



OPSWAT[®]

Trust no file. Trust no device.

OPSWAT の戦略とグローバル最新動向

Benny Czarny, CEO

October 2018

About OPSWAT

8 global offices
180+ employees
24/7 support

1,200+ customer accounts
300+ technology partners
Founded in 2002



Our Vision

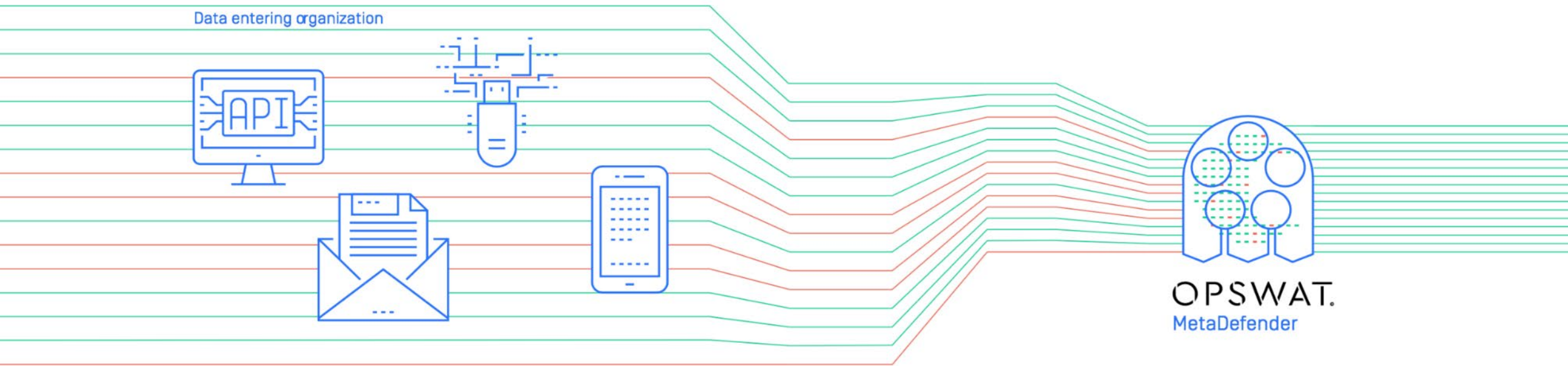
A digital world that is private, immune to malware, and protected against cyberattacks

Our Mission

Protect organizations from content and device based threats
in a simple, elegant, usable, and effective way

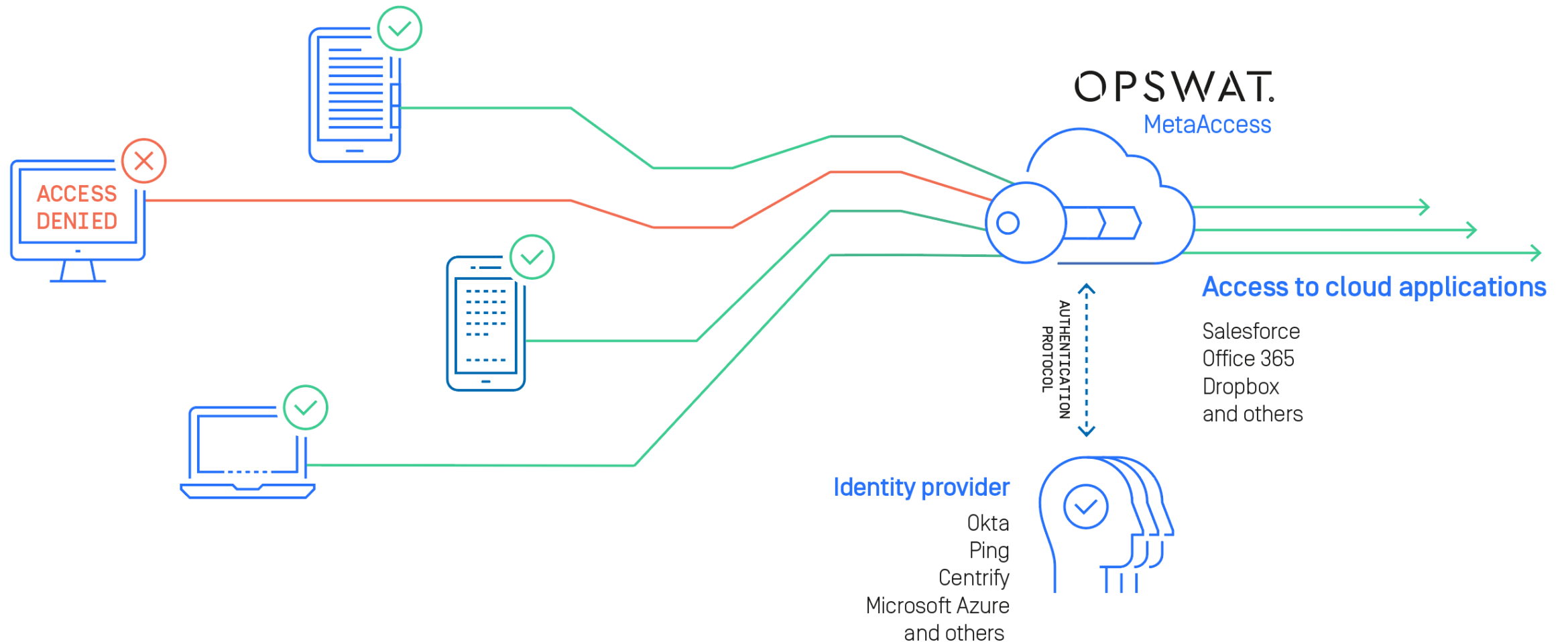
MetaDefender®

Protect organizations from content based threats



MetaAccess[®]

Protect organizations from device based threats



OPSWAT Security Offerings

- Threat Prevention
- Data Loss Prevention
- Threat Detection
- Endpoint Compliance
- Endpoint Vulnerability Management
- Secure Access

Over 1,200 Customers Worldwide

GOVERNMENT



DEFENSE



ENERGY



FINANCE



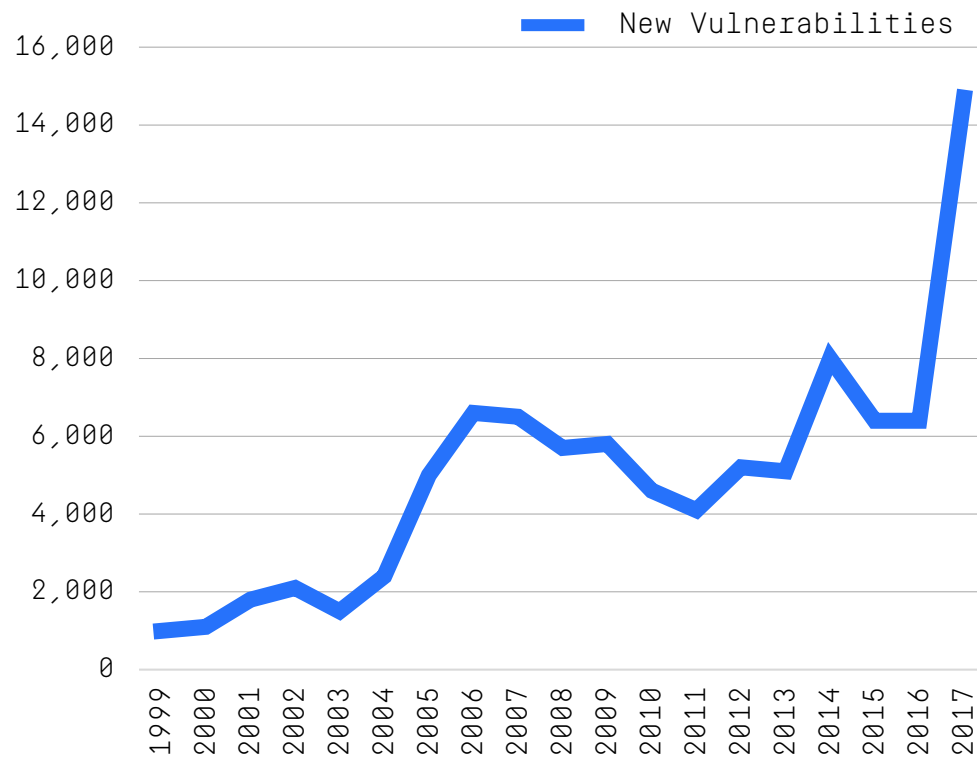
MANUFACTURING



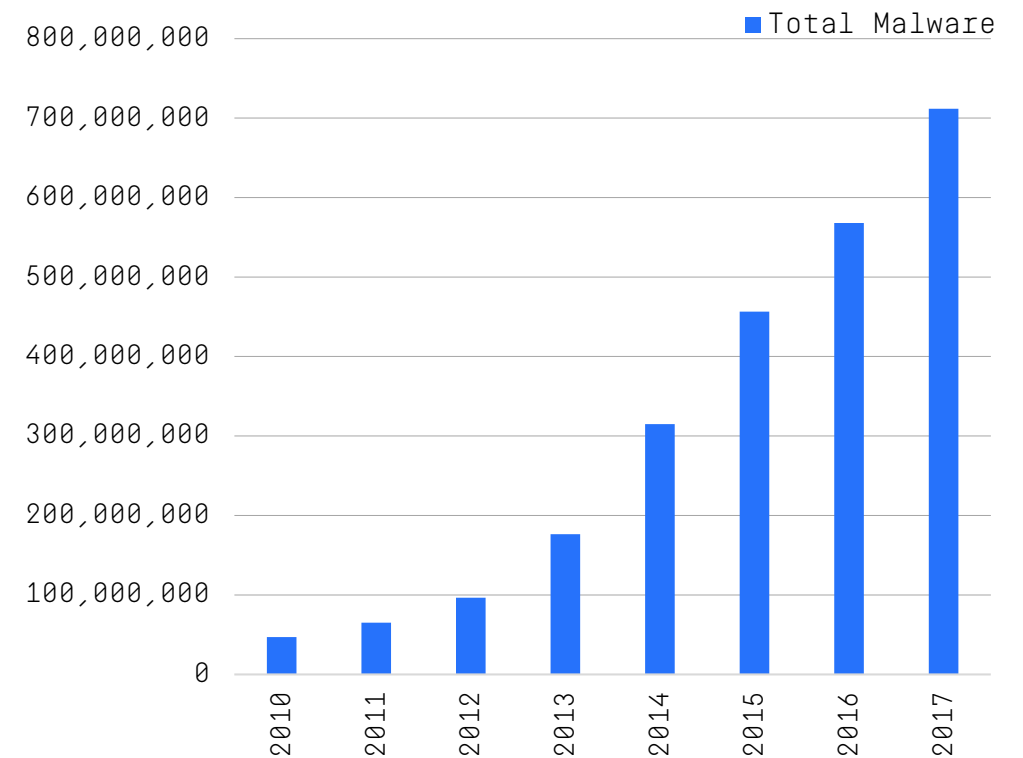
TECHNOLOGY



Growth in Malware and Vulnerabilities

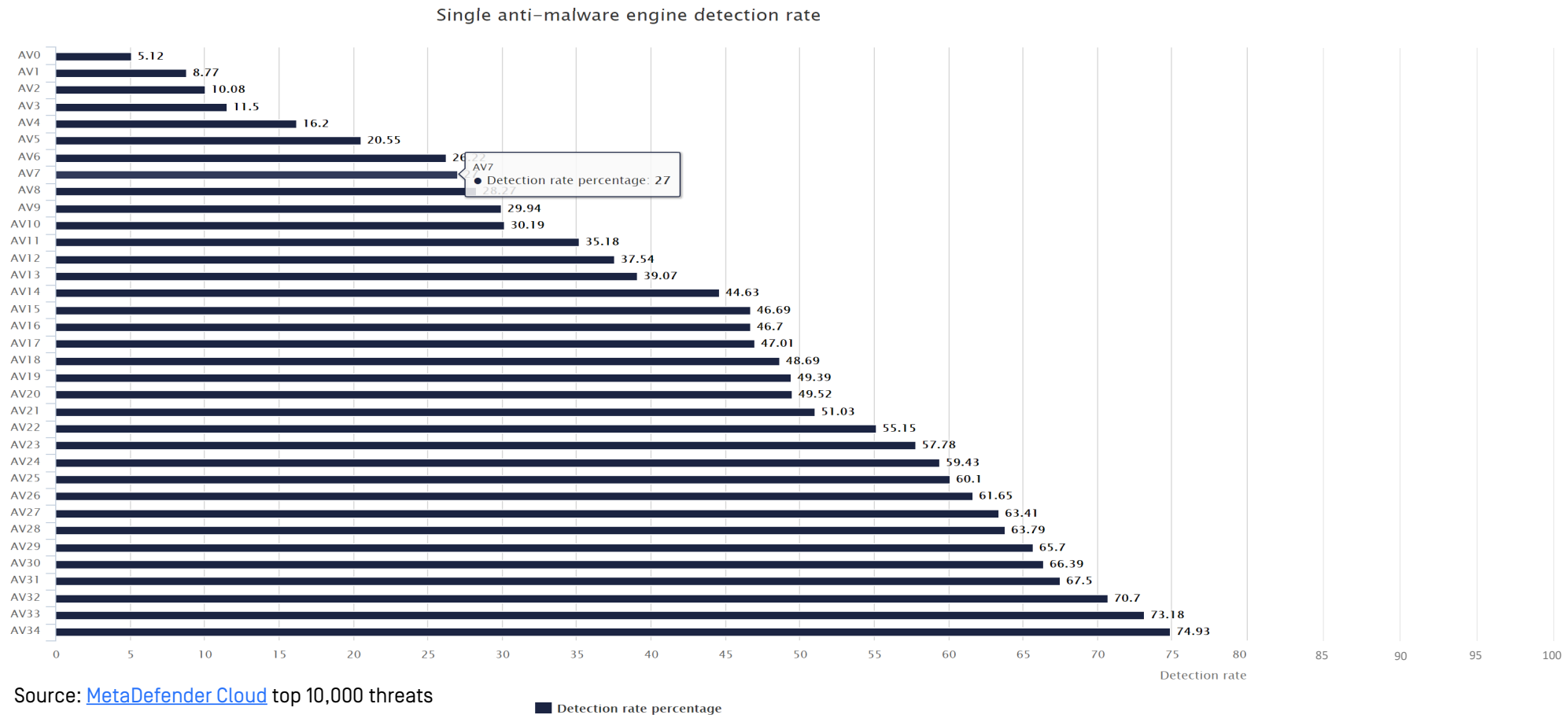


Source: cve.mitre.org



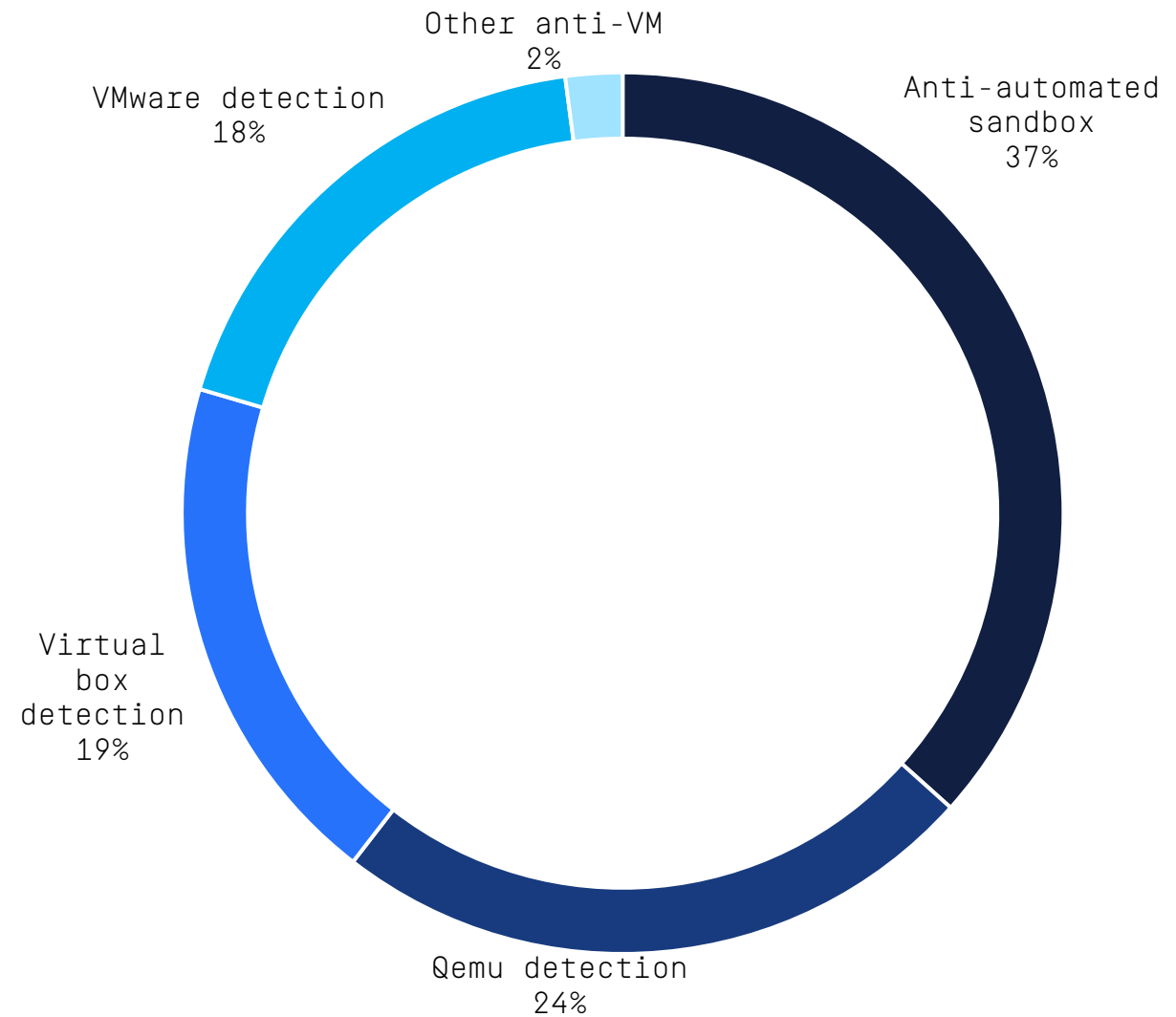
Source: [AV-Test](https://av-test.com)

Single anti-malware and next gen engines provide limited detection



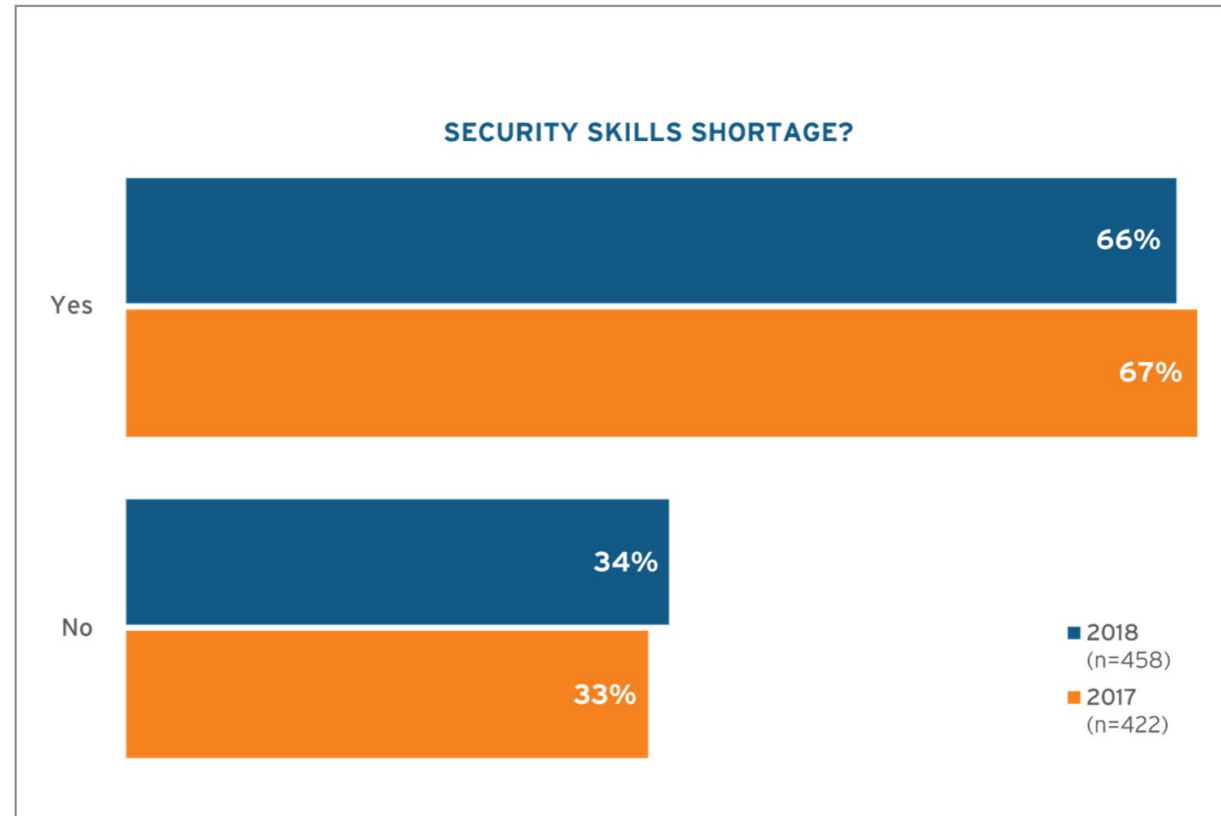
WHY OPSWAT

Malware Evading Sandbox



Source: McAfee

Shortage in IT Security Professionals

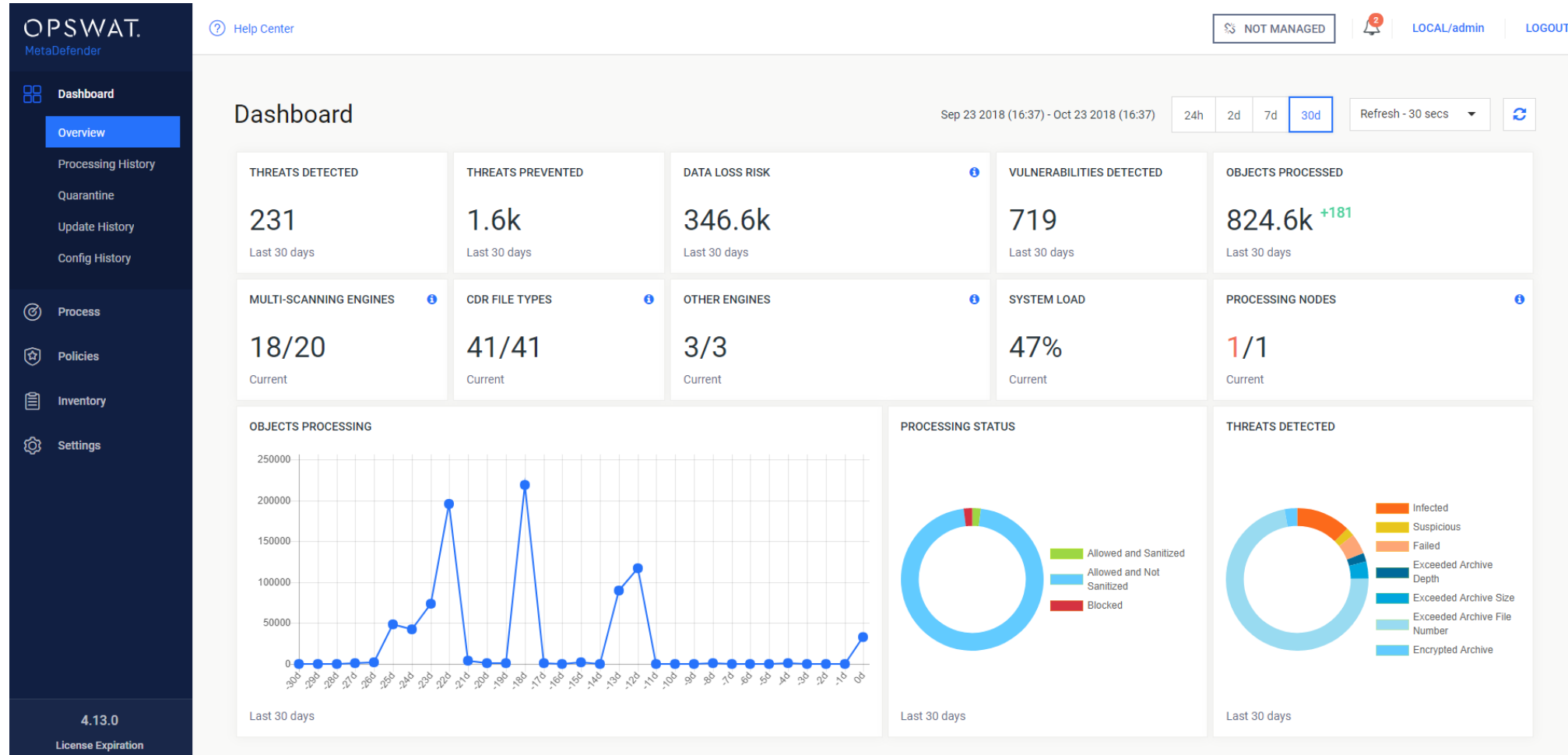


Source: 451 Research, LLC

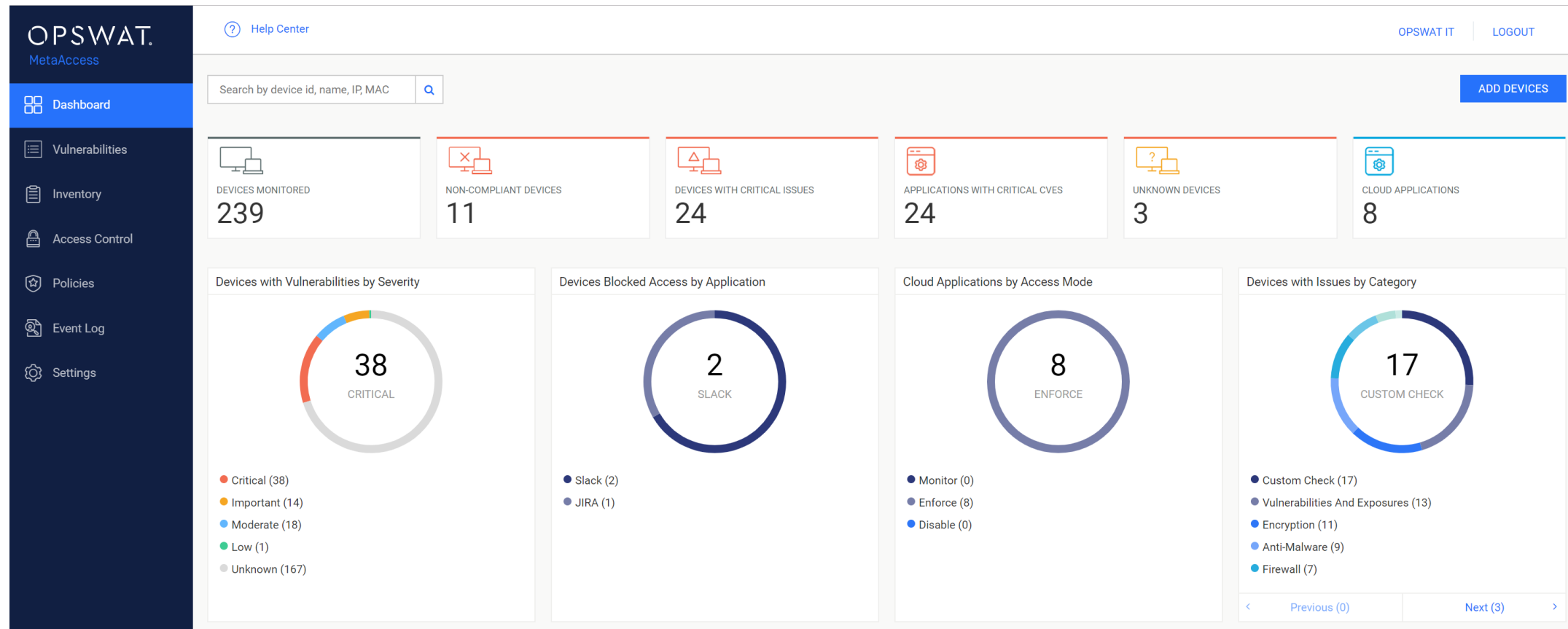
OPSWAT Security Portfolio

Solution	Security platforms for developers	Web portal protection	Malware analysis & forensic tools	Protect critical networks	Data storage security	Web browsing security	2 nd layer defense for email	Endpoint vulnerability	Endpoint compliance	Secure access
Product	MetaDefender API	Kiosk	Vault	ICAP Server	Email Security	MetaDefender Cloud	MetaAccess			
Deployment	Cloud			On-premise			Air-gap			
Technology	Data sanitization [CDR]	Multi-scanning	Vulnerability assessment	Data loss prevention	Big data security & threat intelligence	Endpoint security & compliance	Automatic application cleanup	Cloud access control		

MetaDefender



MetaAccess



MetaAccess

OPSWAT.
MetaAccess

Dashboard

Vulnerabilities

Inventory

Access Control

Policies

Event Log

Settings

Help Center

OPSWAT IT | LOGOUT

Vulnerabilities and Exposures

308 Critical | 493 Important | 746 Moderate | 161 Low | 3 Unknown1711 CVEs

Search by CVE ID

EXPORT

FILTERS

1 - 20 of 1711 CVEs

SEVERITY	CVE ID	UPDATED	OPSWAT SCORE	CVSS 2.0 SCORE	CVSS 3.0 SCORE	NO. OF DEVICES
Critical	CVE-2017-3099	Jan 5, 2018 2:31:35 AM	9.6	10	9.8	1
Critical	CVE-2017-8543	Jul 8, 2017 1:29:20 AM	9.6	10	9.8	1
Critical	CVE-2017-8464	Aug 12, 2017 1:29:06 AM	8.3	9.3	8.8	1
Critical	CVE-2017-0294	Jun 26, 2017 2:51:08 PM	8.8	9.3	7.8	1
Critical	CVE-2017-0292	Jul 8, 2017 1:29:05 AM	8.8	9.3	7.8	1
Critical	CVE-2018-5183	Aug 3, 2018 2:46:26 PM	8.3	7.5	9.8	1
Critical	CVE-2018-5089	Aug 3, 2018 4:53:59 PM	8.3	7.5	9.8	1
Critical	CVE-2018-5145	Aug 3, 2018 4:13:38 PM	8.7	7.5	9.8	1
Critical	CVE-2018-5096	Aug 7, 2018 12:46:45 PM	8.4	7.5	9.8	1

OPSWAT Global Roadmap

- Invest in more R&D
 - Triple QA team members
 - Improve products
 - Quality
 - Security
 - Documentation
 - Usability
 - Performance
 - Release new products
- Enhance training program

OPSWAT's Commitment to Japan

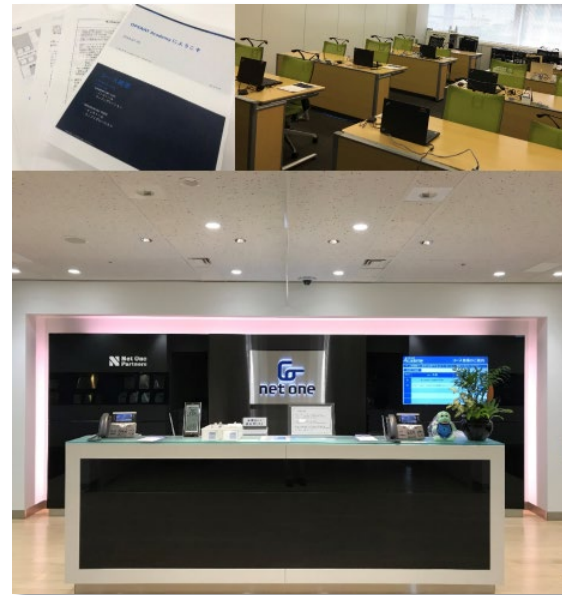
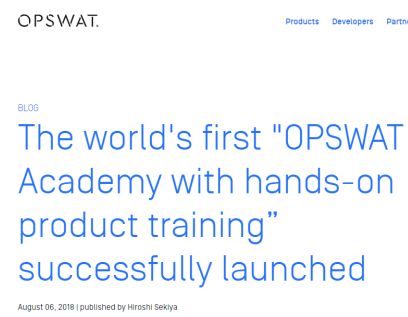
- Opened a local office
- Partnered with Net One Partners
- Worked with Net One Partners to create a local academy
- Created Japanese website
- Localized products to Japanese
- Created various marketing activities
- First to provide JTD support



OPSWAT's Commitment to Japan



Partnered with Net One Partners



OPSWAT Academy



OPSWAT Research

October 2018

Research Topics

Effectiveness of Anti-malware Engines

Effectiveness and Statistics of Data Sanitization [CDR]

Data Diode Players

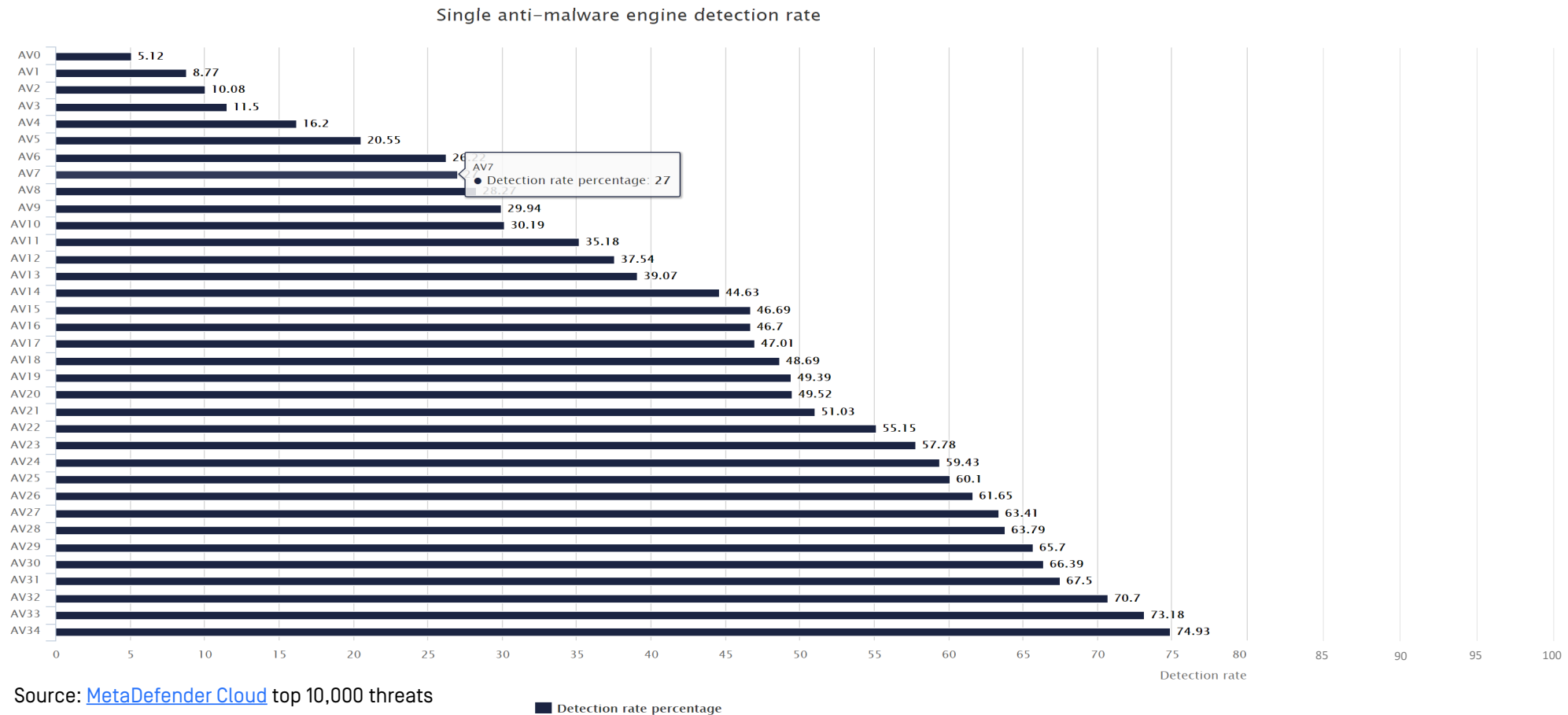
Endpoint Compliance Statistics

Data Collection and Disclaimers

- The source is MetaDefender Cloud ([MetaDefender.com](https://metadefender.com))
- Customers and end users who elect to share the data
- Over 200,000,000 binaries analyzed to produce this data
- Some reports are limited to last 90 days
- Checks were performed on Windows binary only (32 and 64 bits)
- Static analysis only

Anti-malware Engines Detection Rate

For Windows Executable Only







<https://metadefender.opswat.com/reports/sanitization#!/>

Top searched threats

	THREATS 1 - 10	11 - 20	21 - 30	31 - 40	41 - 50	Next >
Jul 30 2018 - Aug 29 2018	Detection of top 10000 threats	Trojan.Android.SmsSend.obgrtf	Trojan.W32.Agent.9545ag	Adware.Stud	Adware.Adload.CRT.Win32.544	Gen.Variant.MSGUkrypt.4
MetaDefender 4	77.90%	*	*	*	*	*
MetaDefender 8	88.60%	*	*	*	*	*
MetaDefender 12	96.37%	*	*	*	*	*
MetaDefender 16	98.29%	*	*	*	*	*
MetaDefender 20	99.43%	*	*	*	*	*
MetaDefender 20+ Custom Engines	99.82%	*	*	*	*	*
MetaDefender ISV	94.86%	*	*	*	*	*
Commercial MetaDefender Cloud	95.88%	*	*	*	*	*

Jul 30 2018 - Aug 29 2018

77.90% 88.60% 96.37% 98.29% 99.43% 99.82% 94.86% 95.88%

Detection of top 10000 threats

Trojan.Android.SmsSend.dzgnrf

Trojan/W32.Agent.954598

Adware.Stud

Adware.AdLoadCRT.Win32.544

Gen:Variant.MSILKrypt.4

Trojan/Generic.Generic

Andr/PomClk-AS

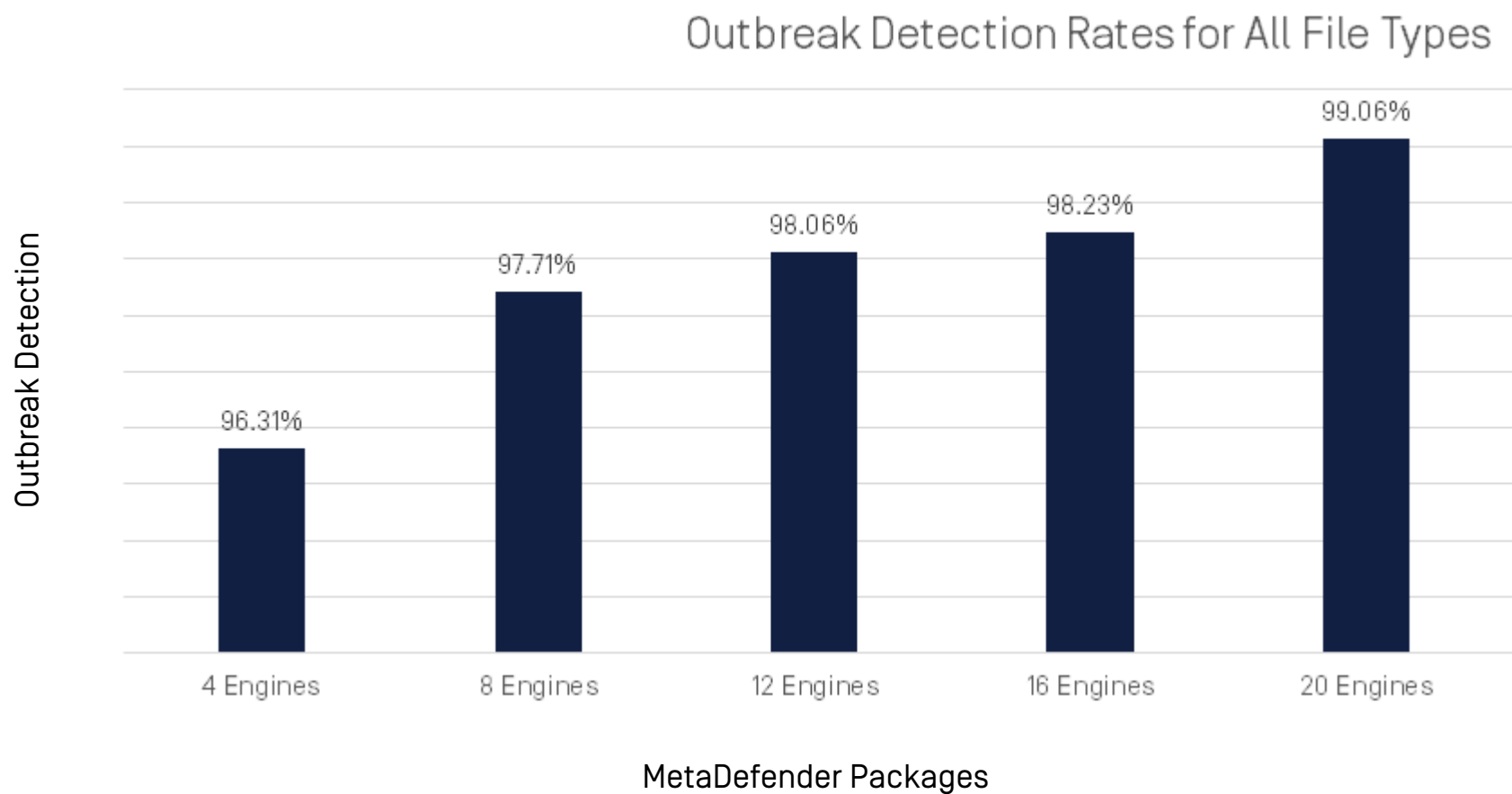
Andr/HiddenAp-y

Downloaded At: 11:53 11 September 2009

TScope.Tmi-

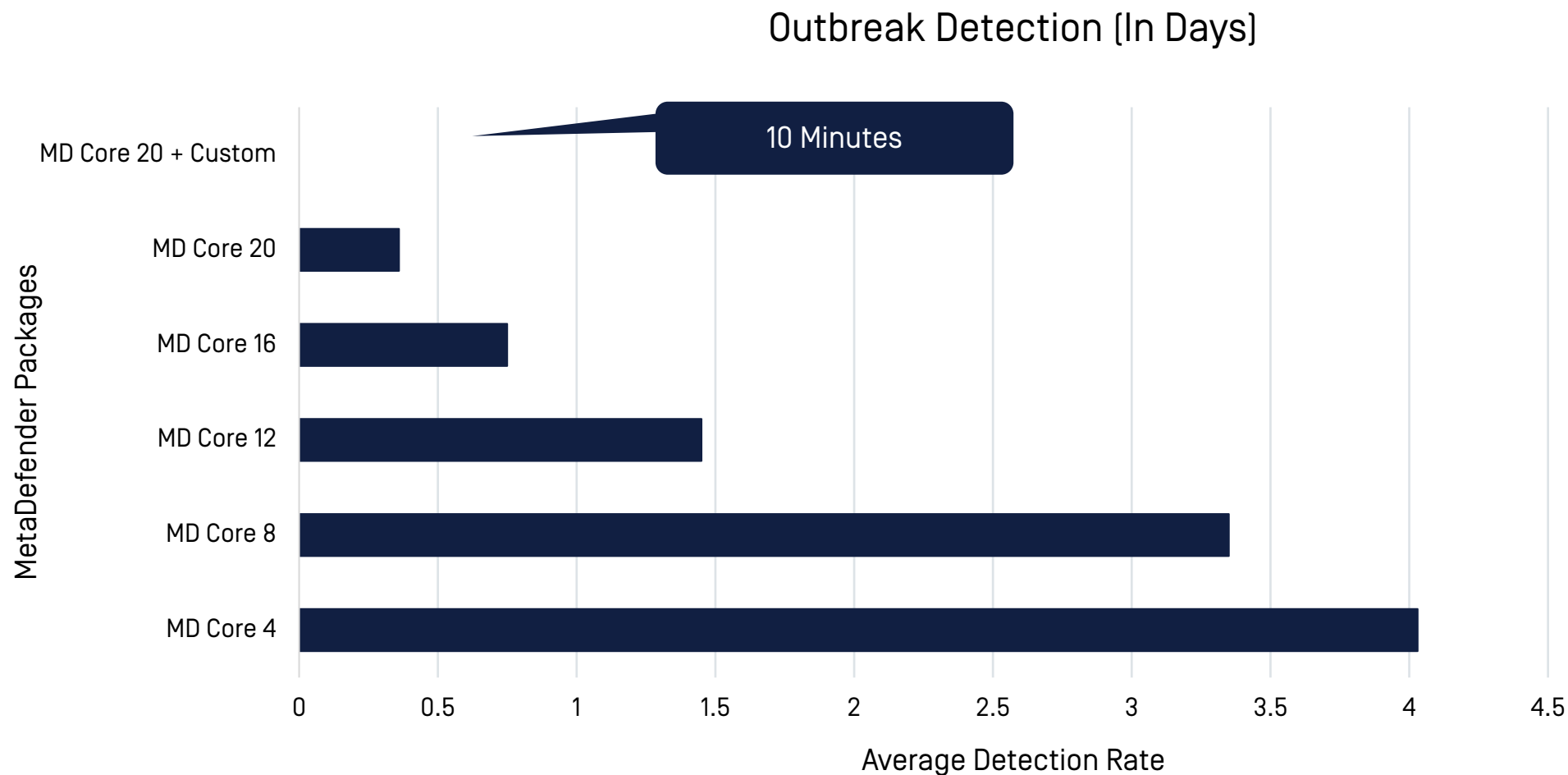
MetaDefender Packages

How Effective is MetaDefender Multi-scanning Threat Detection?



MetaDefender Packages

How Fast Do MetaDefender Engine Packages Detect Zero-Day Threats?



Research Topics

Effectiveness of Anti-malware Engines

Effectiveness and Statistics of Data Sanitization [CDR]

Data Diode Players

Endpoint Compliance Statistics

Data Collection and Disclaimers

- The source is MetaDefender Cloud (MetaDefender.com)
- Customers or end users who elect to share the data
- Over 2,000,000 binaries analyzed to produce this data
- Data reflects last 90 days of analysis

MetaDefender Cloud Scan Results

https://metadefender.opswat.com/reports/sanitization#!/

OPSWAT.

MetaDefender Cloud

Search or scan a CVE, file HASH, IP address

ANALYZE

SIGN IN

XLS

FinancialStatements.xls

MALWARE NAME

Trojan[Downloader]/MSOffice.Agent.kom

INFECTED FILE

18 / 35

NO THREATS FOUND

0 / 35

DOC

N010142018.doc

MALWARE NAME

Trojan-Downloader.VBA.Agent

INFECTED FILE

11 / 35

NO THREATS FOUND

0 / 35

PDF

DOC53409.pdf

MALWARE NAME

Trojan-Downloader.PDF.Agent

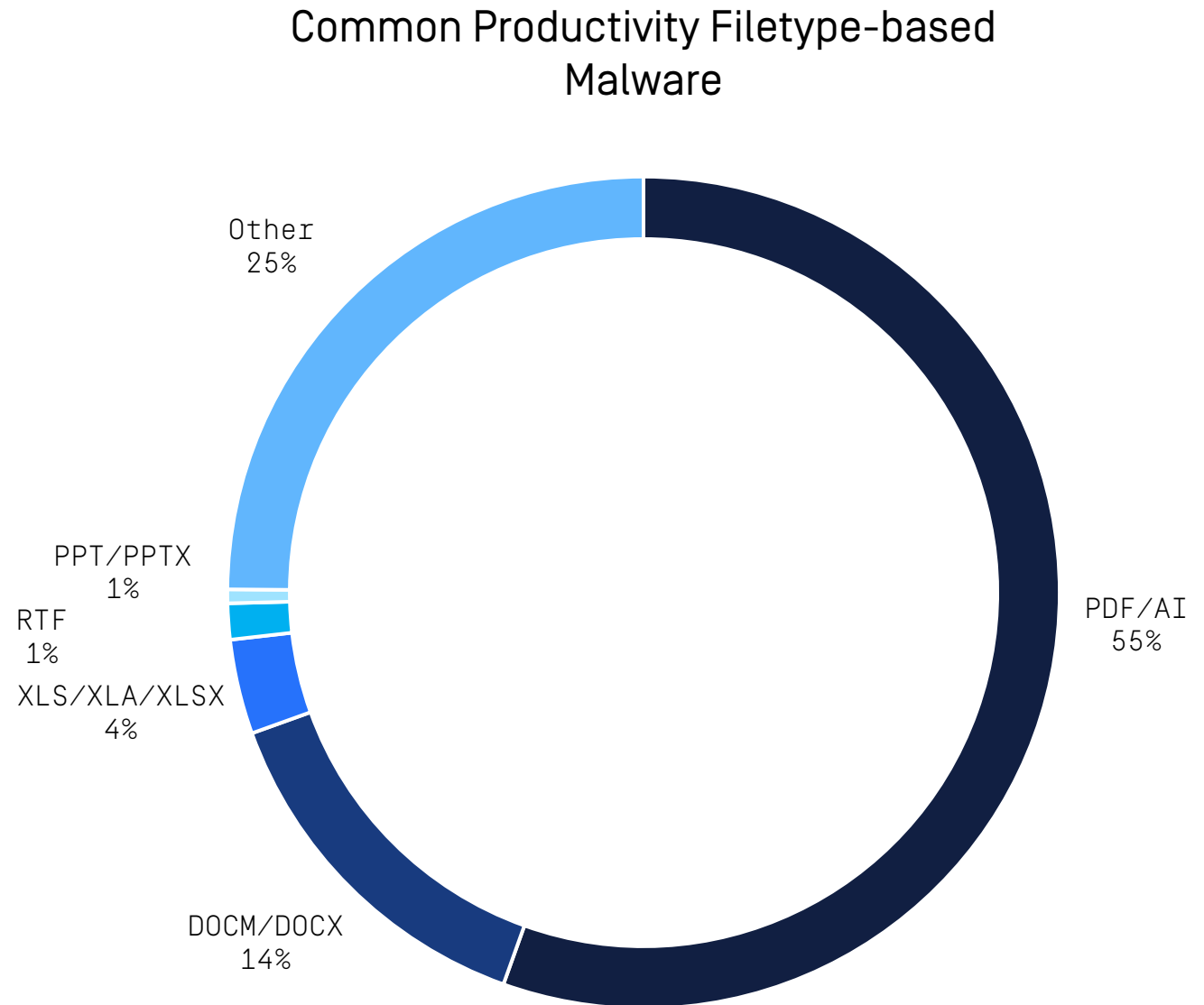
INFECTED FILE

5 / 35

NO THREATS FOUND

0 / 35

Common Productivity Filetype-based Malware



Recent Commonly Infected Attachment Names

test.doc / tester.doc / test.docx	287
payroll.xlsx / payroll.xls	210
template.pdf / template.doc	131
Inquiry.doc	98
pi.doc	66
⋮	⋮
invoice	21

Research Topics

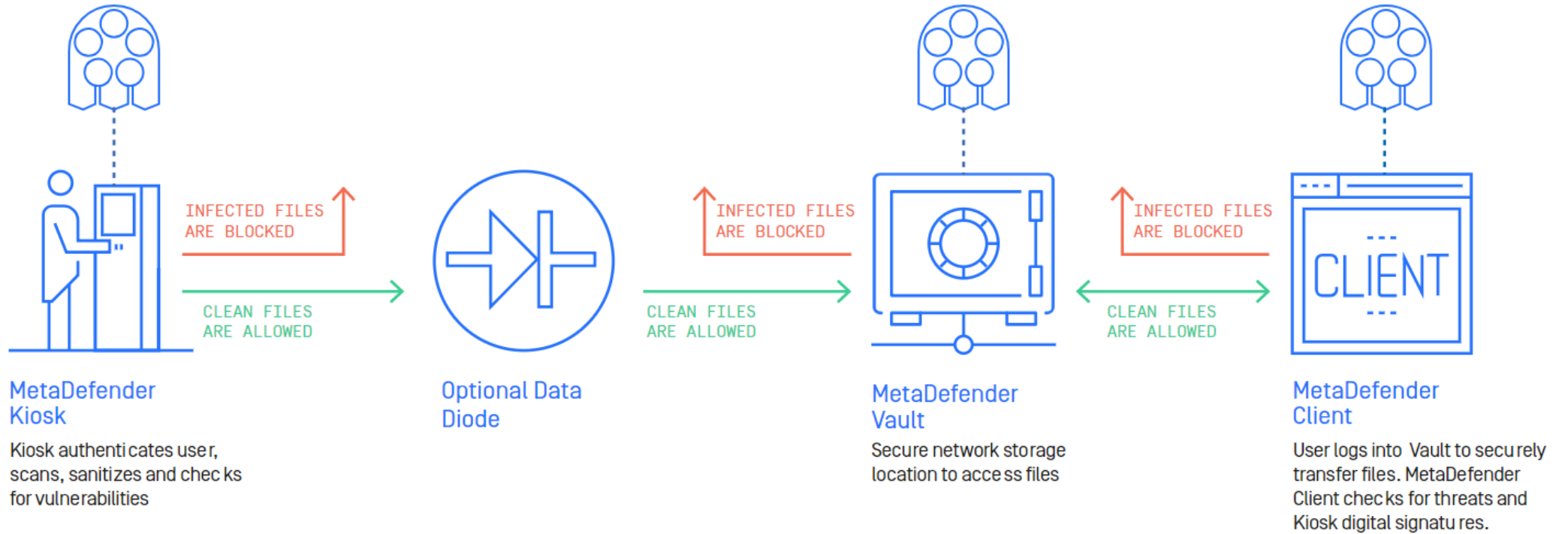
Effectiveness of Anti-malware Engines

Effectiveness and Statistics of Data Sanitization [CDR]

Data Diode Players

Endpoint Compliance Statistics

Secure Data Workflow



Data Diode Vendor Comparison Guide

Vendor	arbit	snc <small>SIERRA NEVADA CORPORATION®</small>	advenica	somerdata	BAE SYSTEMS
Website Link	Arbit Data Diode	Sierra Nevada Corporation	Advenica SecuriCDS Data Diode	AROW Data Diode	BAE Systems - Detica
Products/SKUs	<ul style="list-style-type: none">▪ Arbit Data Diode▪ Arbit TRUST Gateway	<ul style="list-style-type: none">▪ Binary Armor Network▪ Data Guard	<ul style="list-style-type: none">▪ DD1000IUIO▪ DD1000A	<ul style="list-style-type: none">▪ Single▪ Dual▪ High-availability in Standard Gated Mode or Optional Streaming Mode	<ul style="list-style-type: none">▪ Not specified
Weight	22 lbs	1 lb	Not specified	Not specified	2.2 lbs
Physical Dimensions	19" x 10 x 19"	5.3" x 3.2" x 1"	437 x 504 x 44 mm 216 x 167 x 44 mm	341 x 444 x 44 mm	2.5" x 4.6" x 6.8"
Diode Technology	Optical	Unidirectional Software	Optical	Optical	Optical

Research Topics

Effectiveness of Anti-malware Engines

Effectiveness and Statistics of Data Sanitization [CDR]

Data Diode Players

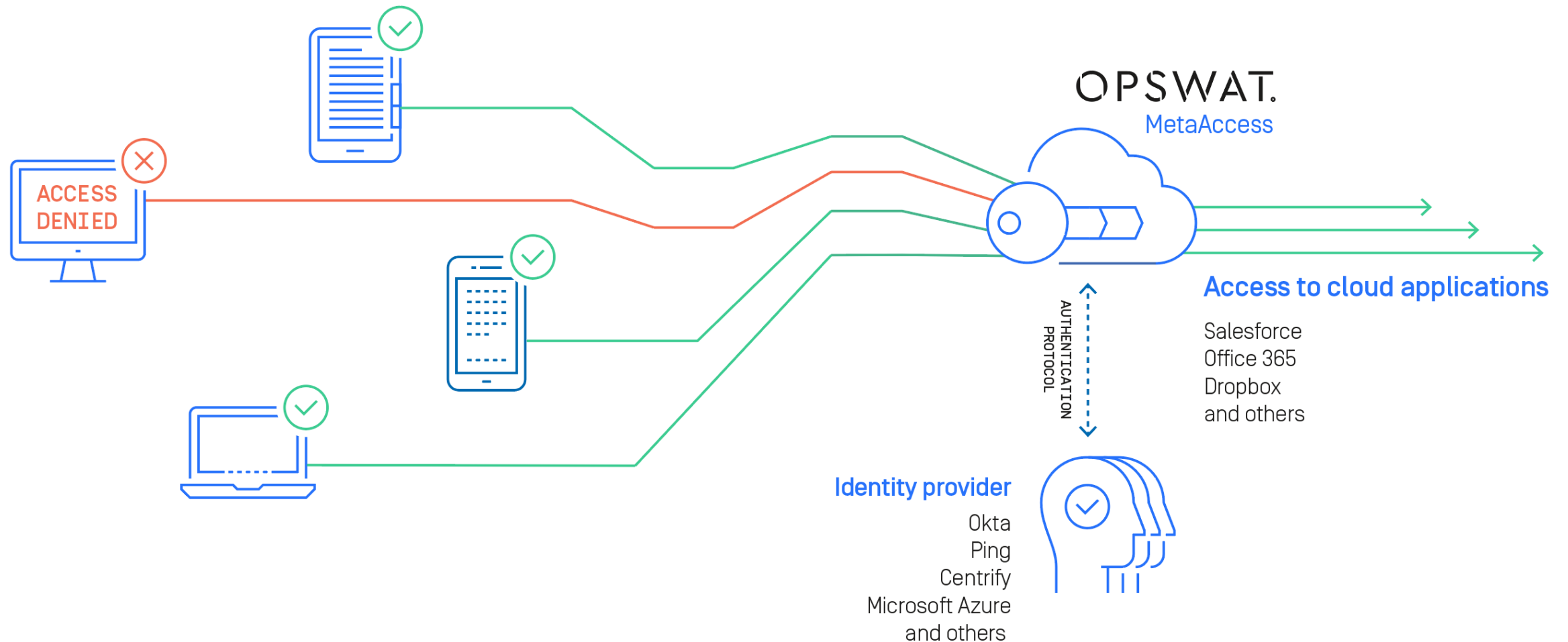
Endpoint Compliance Statistics

Data Collection and Disclaimers

- Source of the data is MetaAccess
- Customers or end users who elect to share the data
- Over 100,000 random endpoint analyzed to produce this data

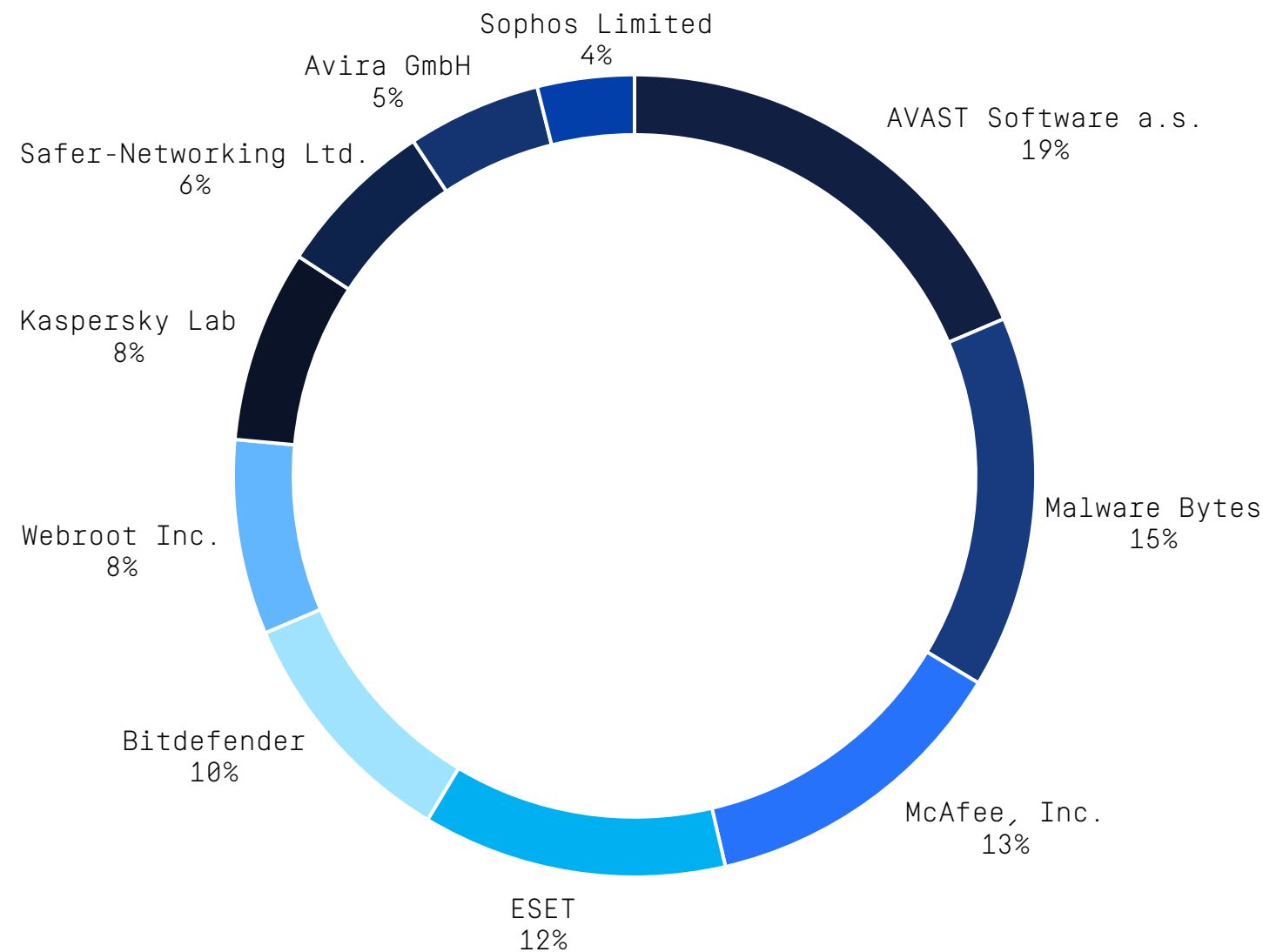
MetaAccess[®]

Protect organizations from device based threats



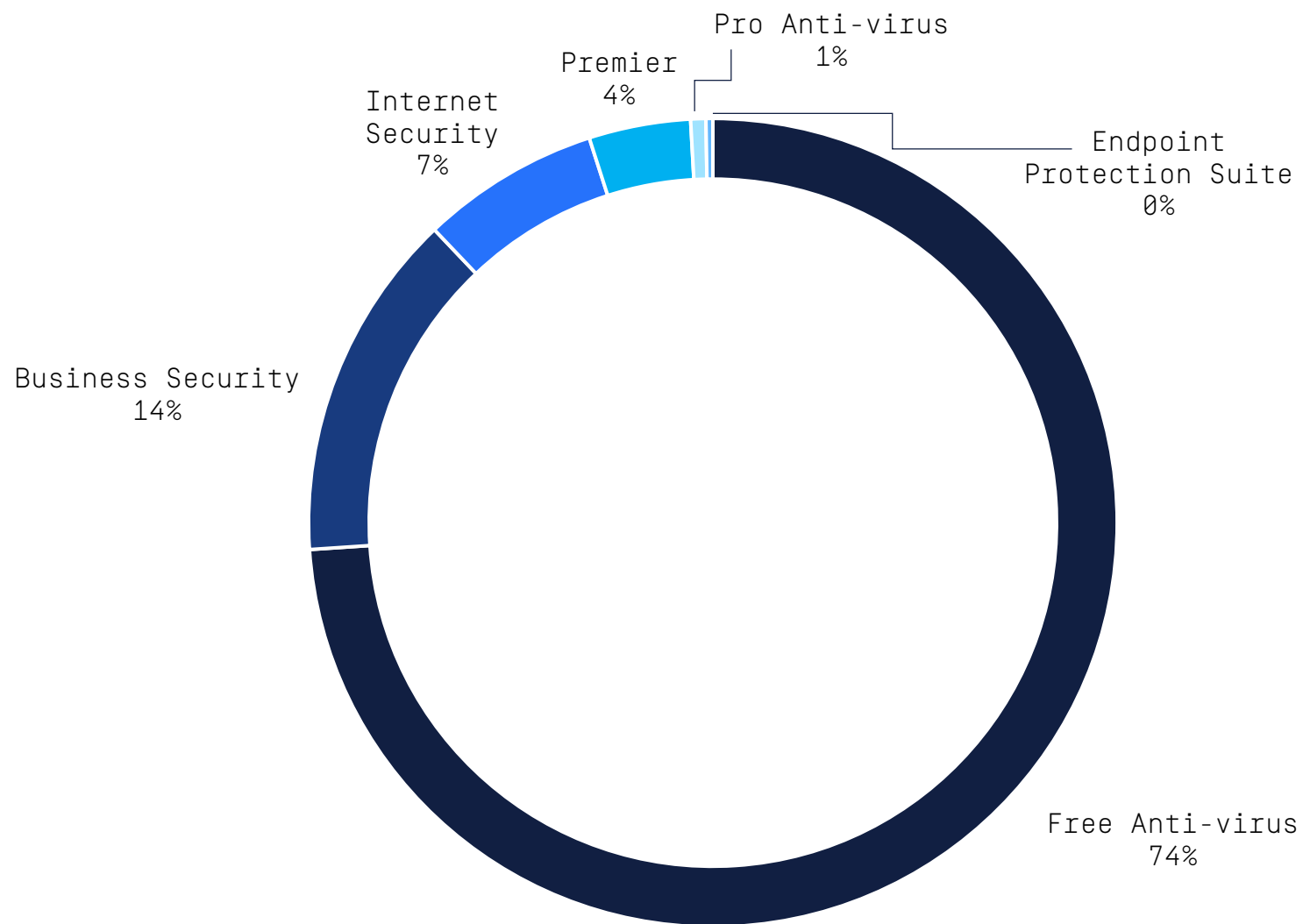
Market Share Report

September 2018 Vendor Comparison



Market Share Report

AVAST Software a.s. [September 2018]

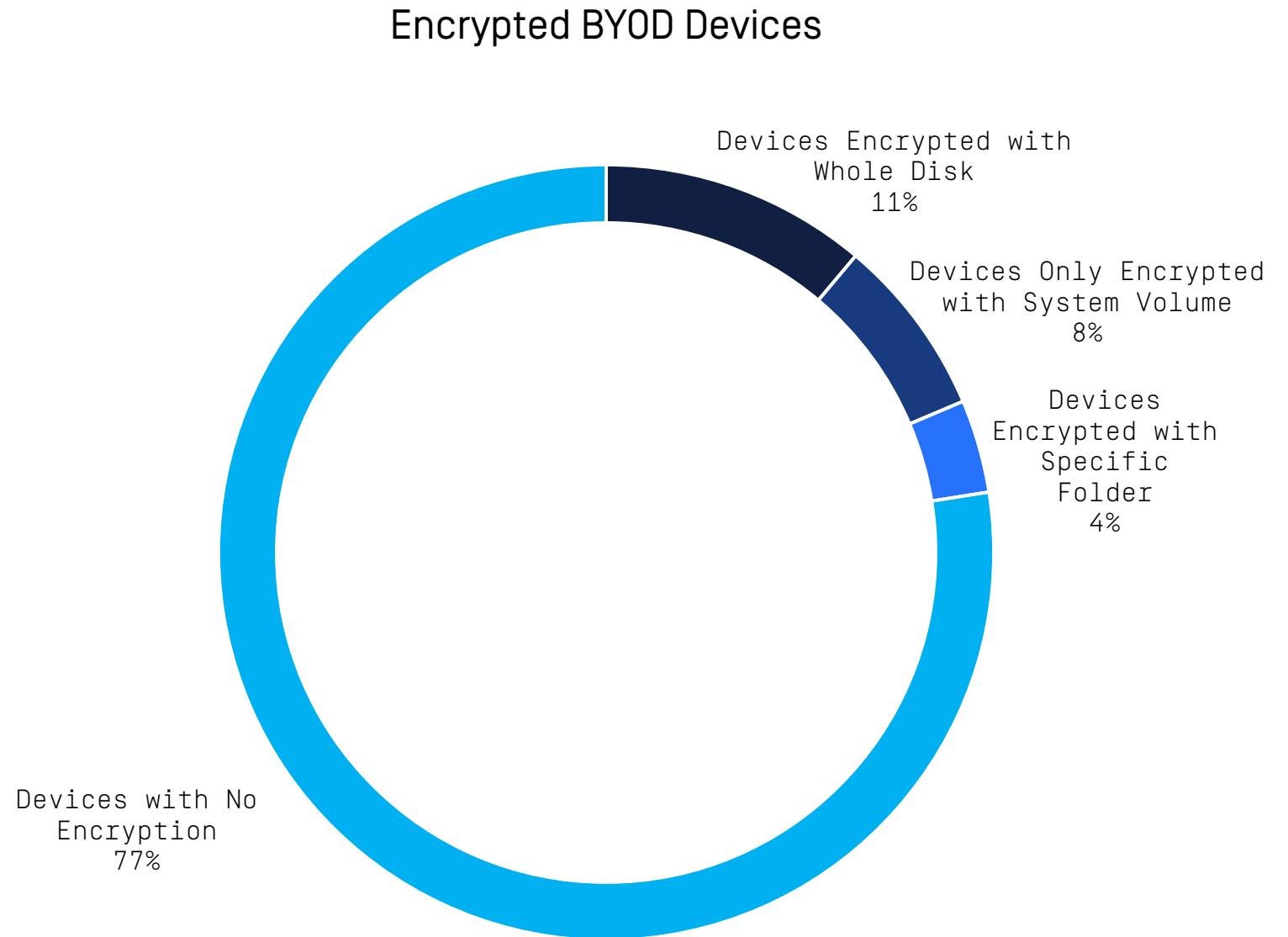


High Risk Vulnerabilities

Top Applications

CVE ID	Attack Vector	Vendor	Product	Version	Risk Level
CVE-2017-0199	Execute arbitrary code via a crafted document	Microsoft Corporation	Microsoft Office	2012 ~ 2016	11.43%
CVE-2017-6984	Execute arbitrary code via a crafted web site	Apple Inc.	iOS system, iTunes, Safari	iOS < 10.3.2 Safari < 10.1.1 iTunes < 12.6.1	7.85%
CVE-2018-5159	Integer overflow resulting in out-of-bounds writes	Mozilla Corporation	Firefox, Thunderbird	Firefox < 60 Thunderbird < 52.8	7.20%
CVE-2017-8527	Allow remote code execution due to improper memory handling	Microsoft Corporation	Microsoft Lync, Office, Silverlight	Lync 2013 Office 2012 ~ 2014 Silverlight 5.x	6.98%
CVE-2017-8669	Execute arbitrary code in the context of the current user due to IE improperly handling objects in memory	Microsoft Corporation	Internet Explorer	IE 11	6.31%

Encrypted BYOD Devices



Thank you