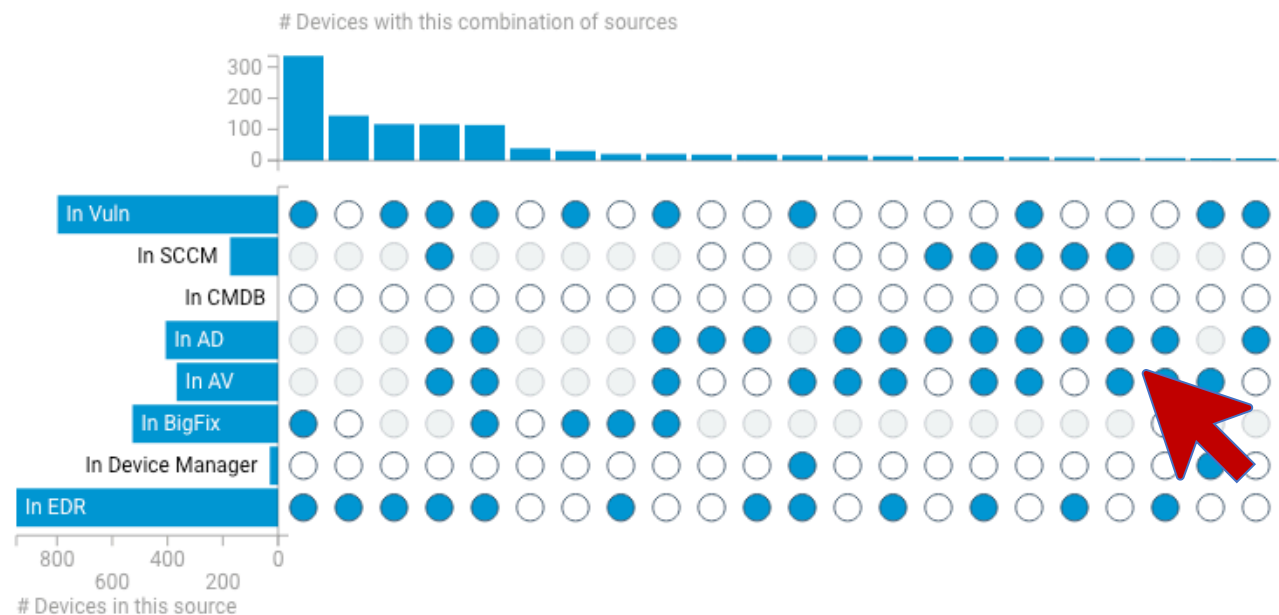


Entity ID	Host	IP Address	Device Type	Region	OS Type	CMDB Last Connection	AV Last Connection	AD Last Connection
View 000DFC	bri-13580.uk.mycompany.com	10.0.15.11	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000D60	bri-13424.uk.mycompany.com	10.0.14.110	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000DF5	bri-13573.uk.mycompany.com	10.0.15.4	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000DE1	bri-13553.uk.mycompany.com	10.0.14.239	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000DFB	bri-13579.uk.mycompany.com	10.0.15.10	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000DF0	bri-13568.uk.mycompany.com	10.0.14.254	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000D50	bri-13408.uk.mycompany.com	10.0.14.94	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000D53	bri-13411.uk.mycompany.com	10.0.14.97	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000D4B	bri-13403.uk.mycompany.com	10.0.14.89	Server	UK	Linux	Never Connected	Never Connected	Never Connected
View 000DED	bri-13565.uk.mycompany.com	10.0.14.251	Server	UK	Linux	Never Connected	Never Connected	Never Connected

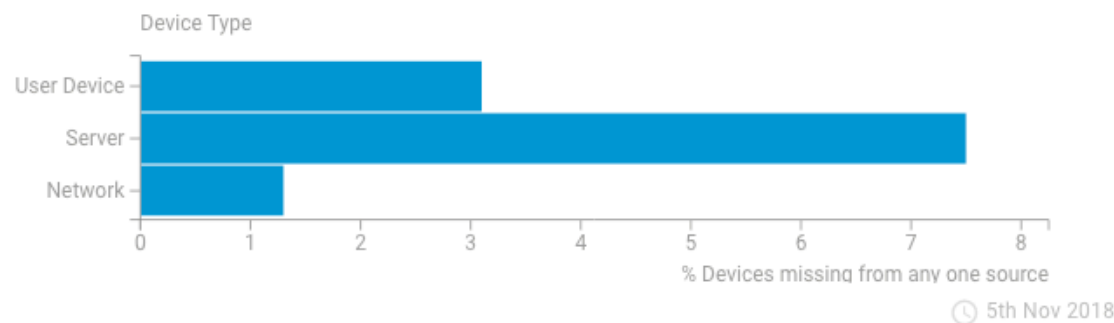
Previous 1/115 Next



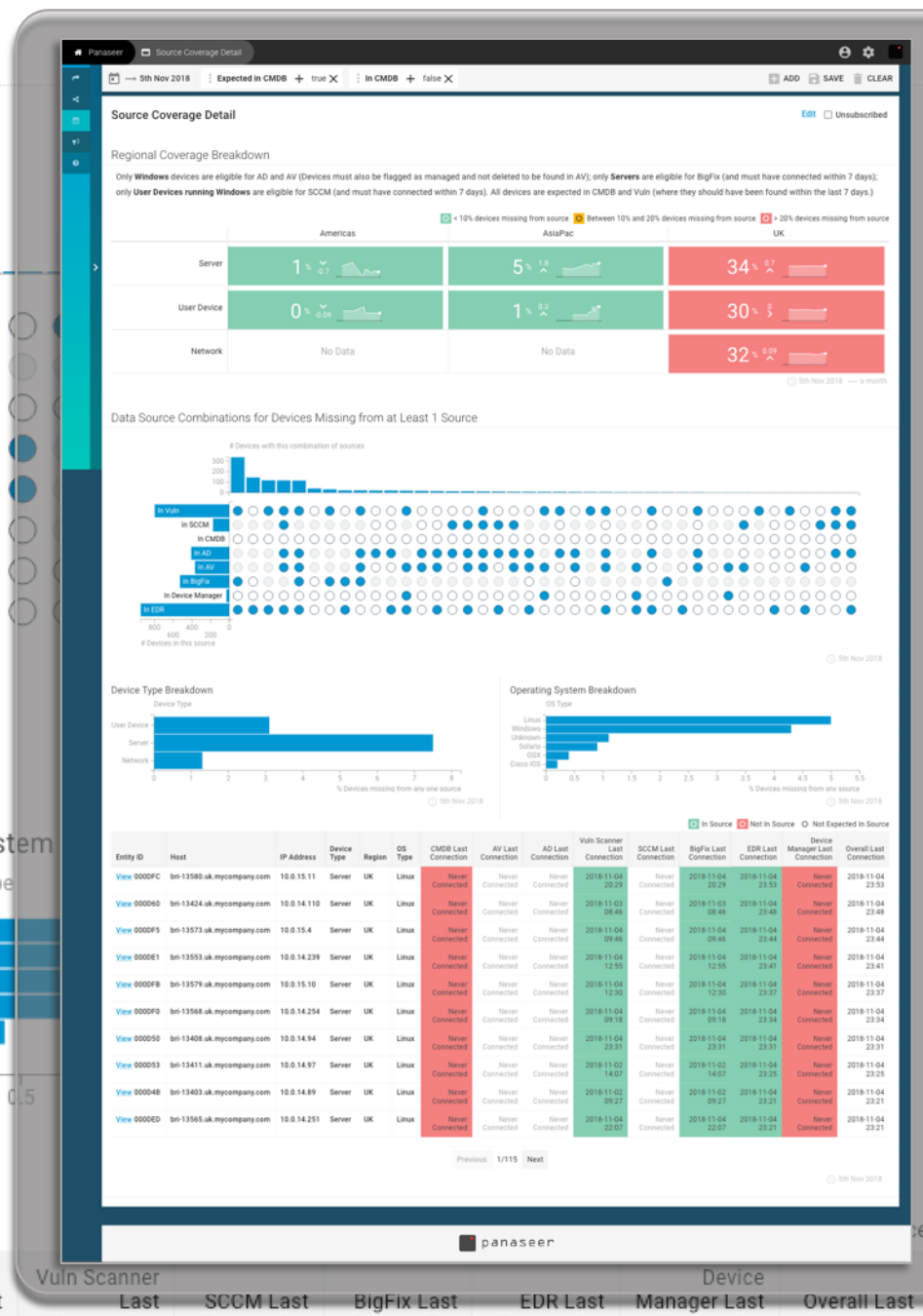
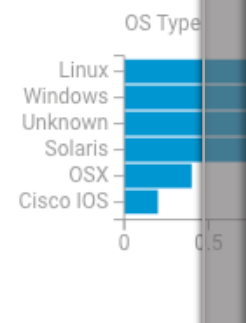
Data Source Combinations for Devices Missing from at Least 1 Source



Device Type Breakdown



Operating System



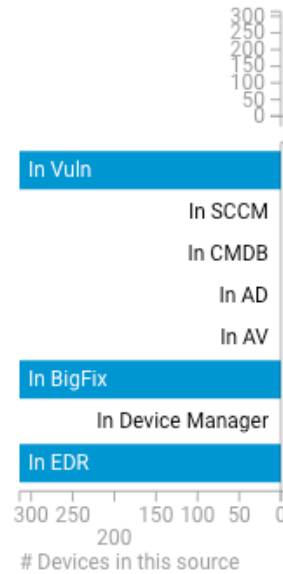
UK

Server

16% 15.3%

Data Source Combinations for Devices Missing from at Least 1 Source

Devices with this combination of sources



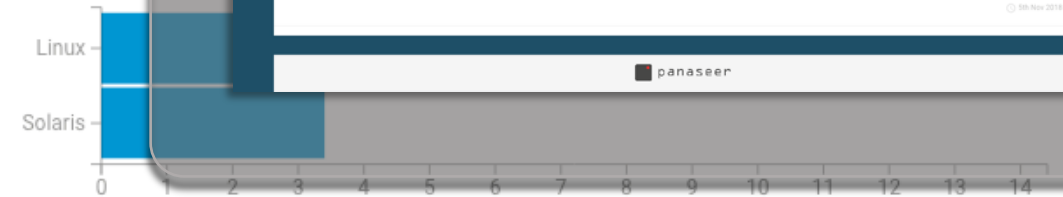
Device Type Breakdown

Device Type



Operating System

OS Type



Source Coverage Detail

5th Nov 2018 In EDR + true X In Device Manager + false X In BigFix + true X In AV + NULL X 11 Show all ADD SAVE CLEAR

only User Devices running Windows are eligible for SCCM (and must have connected within 7 days). All devices are expected in CMDB and Vuln (where they should have been found within the last 7 days.)

< 10% devices missing from source Between 10% and 20% devices missing from source > 20% devices missing from source

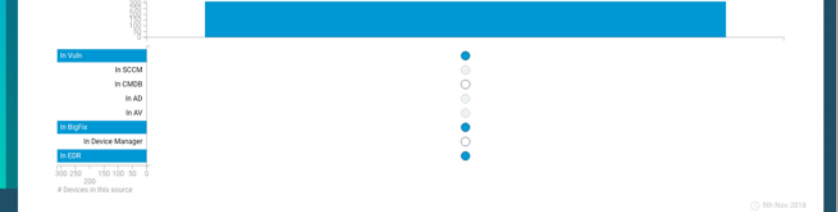
UK

Server 16% 15.3%

5th Nov 2018 4 months

Data Source Combinations for Devices Missing from at Least 1 Source

Devices with this combination of sources



Device Type Breakdown

Device Type



Operating System Breakdown

OS Type



															In Source	Not In Source	Not Expected in Source
Entity ID	Host	IP Address	Device Type	Region	OS Type	CMDB Last Connection	AV Last Connection	AD Last Connection	Vuln Scanner Last Connection	SCCM Last Connection	BigFix Last Connection	EDR Last Connection	Device Manager Last Connection	Overall Last Connection			
View 000DFC	bn-13583.uk.mycompany.com	10.0.15.11	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 20:29	Never Connected	2018-11-04 20:29	2018-11-04 23:53	Never Connected	2018-11-04 23:53	In Source	Not In Source	Not Expected in Source
View 000D60	bn-13424.uk.mycompany.com	10.0.14.110	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-03 08:46	Never Connected	2018-11-03 08:46	2018-11-04 23:48	Never Connected	2018-11-04 23:48	In Source	Not In Source	Not Expected in Source
View 000DF5	bn-13573.uk.mycompany.com	10.0.15.4	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 09:46	Never Connected	2018-11-04 09:46	2018-11-04 23:44	Never Connected	2018-11-04 23:44	In Source	Not In Source	Not Expected in Source
View 000DE1	bn-13553.uk.mycompany.com	10.0.14.239	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 12:55	Never Connected	2018-11-04 12:55	2018-11-04 23:41	Never Connected	2018-11-04 23:41	In Source	Not In Source	Not Expected in Source
View 000DFB	bn-13579.uk.mycompany.com	10.0.15.10	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 12:30	Never Connected	2018-11-04 12:30	2018-11-04 23:37	Never Connected	2018-11-04 23:37	In Source	Not In Source	Not Expected in Source
View 000DF0	bn-13568.uk.mycompany.com	10.0.14.254	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 09:18	Never Connected	2018-11-04 09:18	2018-11-04 23:34	Never Connected	2018-11-04 23:34	In Source	Not In Source	Not Expected in Source
View 000D50	bn-13408.uk.mycompany.com	10.0.14.94	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 22:31	Never Connected	2018-11-04 22:31	2018-11-04 23:31	Never Connected	2018-11-04 23:31	In Source	Not In Source	Not Expected in Source
View 000D53	bn-13411.uk.mycompany.com	10.0.14.97	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-03 14:07	Never Connected	2018-11-03 14:07	2018-11-04 23:25	Never Connected	2018-11-04 23:25	In Source	Not In Source	Not Expected in Source
View 000D4B	bn-13403.uk.mycompany.com	10.0.14.89	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-02 09:27	Never Connected	2018-11-02 09:27	2018-11-04 23:21	Never Connected	2018-11-04 23:21	In Source	Not In Source	Not Expected in Source
View 000DED	bn-13565.uk.mycompany.com	10.0.14.251	Server	UK	Linux	Never Connected	Never Connected	Never Connected	2018-11-04 22:07	Never Connected	2018-11-04 22:07	2018-11-04 23:21	Never Connected	2018-11-04 23:21	In Source	Not In Source	Not Expected in Source

Previous 1/32 Next

panaseer

Create Campaign

Objective *

CMDB coverage

Title *

CMDB Coverage clean up C1

Start Date*



2018-11-05

End Date*



2018-12-05

Scope

Expected in CMDB + true X

In AD + false X

In AV + false X

In BigFix + = true X

In CMDB + = false X false X

In Device Manager + = false X

In EDR + = true X

In SCCM + false X

In Vuln + = true X

Device Type + Server X

Region + UK X

Timestamp + 1541383200 X

Initial Workload

314 devices not in CMDB

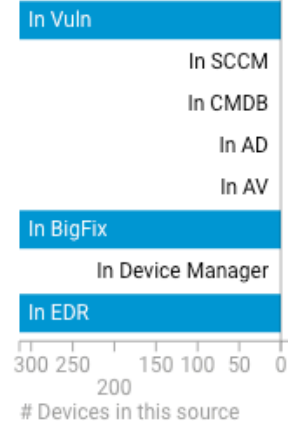
Notes

Campaign Management

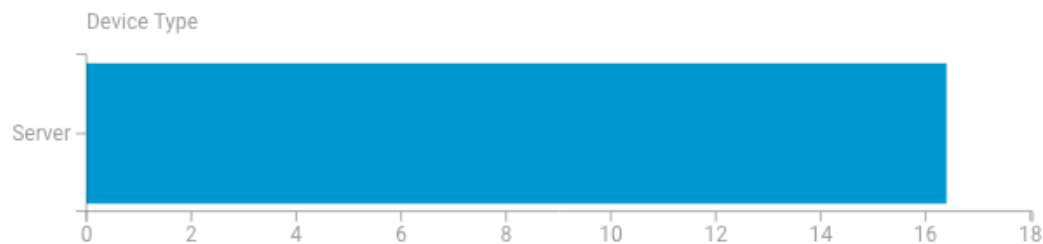
Track Campaigns
Monitor the progress of open campaigns.

Closed Campaigns
Browse closed campaigns.

+ New Campaign
Create a new campaign, based on the scope of the current dashboard filters.



Device Type Breakdown



UK

16% 15.3%

Least 1 Source



Source Coverage Detail

5th Nov 2018 In EDR + true X In Device Manager + false X In BigFix + true X In AV + NULL X 11 Show all. ADD SAVE CLEAR

Only User Devices running Windows are eligible for SCCM (and must have connected within 7 days). All devices are expected in CMDB and Vuln (where they should have been within the last 7 days).

< 10% devices missing from source Between 10% and 20% devices missing from source > 20% devices missing from source

UK

Server 16% 15.3%

5th Nov 2018 4 months

Data Source Combinations for Devices Missing from at Least 1 Source

Devices with this combination of sources

In Vuln In SCCM In CMDB In AD In AV In BigFix In Device Manager In EDR

5th Nov 2018

Operating System Breakdown

OS Type

Linux Solaris

5th Nov 2018

Device Type Breakdown

Device Type

Server

5th Nov 2018

Operating System Breakdown

OS Type

Linux Solaris

5th Nov 2018

Device Type Breakdown

Device Type

Server

5th Nov 2018

Operating System Breakdown

OS Type

Linux Solaris

5th Nov 2018

Device Type Breakdown

Device Type

Server

5th Nov 2018

Operating System Breakdown

OS Type

Linux Solaris

5th Nov 2018

Device Type Breakdown

Device Type

Server

Global SMB/EternalBlue Cleanup

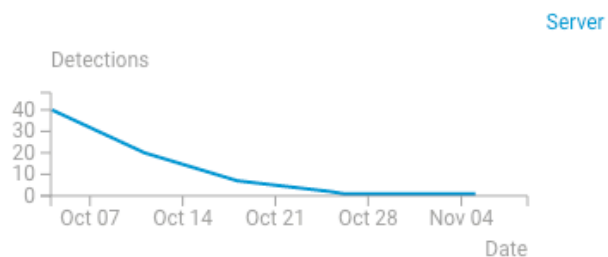


Remaining	1 detections / 40 detections		
End	2018-11-12 (6 months ago)	Started	2018-10-04

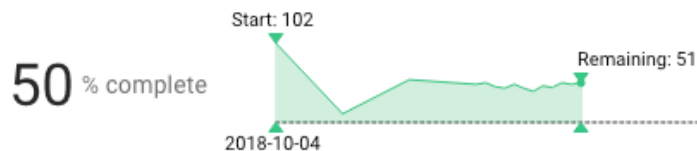
Scope

CVE + CVE-2017-0144 X

Campaign Progress by Device Type



Solaris Scan Coverage



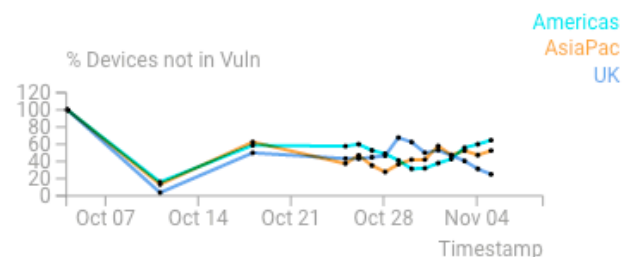
Remaining	51 devices not scanned / 102 devices not scanned		
End	2018-12-05 (5 months ago)	Started	2018-10-04

Scope

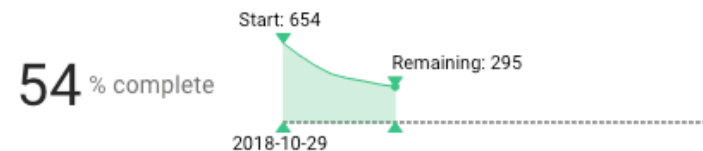
In Vuln + false X

OS Type + Solaris X

Devices Not Covered by Region



CrowdStrike Final Phase



Remaining	295 devices without EDR / 654 devices without EDR		
End	2018-12-05 (5 months ago)	Started	2018-10-29

Scope

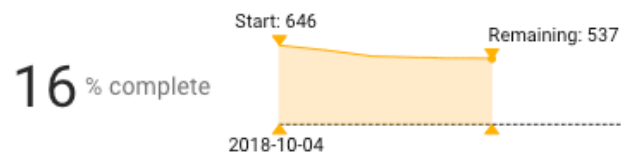
Device Type + User Device X

Region + Americas X

EDR Missing by BU

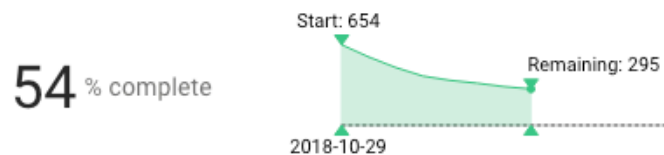


UK Inventory Refresh



5th Nov 2018 No Filters

CrowdStrike Final Phase



Remaining	295 devices without EDR / 654 devices without EDR		
End	2018-12-05 (5 months ago)	Started	2018-10-29

Scope

Device Type + User Device X Region + Americas X

Exceptions

+ ADD FROM FILTERS

Notes

Action History

EXPORT HISTORY

EDR Source Coverage

EDR Missing by Region

Americas

EDR Missing by Device

User Device

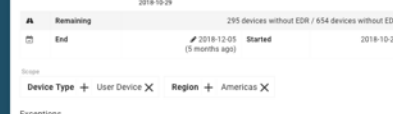
List of Devices with

Entity ID

[View](#) 0000A3[View](#) 0000A4[View](#) 0000A5

CrowdStrike Final Phase

54% complete



Remaining	295 devices without EDR / 654 devices without EDR		
End	2018-12-05 (5 months ago)	Started	2018-10-29

Scope

Device Type + User Device X Region + Americas X

Exceptions

Notes

Action History

EXPORT HISTORY

EDR Source Coverage

EDR Missing by Region

Americas

EDR Missing by Device Type

User Device

List of Devices with EDR Missing - Start of Campaign

Entity ID	DNS Name	IP Address	Device Type	Region	OS Type	EDR Conn
View 0000A3	bos-10163.americas.mycompany.com	10.0.1.164	User Device	Americas	Windows	N Conn
View 0000A4	bos-10164.americas.mycompany.com	10.0.1.165	User Device	Americas	Windows	N Conn
View 0000A5	bos-10165.americas.mycompany.com	10.0.1.166	User Device	Americas	Windows	N Conn
View 0000A6	bos-10166.americas.mycompany.com	10.0.1.167	User Device	Americas	Windows	N Conn
View 0000A7	bos-10167.americas.mycompany.com	10.0.1.168	User Device	Americas	Windows	N Conn
View 0000A9	bos-10169.americas.mycompany.com	10.0.1.170	User Device	Americas	OSX	N Conn
View 0000AA	bos-10170.americas.mycompany.com	10.0.1.171	User Device	Americas	OSX	N Conn
View 0000AB	bos-10171.americas.mycompany.com	10.0.1.172	User Device	Americas	OSX	N Conn
View 0000AC	bos-10172.americas.mycompany.com	10.0.1.173	User Device	Americas	OSX	N Conn
View 0000AD	bos-10173.americas.mycompany.com	10.0.1.174	User Device	Americas	OSX	N Conn

List of Devices with EDR Missing - Remaining in Campaign

Entity ID	Past Entity ID	DNS Name	IP Address	Device Type	Region	OS Type
View 0000A3	0000A3	bos-10163.americas.mycompany.com	10.0.1.164	User Device	Americas	Window
View 0000A4	0000A4	bos-10164.americas.mycompany.com	10.0.1.165	User Device	Americas	Window
View 0000A5	0000A5	bos-10165.americas.mycompany.com	10.0.1.166	User Device	Americas	Window
View 0000A6	0000A6	bos-10166.americas.mycompany.com	10.0.1.167	User Device	Americas	Window
View 0000A7	0000A7	bos-10167.americas.mycompany.com	10.0.1.168	User Device	Americas	Window
View 0000A9	0000A9	bos-10169.americas.mycompany.com	10.0.1.170	User Device	Americas	OSX
View 0000AA	0000AA	bos-10170.americas.mycompany.com	10.0.1.171	User Device	Americas	OSX
View 0000AB	0000AB	bos-10171.americas.mycompany.com	10.0.1.172	User Device	Americas	OSX
View 0000AC	0000AC	bos-10172.americas.mycompany.com	10.0.1.173	User Device	Americas	OSX
View 0000AD	0000AD	bos-10173.americas.mycompany.com	10.0.1.174	User Device	Americas	OSX



→ 5th Nov 2018 No Filters

Key Controls Assurance

Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB



5th Nov 2018 a month

Metric: Inventory Rate

average days to inventory new device



5th Nov 2018 a month

Other Information: Completeness

% CMDB records with complete data



Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB



5th Nov 2018 a month

Metric: Inventory Rate

average days to inventory new device



5th Nov 2018 a month

Other Information: Completeness

% CMDB records with complete data



5th Nov 2018 a month

Other Information: Onboarding

% devices inventoried on day of install



5th Nov 2018 a month

Vulnerability Management

Metric: Coverage Failures

% devices not scanned in last 7 days



5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA



5th Nov 2018 a month

Other Information: Typical Device

average critical detections per device



Vulnerability Management

Metric: Coverage Failures

% devices not scanned in last 7 days



5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA



5th Nov 2018 a month

Other Information: Typical Device

average critical detections per device



5th Nov 2018 a month

Other Information: Outliers

% devices accounting for 80% of backlog



5th Nov 2018 a month

Malware Defences

AV: Coverage Failures

AV: SLA Breaches

EDR: Coverage Failures

EDR: Policy Breaches

Malware Defences

AV: Coverage Failures

% endpoints not installed



5th Nov 2018 a month

AV: SLA Breaches

% devices not scanned/updated in 7 days



5th Nov 2018 a month

EDR: Coverage Failures

% endpoints not installed



5th Nov 2018 a month

EDR: Policy Breaches

% agents not connecting or out of date



5th Nov 2018 a month

Security Skills Assessment

Metric: Phishing Tests Sent

% employees not sent test in last month



5th Nov 2018 a month

Metric: Phishing Click Rate

% phishing bait clicked through



5th Nov 2018 a month

Other Information: Campaigns

phishing campaigns completed



5th Nov 2018 a month

Other Information: Worst Offenders

% repeat click-through offenders



5th Nov 2018 a month

Application Software Security

Metric: Applications Reviewed

% applications not scanned (12 months)



5th Nov 2018 a month

Metric: Issues Failing SLA

% open critical/high detections failing SLA



5th Nov 2018 a month

Other Information: Worst Offenders

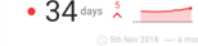
applications with open critical detections



5th Nov 2018 a month

Other Information: Fix Rate

average age of open detections



5th Nov 2018 a month

→ 5th Nov 2018 No Filters

Key Metrics: Vulnerability Technical Debt

Key Metrics Overview

Vulnerability Scan Coverage

% eligible devices scanned recently

81 %

5th Nov 2018 a month

Performance KPI

avg # detections per device

5

5th Nov 2018 a month

Technical Debt

% detections in backlog

78

5th

Key Areas to Address: Backlog Breakdown and Worst Offending Devices

Each cell is the number of vulnerability detections in the backlog for a given region and device type combination, as a percentage of the total number of identified devices for this combination.

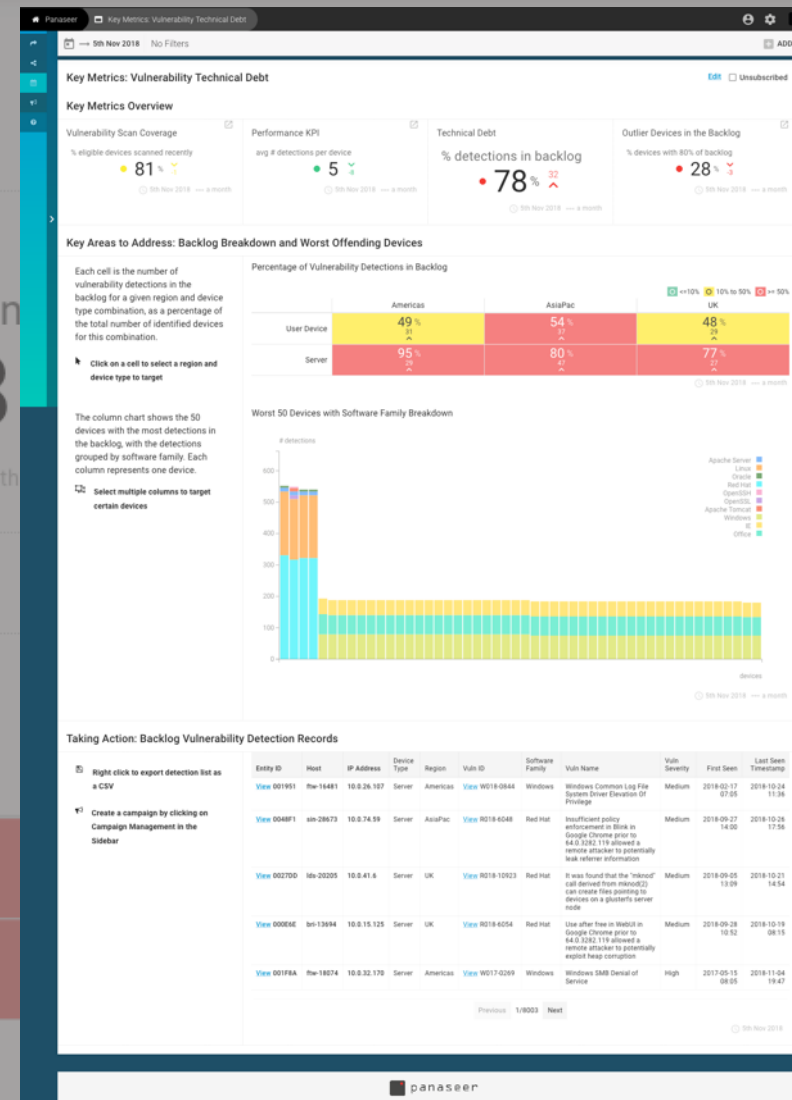
Click on a cell to select a region and device type to target

Percentage of Vulnerability Detections in Backlog

	Americas
User Device	49 % 31
Server	95 % 29

Worst 50 Devices with Software Family Breakdown

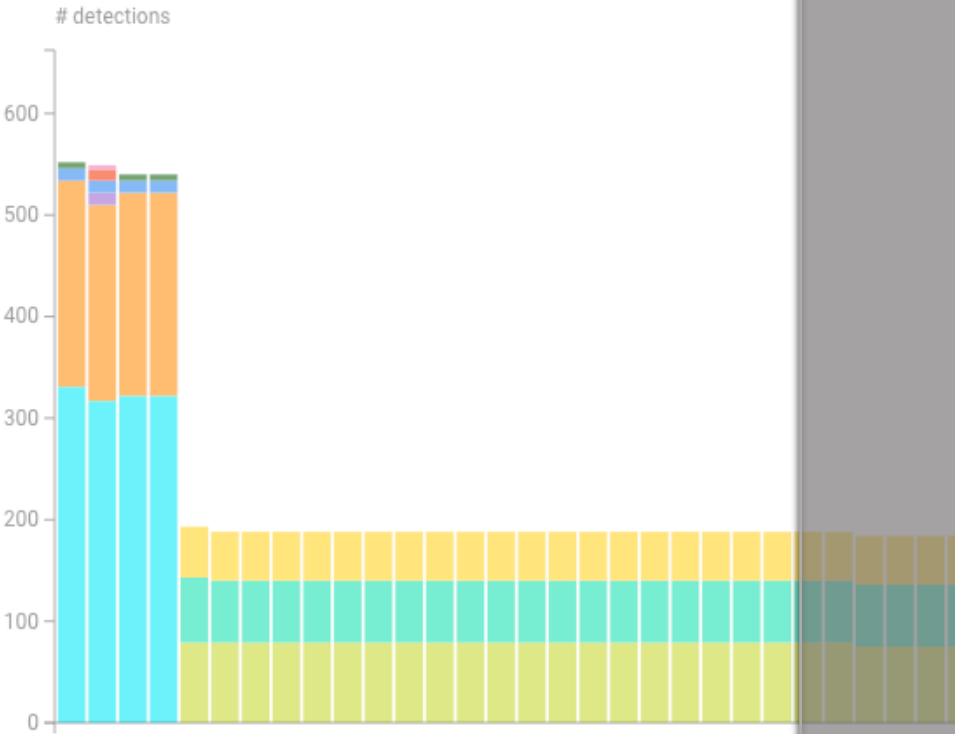
The column chart shows the 50 devices with the most detections in



The column chart shows the 50 devices with the most detections in the backlog, with the detections grouped by software family. Each column represents one device.

Select multiple columns to target certain devices

Worst 50 Devices with Software Family Breakdown



Taking Action: Backlog Vulnerability Detection Records

Right click to export detection list as a CSV

Entity ID	Host	IP Address	Device Type	Region	Vuln ID	Software Family	Vuln Name	Severity	First Seen	Timestamp
View 001951	ftw-16481	10.0.26.107	Server	Americas	View W018-0844	Windows	Windows Common Log File System Driver Elevation Of Privilege	Medium	2018-02-17 07:05	2018-10-24 11:36

panaseer

Key Metrics: Vulnerability Technical Debt

Key Metrics Overview

Vulnerability Scan Coverage

% eligible devices scanned recently

81%

Performance KPI

avg # detections per device

5

Technical Debt

% detections in backlog

78%

Outlier Devices in the Backlog

% devices with 80% of backlog

28%

Key Areas to Address: Backlog Breakdown and Worst Offending Devices

Each cell is the number of vulnerability detections in the backlog for a given region and device type combination, as a percentage of the total number of identified devices for this combination.

Click on a cell to select a region and device type to target

	Americas	AsiaPac	UK
User Device	49%	54%	48%
Server	95%	80%	77%

The column chart shows the 50 devices with the most detections in the backlog, with the detections grouped by software family. Each column represents one device.

Select multiple columns to target certain devices

Taking Action: Backlog Vulnerability Detection Records

Right click to export detection list as a CSV

Create a campaign by clicking on Campaign Management in the sidebar

Entity ID	Host	IP Address	Device Type	Region	Vuln ID	Software Family	Vuln Name	Severity	First Seen	Last Seen
View 001951	ftw-16481	10.0.26.107	Server	Americas	View W018-0844	Windows	Windows Common Log File System Driver Elevation Of Privilege	Medium	2018-02-17 07:05	2018-10-24 11:36
View 0048F1	win-28679	10.0.74.59	Server	AsiaPac	View R018-6048	Red Hat	Insufficient patch enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referral information	Medium	2018-09-27 14:00	2018-10-26 17:56
View 0027D0	ids-20205	10.0.41.6	Server	UK	View R018-10923	Red Hat	It was found that the "telnetd" call derived from libnet(2) can create files pointing to devices on a glusterfs server node	Medium	2018-09-05 13:09	2018-10-21 14:54
View 0006E6	bin-13694	10.0.15.125	Server	UK	View R018-6054	Red Hat	User after free in libcurl in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption	Medium	2018-09-28 10:52	2018-10-19 08:15
View 001F8A	ftw-18074	10.0.32.170	Server	Americas	View W017-0269	Windows	Windows SMB Denial of Service	High	2017-05-15 08:55	2018-11-04 19:47

Criticality + Critical X

Search

What dimension do you want to apply a filter for?

# Detections	!	>
# Devices	!	>
Business Unit	!	>
CVE	!	>
City	!	>
Country	!	>
Criticality	!	>
Cumul Detect	!	>
Cumul Perc	!	>
DNS	!	>
Days Between Vuln Published First Seen	!	>
Days Between Vuln Published First Seen Bins	!	>
Days Since Last Connect	!	>


+ Include

 TOGGLE  Clear



VALUES

PATTERN

Search / Add Values

 Add☐ Select All☒ Critical☐ High☐ Low☐ Moderate

<> SQL Console

Are you finding the filter interface helpful?   Cancel Apply

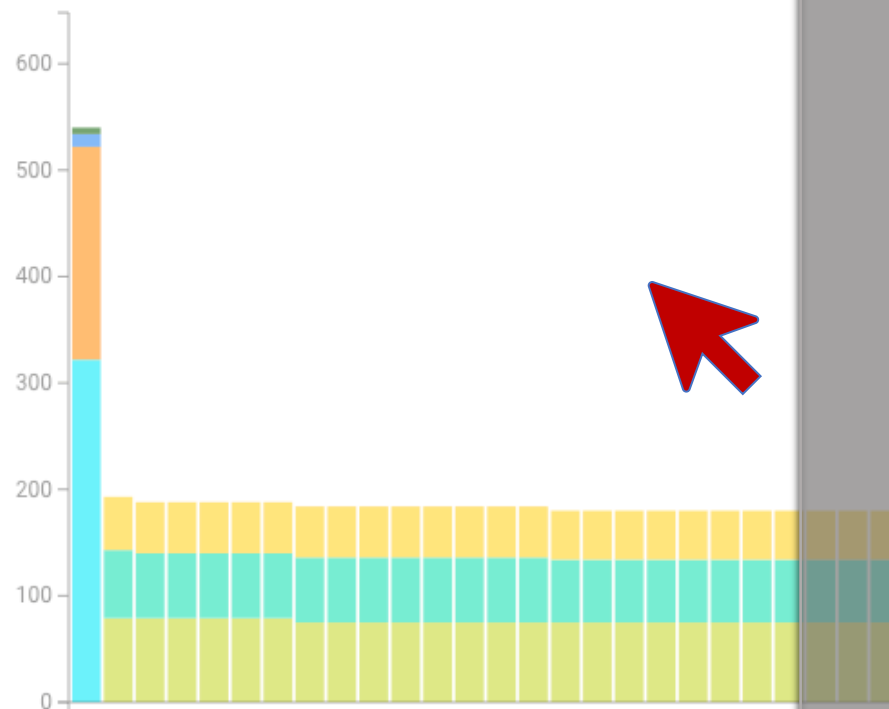
device type to target

The column chart shows the 50 devices with the most detections in the backlog, with the detections grouped by software family. Each column represents one device.

Select multiple columns to target certain devices

Worst 50 Devices with Software Family Breakdown

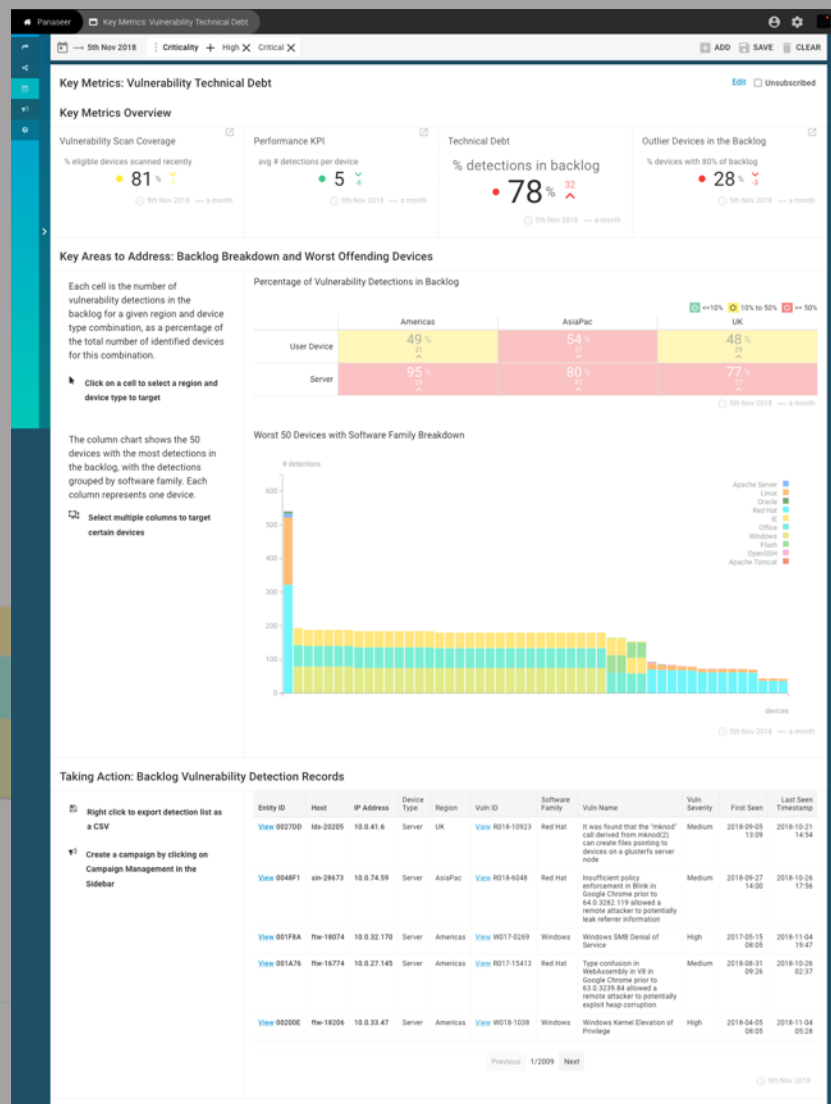
detections



Taking Action: Backlog Vulnerability Detection Records

Right click to export detection list as a CSV

Entity ID	Host	IP Address	Device Type	Region	Vuln ID	Software Family	Vuln Name	Severity	First Seen	Last Seen Timestamp
View 0027DD	lds-20205	10.0.41.6	Server	UK	View R018-10923	Red Hat	It was found that the "mknd" call derived from mknd(2) can create files pointing to devices on a glusterfs server node	Medium	2018-09-05 13:09	2018-10-21 14:54
View 0048F1	sin-28473	10.0.74.59	Server	AsiaPac	View R018-6048	Red Hat	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referer information	Medium	2019-09-27 14:00	2019-10-26 17:56
View 001F8A	the-18074	10.0.32.170	Server	Americas	View W017-0269	Windows	Windows SMB Denial of Service	High	2017-05-15 08:05	2018-11-04 19:47
View 001A76	the-18774	10.0.27.145	Server	Americas	View R017-15413	Red Hat	Type confusion in WebAssembly in V8 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption	Medium	2018-08-31 09:26	2018-10-26 02:37
View 00200E	the-18206	10.0.33.47	Server	Americas	View W018-1038	Windows	Windows Kernel Elevation of Privilege	High	2019-04-05 08:05	2018-11-04 05:28





[< Back to "Key Metrics: Vulnerability Technical Debt" Dashboard](#)



LDS-19599

Serial Number List: ASST29599S

Edit

Device Identifiers

Serial Number List	ASST29599S
Host List	LDS-19599
DNS List	lds-19599.uk.mycompany.com
MAC Address List	ab:cd:ef:63:c3:64
IP Address List	10.0.38.165
Netbios List	-

Device Context

Device Type	Server
Device Subtype	Web application
OS	RHEL 6.7

Network Context

Environment Type	Test
Network Location	External
Domain	-
Distinguished Name	-

Business Context

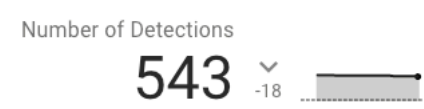
Criticality	High
Region	UK
Country	UK
Business Unit	Investment Management
Division	-
Functional Role	Unknown
Owner	Brady Troup
Manager	Wynn Sarney
Assignee	Brady Troup

Data Source Coverage

BigFix	2018-11-04 13:37
CrowdStrike	2018-11-03 23:06
ServiceNow	2018-10-31 22:27
Tenable SC	2018-11-04 13:37

5th Nov 2018

Vulnerabilities



Hosted Applications



Endpoint Protection

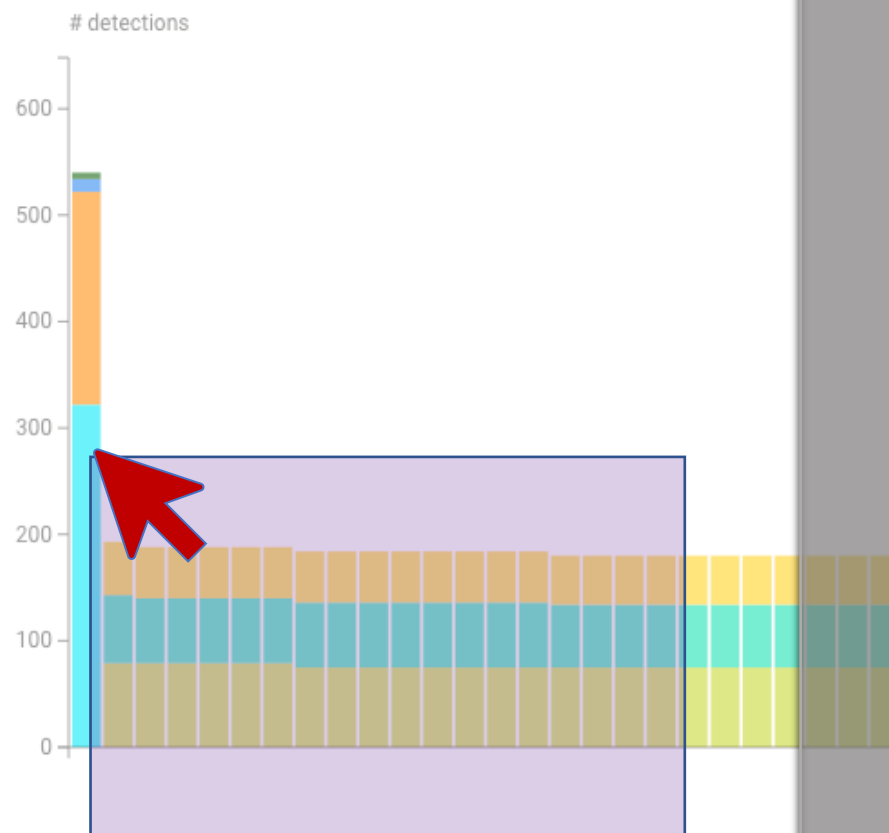
No Data

device type to target

The column chart shows the 50 devices with the most detections in the backlog, with the detections grouped by software family. Each column represents one device.

Select multiple columns to target certain devices

Worst 50 Devices with Software Family Breakdown



Taking Action: Backlog Vulnerability Detection Records

Right click to export detection list as a CSV

Entity ID	Host	IP Address	Device Type	Region	Vuln ID	Software Family	Vuln Name	Severity	First Seen	Last Seen
View 0027DD	Ids-20205	10.0.41.6	Server	UK	View R018-10923	Red Hat	It was found that the "mknd" call derived from mknd(2) can create files pointing to devices on a glusterfs server node	Medium	2018-09-05 13:09	2018-10-21 14:54
View 0048F1	sin-28473	10.0.74.59	Server	AsiaPac	View R018-6048	Red Hat	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referer information	Medium	2018-09-27 14:00	2018-10-26 17:56
View 001F8A	the-18074	10.0.32.170	Server	Americas	View W017-0269	Windows	Windows SMB Denial of Service	High	2017-05-15 08:05	2018-11-04 19:47
View 001A76	the-18774	10.0.27.145	Server	Americas	View R017-15413	Red Hat	Type confusion in WebAssembly in V8 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption	Medium	2018-08-31 09:26	2018-10-26 02:37
View 00200E	the-18206	10.0.33.47	Server	Americas	View W018-1038	Windows	Windows Kernel Elevation of Privilege	High	2018-04-05 08:05	2018-11-04 05:28

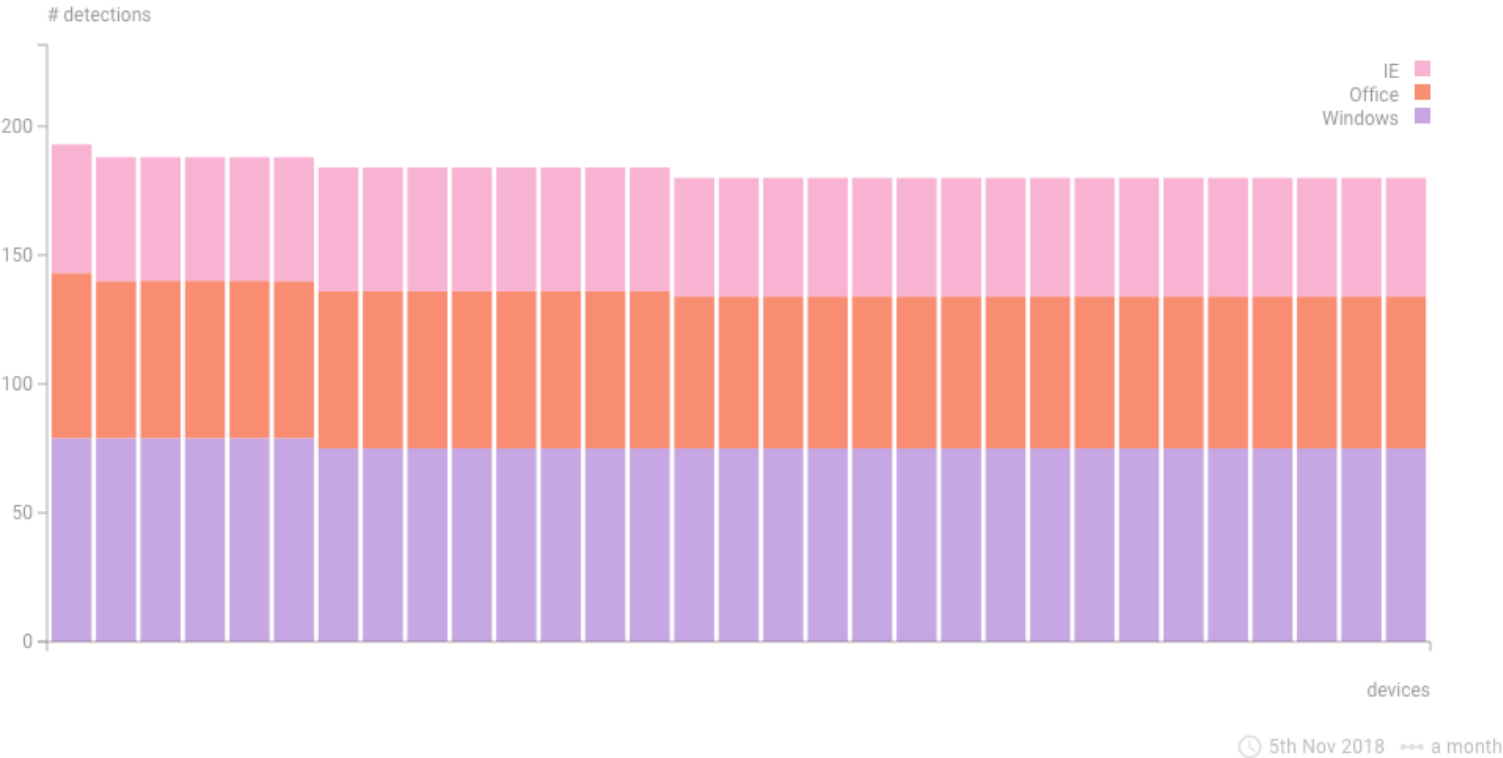


device type to target

The column chart shows the 50 devices with the most detections in the backlog, with the detections grouped by software family. Each column represents one device.

Select multiple columns to target certain devices

Worst 50 Devices with Software Family Breakdown



Taking Action: Backlog Vulnerability Detection Records

- Right click to export detection list as a CSV
- Create a campaign by clicking on Campaign Management in the Sidebar

Entity ID	Host	IP Address	Device Type	Region	Vuln ID	Software Family	Vuln Name	Vuln Severity	First Seen	Last Seen Timestamp
View 001F8A	ftw-18074	10.0.32.170	Server	Americas	View W017-0269	Windows	Windows SMB Denial of Service	High	2017-05-15 08:05	2018-11-04 19:47
View 002116	ftw-18470	10.0.34.56	Server	Americas	View W017-0298	Windows	Windows COM Session Elevation of Privilege	Medium	2018-05-20 01:16	2018-10-25 14:16
View 00200E	ftw-18206	10.0.33.47	Server	Americas	View W018-1038	Windows	Windows Kernel	High	2018-04-05	2018-11-04

Vulnerability Management

Metric: Coverage Failures

% devices not scanned in last 7 days



5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA



5th Nov 2018 a month

Other Information: Typical Device

average critical detections per device



Other Information: Outliers

% devices accounting for 80% of backlog



Malware Defences

AV: Coverage Failures

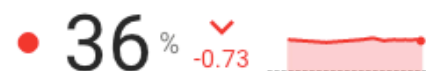
% endpoints not installed



5th Nov 2018 a month

AV: SLA Breaches

% devices not scanned/updated in 7 days



5th Nov 2018 a month

EDR: Coverage Failures

% endpoints not installed



Security Skills Assessment

Metric: Phishing Tests Sent

% employees not sent test in last month



5th Nov 2018 a month

Metric: Phishing Click Rate

% phishing bait clicked through



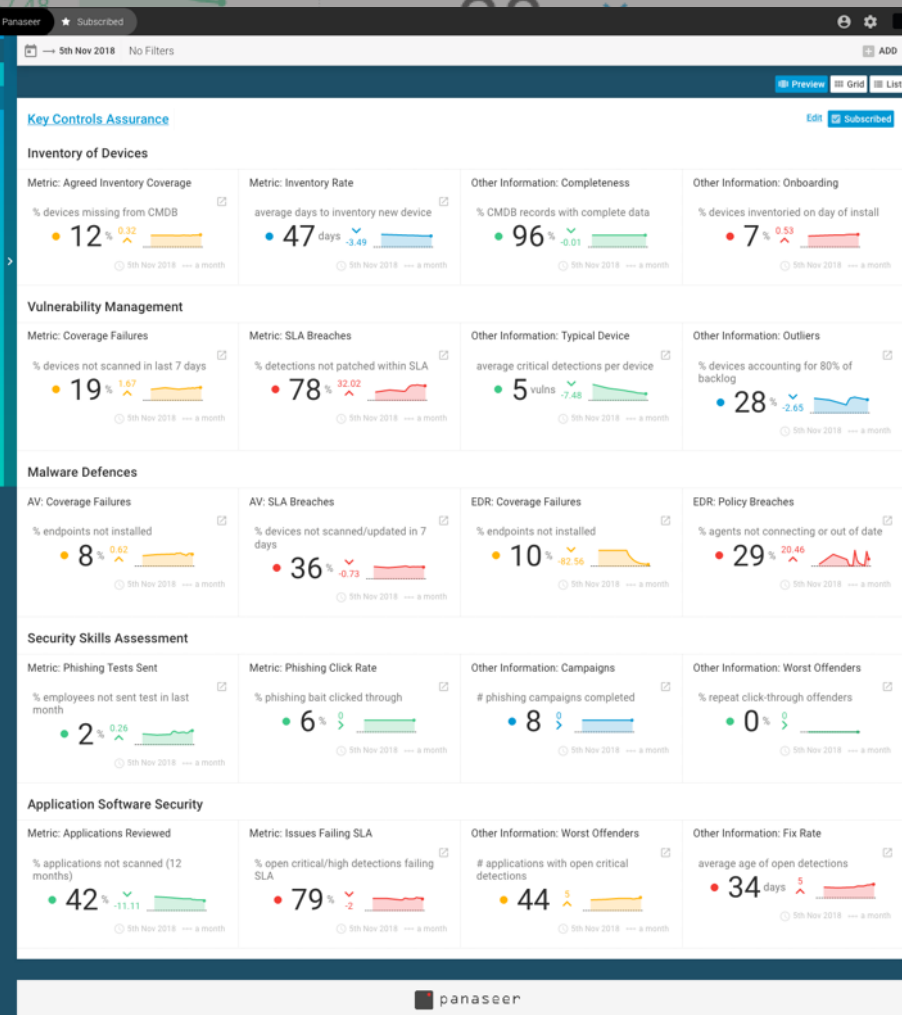
5th Nov 2018 a month

Other Information: Phishing Campaigns

phishing campaigns completed



Application Software Security









5th Nov 2018 No Filters

AV SLA Report

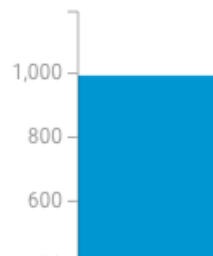
% devices failing policy

7+ days since last scan OR 1+ days since expiry

	Americas	AsiaPac
Desktop	20% 	4% 
Laptop	46% 	32% 
Server	49% 	35% 

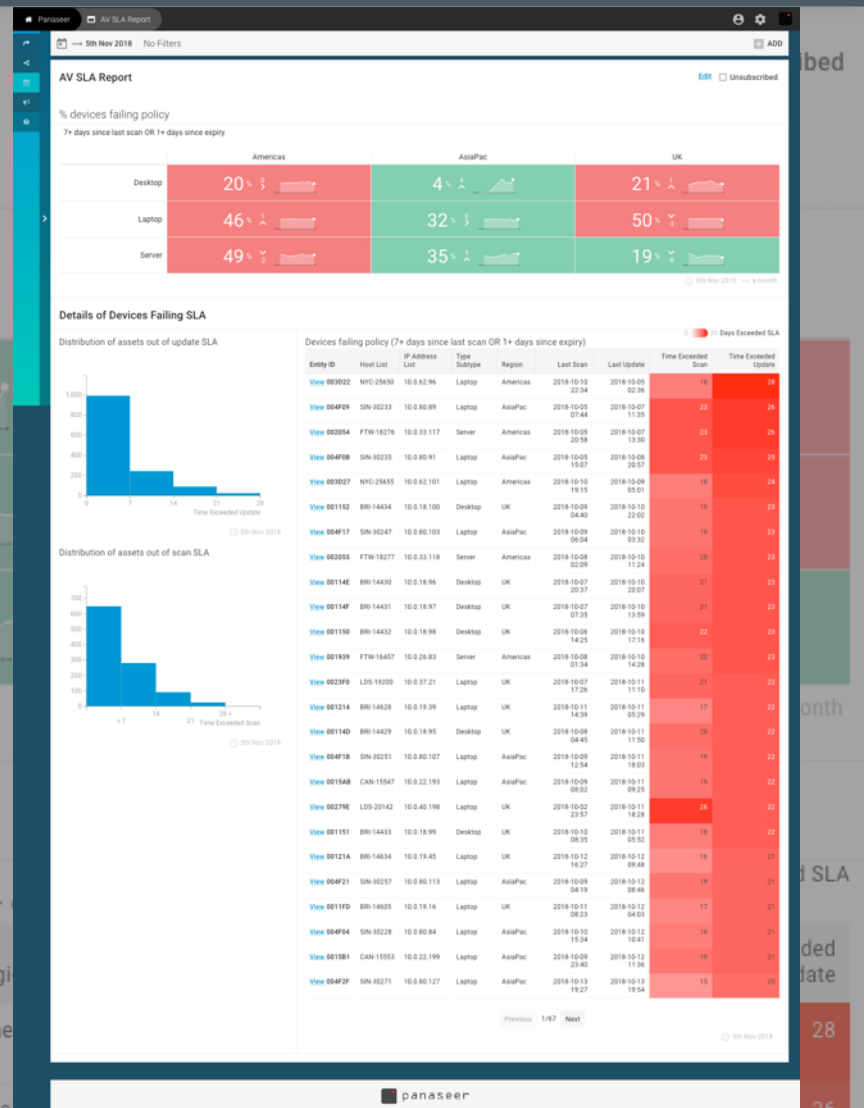
Details of Devices Failing SLA

Distribution of assets out of update SLA



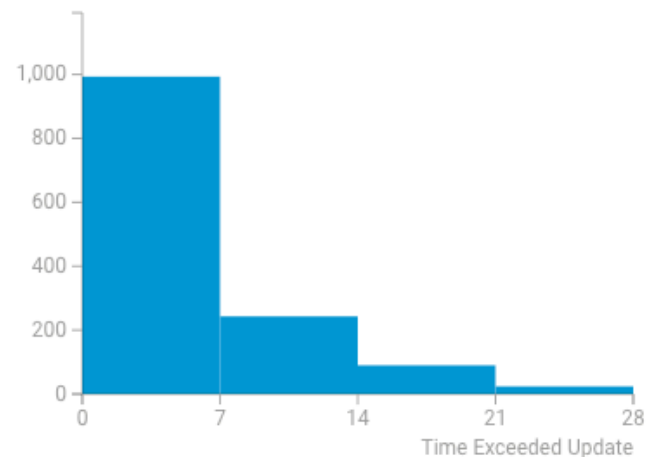
Devices failing policy (7+ days since last scan OR 1+

Entity ID	Host List	IP Address List	Type Subtype	Region
View 003D22	NYC-25650	10.0.62.96	Laptop	Ame
View 004F09	SIN-30233	10.0.80.89	Laptop	Asia
View 002054	FTW-18276	10.0.33.117	Server	Americas



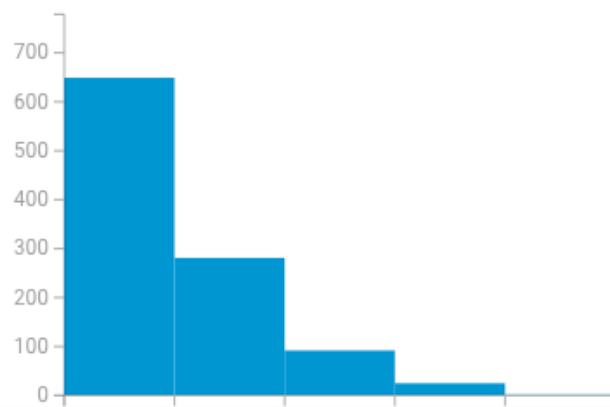
Details of Devices Failing SLA

Distribution of assets out of update SLA



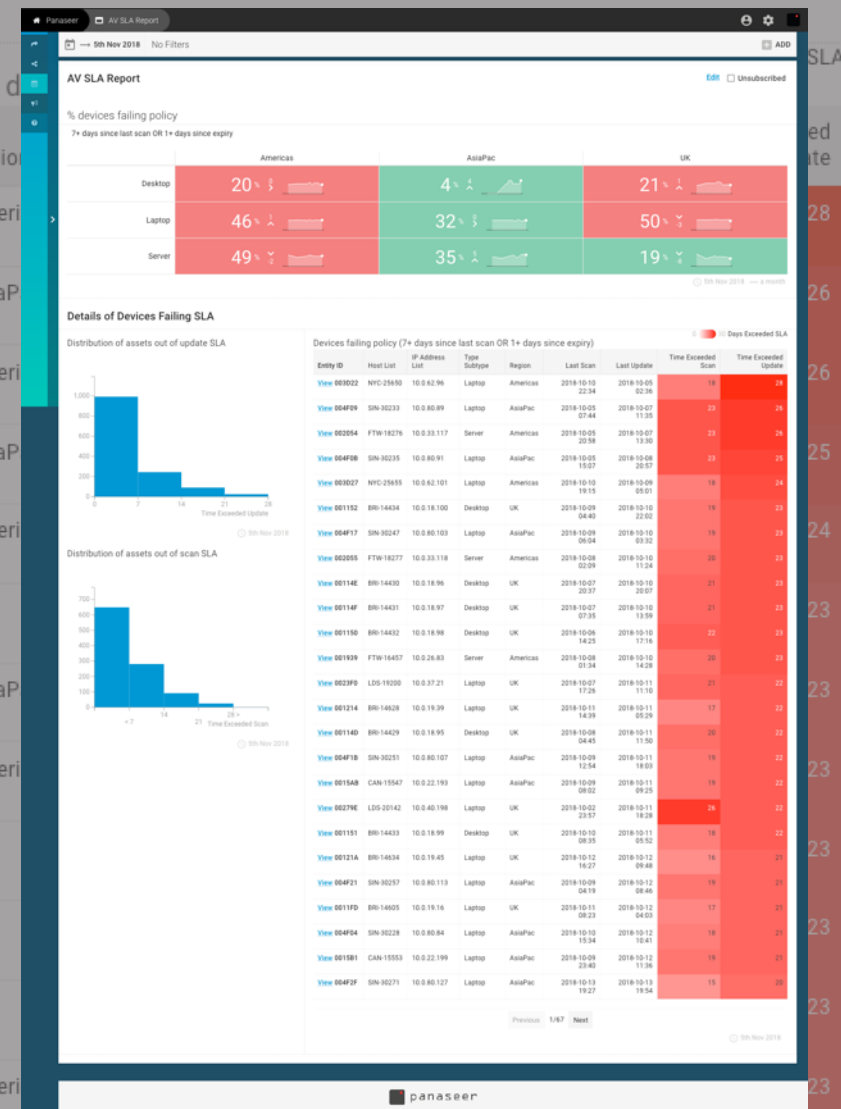
5th Nov 2018

Distribution of assets out of scan SLA



Devices failing policy (7+ days since last scan OR 1+ days since update)

Entity ID	Host List	IP Address List	Type Subtype	Region
View 003D22	NYC-25650	10.0.62.96	Laptop	Americas
View 004F09	SIN-30233	10.0.80.89	Laptop	AsiaPac
View 002054	FTW-18276	10.0.33.117	Server	Americas
View 004F0B	SIN-30235	10.0.80.91	Laptop	AsiaPac
View 003D27	NYC-25655	10.0.62.101	Laptop	Americas
View 001152	BRI-14434	10.0.18.100	Desktop	UK
View 004F17	SIN-30247	10.0.80.103	Laptop	AsiaPac
View 002055	FTW-18277	10.0.33.118	Server	Americas
View 00114E	BRI-14430	10.0.18.96	Desktop	UK
View 00114F	BRI-14431	10.0.18.97	Desktop	UK
View 001150	BRI-14432	10.0.18.98	Desktop	UK
View 001939	FTW-16457	10.0.26.83	Server	Americas
View 0023F0	LDS-19200	10.0.37.21	Laptop	UK
View 001214	BRI-14628	10.0.19.39	Laptop	UK

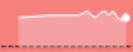







5th Nov 2018 No Filters

AV SLA Report

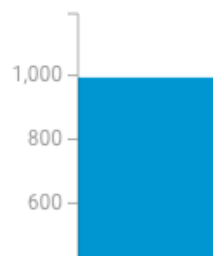
% devices failing policy

7+ days since last scan OR 1+ days since expiry

	Americas	AsiaPac
Desktop	20% 	4% 
Laptop	46% 	32% 
Server	49% 	35% 

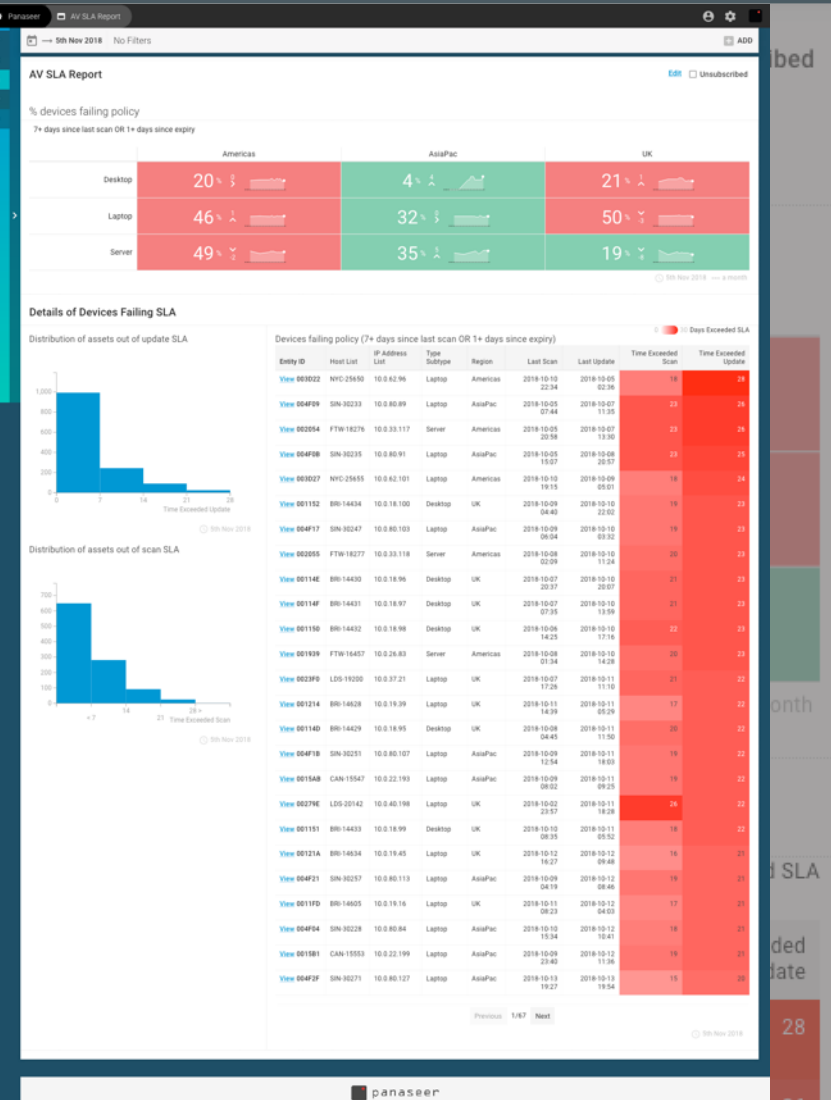
Details of Devices Failing SLA

Distribution of assets out of update SLA



Devices failing policy (7+ days since last scan OR 1+ days since expiry)

Entity ID	Host List	IP Address List	Type Subtype	Region
View 003D22	NYC-25650	10.0.62.96	Laptop	Americas
View 004F09	SIN-30233	10.0.80.89	Laptop	AsiaPac
View 002054	FTW-18276	10.0.33.117	Server	Americas



5th Nov 2018






Region + AsiaPac X

Type Subtype + Desktop X

AV SLA Report

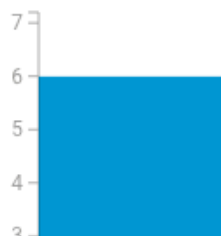
% devices failing policy

7+ days since last scan OR 1+ days since expiry

	Americas	AsiaPac
Desktop	20% 	4% 
Laptop	46% 	32% 
Server	49% 	35% 

Details of Devices Failing SLA

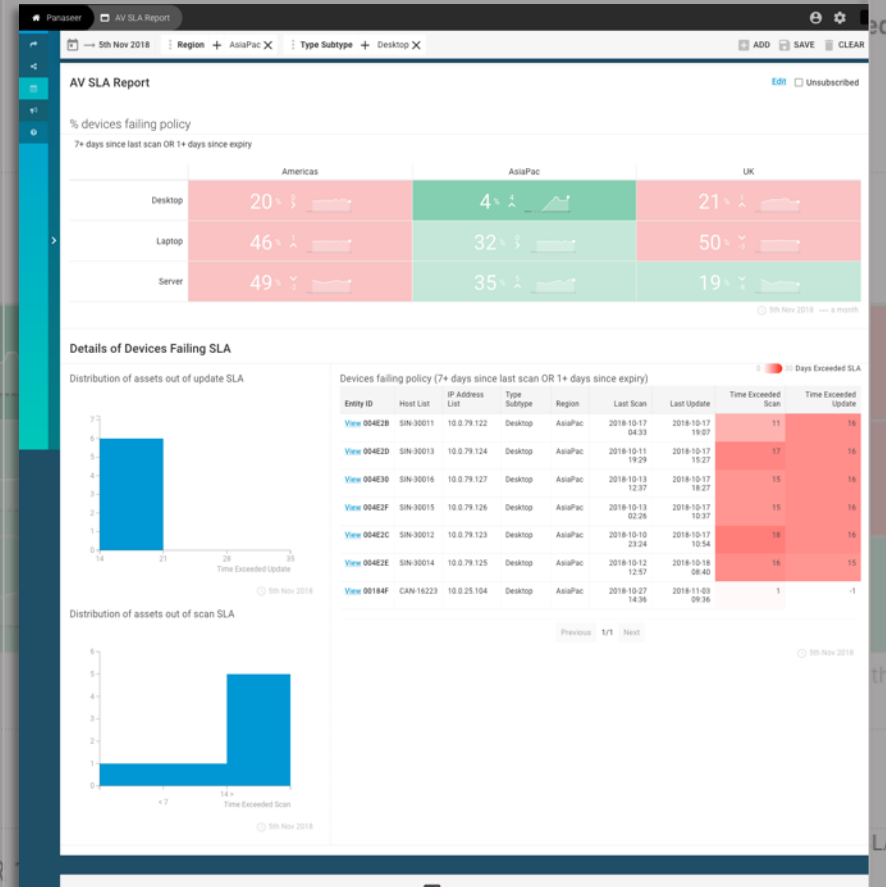
Distribution of assets out of update SLA



Devices failing policy (7+ days since last scan OR 1+ days since expiry)

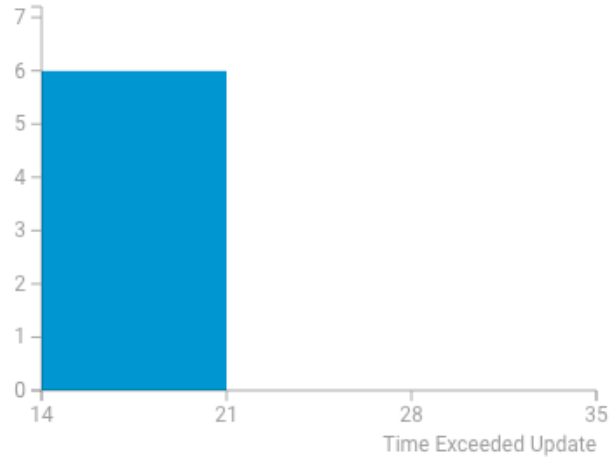
Entity ID	Host List	IP Address List	Type Subtype	Region	Last Scan	Last Update	Time Exceeded Scan	Time Exceeded Update
View 004E2B	SIN-30011	10.0.79.122	Desktop	AsiaPac	2018-10-17 04:33	2018-10-17 19:07	11	16
View 004E2D	SIN-30013	10.0.79.124	Desktop	AsiaPac	2018-10-11 19:29	2018-10-17 15:27	17	16
View 004E30	SIN-30016	10.0.79.127	Desktop	AsiaPac	2018-10-13 12:37	2018-10-17 18:27	15	16

+ ADD SAVE CLEAR



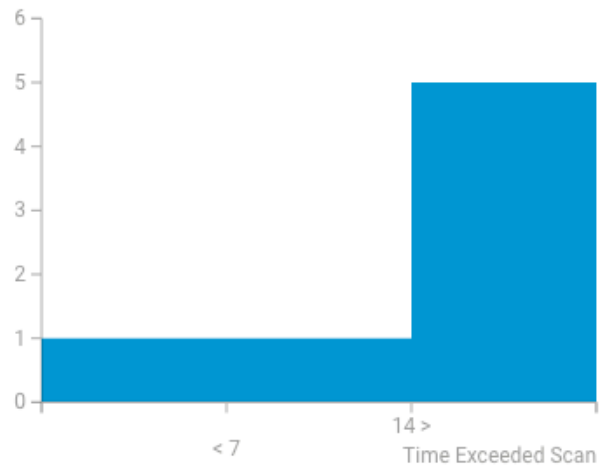
Details of Devices Failing SLA

Distribution of assets out of update SLA



5th Nov 2018

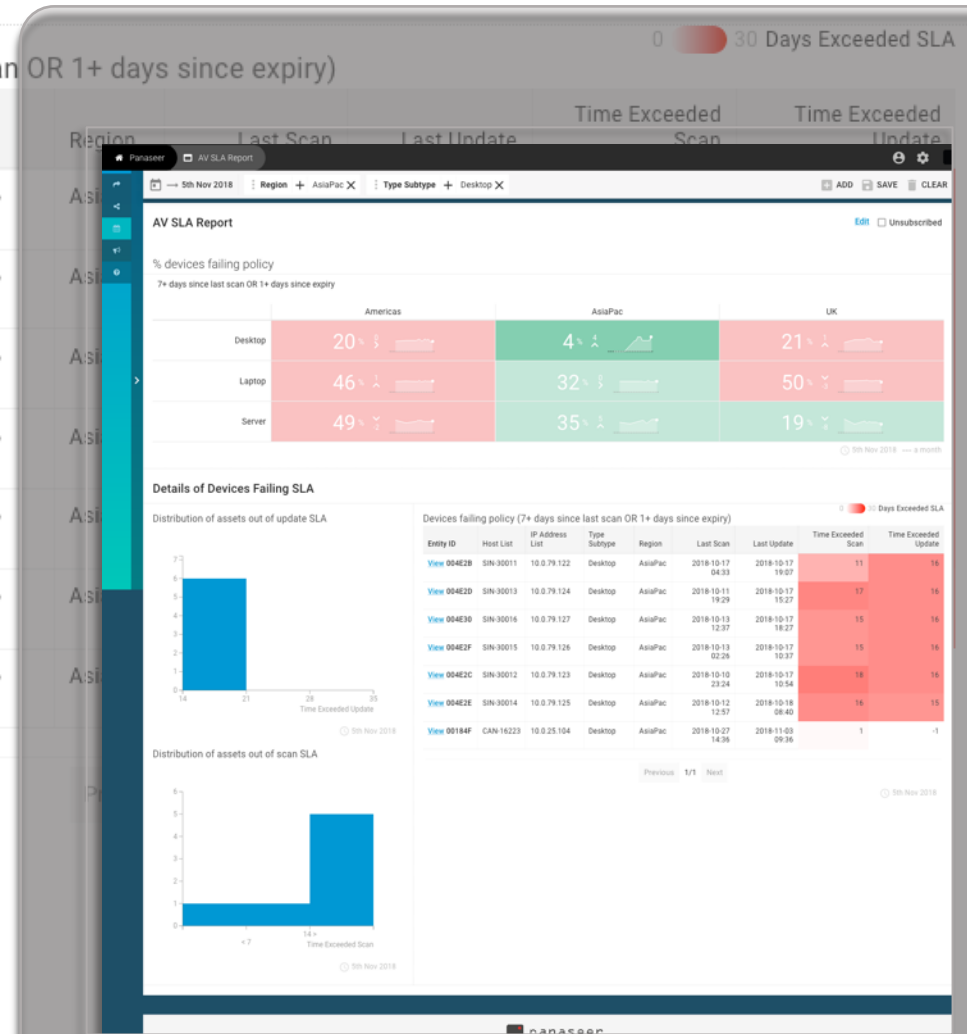
Distribution of assets out of scan SLA



5th Nov 2018

Devices failing policy (7+ days since last scan OR 1+ days since expiry)

Entity ID	Host List	IP Address List	Type Subtype
View 004E2B	SIN-30011	10.0.79.122	Desktop
View 004E2D	SIN-30013	10.0.79.124	Desktop
View 004E30	SIN-30016	10.0.79.127	Desktop
View 004E2F	SIN-30015	10.0.79.126	Desktop
View 004E2C	SIN-30012	10.0.79.123	Desktop
View 004E2E	SIN-30014	10.0.79.125	Desktop
View 00184F	CAN-16223	10.0.25.104	Desktop



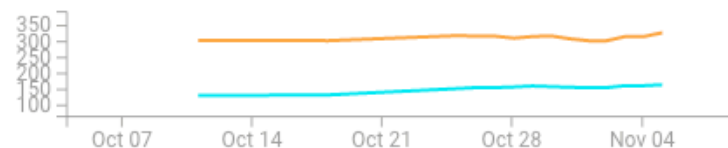
- 

ADD

🕒 5th Nov 2018
📅 a month

🕒 5th Nov 2018
🔍 a month

Detections



🕒 5th Nov 2018 📅 a month

Detections



Not subscribed

en

days

th Nov 2018

100%

100%

100%

Pass

100%

100%

--- a month

100%

Education Issues

Measurement Errors

Code Quality

s Management

Security Insights Dashboards

> ★ Subscribed

> ⌚ Recent

👤 Shared With You

▼ 📁 NIST Controls Assurance

▼ 📁 Identify

▼ 📁 Asset Management

▼ 📁 Device Inventory

📊 Device Inventory Rate

📁 Software Inventory

▼ 📁 Data Source Coverage

▼ 📁 CISO

📊 CISO Data Source Coverage

📊 Source Coverage Detail

▼ 📁 Program Manager

📊 Source Coverage Detail

▼ 📁 Protect

📁 Configuration Management

▼ 📁 Privileged Access Management

▼ 📁 Administrative Privilege and Permissions

📊 PAM: Linux/Unix Administrative Privileges

📊 PAM: Windows Administrative Privileges

▼ 📁 Authentication Events and Infringements

📊 PAM: Linux/Unix Infringement Report

📊 PAM: Windows Infringement Report

▼ 📁 Access Management

📊 Service Accounts

📊 No Logon in Required Timeframe

📊 No Password Reset in Required Timeframe

📊 Average Active Time of Leaver Accounts

📊 Active Leaver Accounts

📊 Privileged Access

📁 Perimeter Logging and Analysis

▼ 📁 Security Skills Training

▼ 📁 Phishing Training

📊 Clicked URL

📊 Clicked URL Again

📊 Test Coverage

📊 Active Campaigns

📊 Emails Sent

▼ 📁 Data Protection

📁 Data Loss Prevention

▼ 📁 Detect

▼ 📁 Vulnerability Management

▼ 📁 Key Insights and Actions

📊 Key Metrics: Vulnerability Scan Coverage

📊 Key Metrics: Vulnerability Performance KPI

📊 Key Metrics: Vulnerability Technical Debt

📊 Key Metrics: Backlog Outlier Devices

▼ 📁 Patch Management

📊 Deployed Patches in Breach of SLA

📊 Devices Failing Patching SLA

📊 Vulnerability Exposure

📊 Vulnerability Diagnostics

📊 Vulnerability SLA Report

▼ 📁 Application Security

📊 Application Security

📊 Application Security Program Manager

▼ 📁 Malware Defences

📊 AV SLA Report

📊 AV Threat Report

📊 EDR SLA Report

▼

📁 All Dashboards

📊

[Business Overview](#)

📊

Business Unit Vulnerabilities

📊

Cross-Source Coverage

📊

Key Controls Assurance

📊

Vulnerability Key Insights and Actions

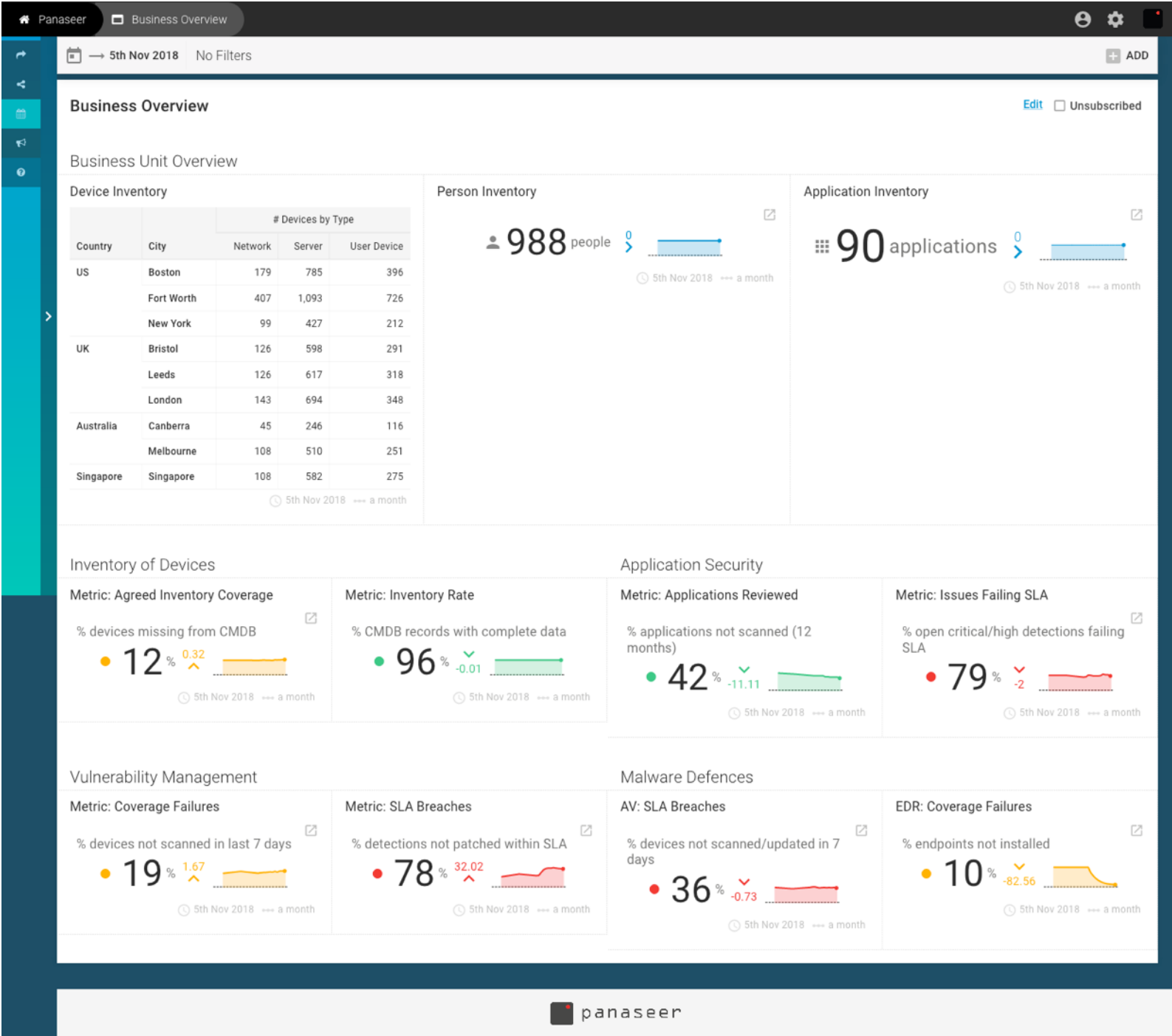
Inventories

Search for any entity

Search

>

📁 All Inventories



Inventory of Devices

Metric: Agreed Inventory Coverage

% devices missing from CMDB

12%

0.32

5th Nov 2018 a month

Metric: Inventory Rate

% CMDB records with complete data

96%

-0.01

5th Nov 2018 a month

Application Security

Metric: Applications Reviewed

% applications not scanned (12 months)

42%

-11.11

5th Nov 2018 a month

Metric: Issues Failing SLA

% open critical/high detections failing SLA

79%

-2

5th Nov 2018 a month

Vulnerability Management

Metric: Coverage Failures

% devices not scanned in last 7 days

19%

1.67

5th Nov 2018 a month

Metric: SLA Breaches

% detections not patched within SLA

78%

32.02

5th Nov 2018 a month

Malware Defences

AV: SLA Breaches

% devices not scanned/updated in 7 days

36%

-0.73

5th Nov 2018 a month

EDR: Coverage Failures

% endpoints not installed

10%

-82.56

5th Nov 2018 a month

panaseer

Continuous Controls Monitoring

