Advanced Reporting Tool

Getting Started Guide

Revision Date: December 2020

a WatchGuard brand

About This Guide

The *Panda Advanced Reporting Tool Getting Started Guide* provides an introduction to the Panda Advanced Reporting Tool.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 12/14/2020

Copyright, Trademark, and Patent Information

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an/if and when available basis. WatchGuard, the WatchGuard logo, AuthPoint, Panda Security are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All trademarks or trade names mentioned herein, if any, are the property of their respective owners. Complete copyright, trademark, and licensing information can be found in the Copyright and Licensing Guide, available online at http://www.watchguard.com/help/documentation/.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by over 18,000 security resellers and service providers to protect 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

How to Use This Guide **4**

Identify Security Incidents **6**

Key Security Indicators 7

Detailed Information 10

Manage Misuse of Corporate Networks and Applications **14**

IT Applications 15

Bandwidth-consuming Applications 18

Special Applications and Tools 19

Example: Monitor Microsoft Operating System Use 23

Manage Access to Critical Business Information **25**

Outbound Network Traffic 26

Bandwidth Consumers 28

Data Files Accessed 30

Real-time Alerts **31**

Configure Real-time Alerts 32

Example: Create Alerts for RDP Sessions 34

Appendix: Sample SQL Query Text **36**

How to Use This Guide

This *Getting Started Guide* provides an introduction to the Panda Advanced Reporting Tool. The Advanced Reporting Tool (ART) is available from the Adaptive Defense 360 interface and generates security intelligence data. It includes tools to detect and analyze security threats, as well as determine what network users do with their computers, such as application installation and execution, and bandwidth usage. ART identifies applications that have vulnerabilities which latest generation malware could exploit.

The ART preconfigured dashboards provide key indicators, search options, and default alerts for these functional areas:

- Security Incidents — Shows malware activity across the network and related information about malware execution in endpoints
- Application Control — Offers detailed information about the installed applications that run on your users' computers
- Data Access Control — Displays information about data flows in your network so you can detect data leaks and theft

To illustrate the power and flexibility of ART, this guide describes the features in each functional area.

For detailed information on the Advanced Reporting Tool, see the *Advanced Reporting Tool Administration Guide*.

Document Conventions

This document uses these formatting conventions to highlight specific types of information:

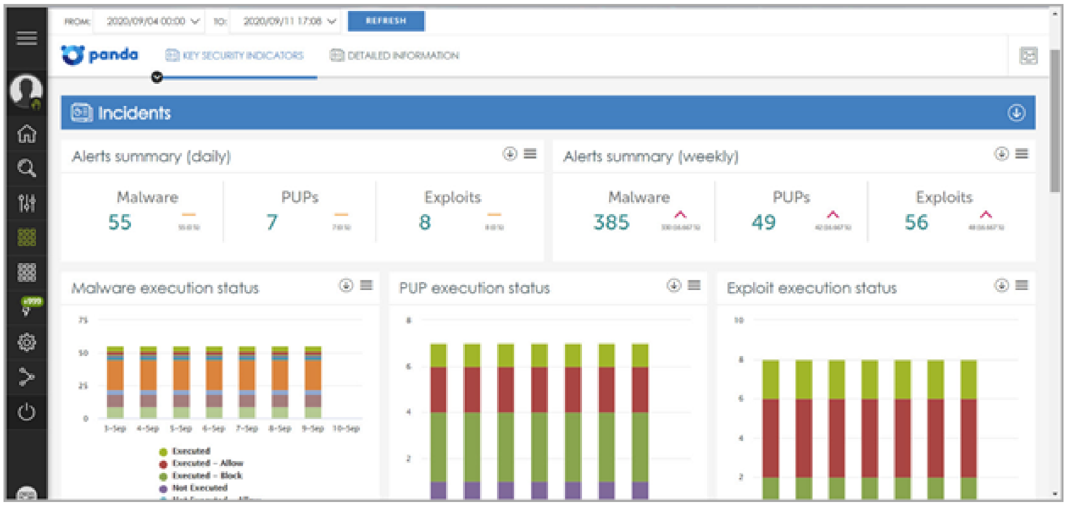
This is a recommended practice. It highlights steps or actions that WatchGuard recommends you take.

ⓘ This is a note. It highlights additional information.

ⓘ This is a caution. Read carefully. There is a risk that you could lose data, compromise system integrity, or impact device performance if you do not follow instructions or recommendations.

Identify Security Incidents

The Security Incidents dashboard enables you to analyze malware activity on user computers, and generate baseline data for forensic analysis of malware incidents.



The Security Incidents dashboard shows:

- Malware, exploits, potentially unwanted programs (PUPs), and anomalous processes detected and their execution status
- Endpoints with the most infection attempts and detected malware

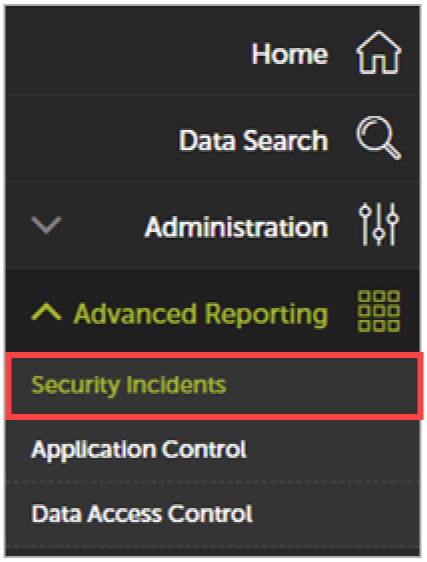
Key Security Indicators

The **Key Security Indicators** page provides an overview of malware activity on your network. This includes the types of malware, potentially unwanted programs (PUPs), and exploits detected, the endpoints affected, and whether the malware executed successfully.

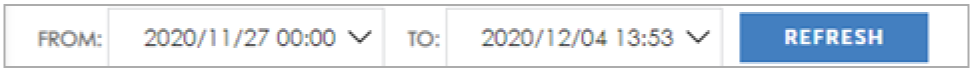
Identify Attacks and Unusual Behavior

To identify attacks:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Security Incidents**.

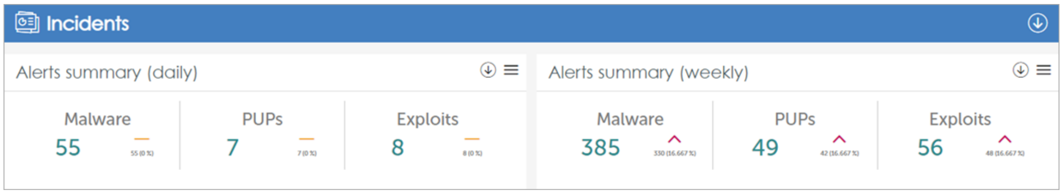


4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. On the **Key Security Indicators** page, in the **Incidents** section, review the **Alerts summary** tiles.
These summary tiles show the change in the number of detected incidents compared to the previous day (Daily) and the previous week (Weekly).



Incidents

Alerts summary (daily)

Malware 55 55 (0 %)

PUPs 7 7 (0 %)

Exploits 8 8 (0 %)

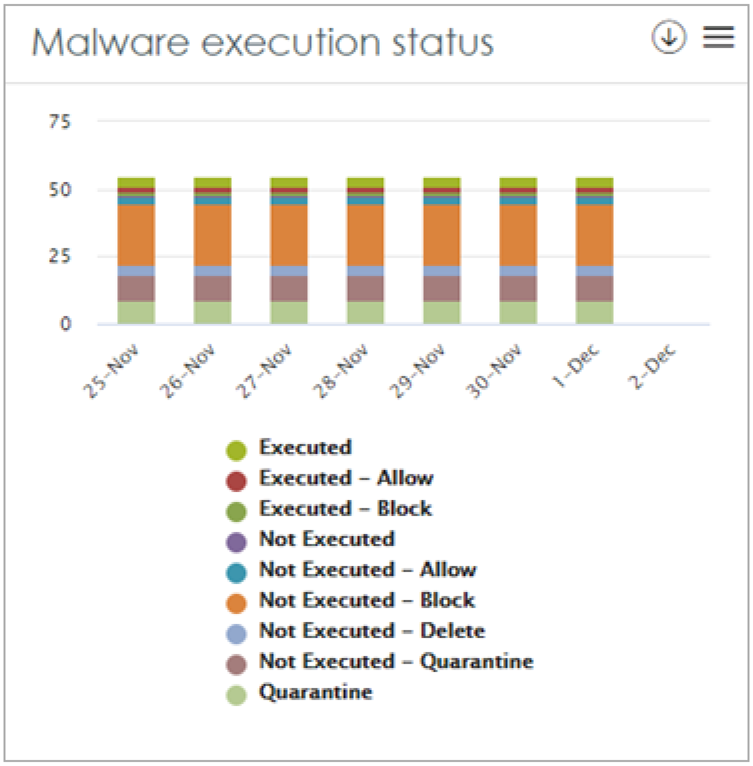
Alerts summary (weekly)

Malware 385 330 (16.667 %)

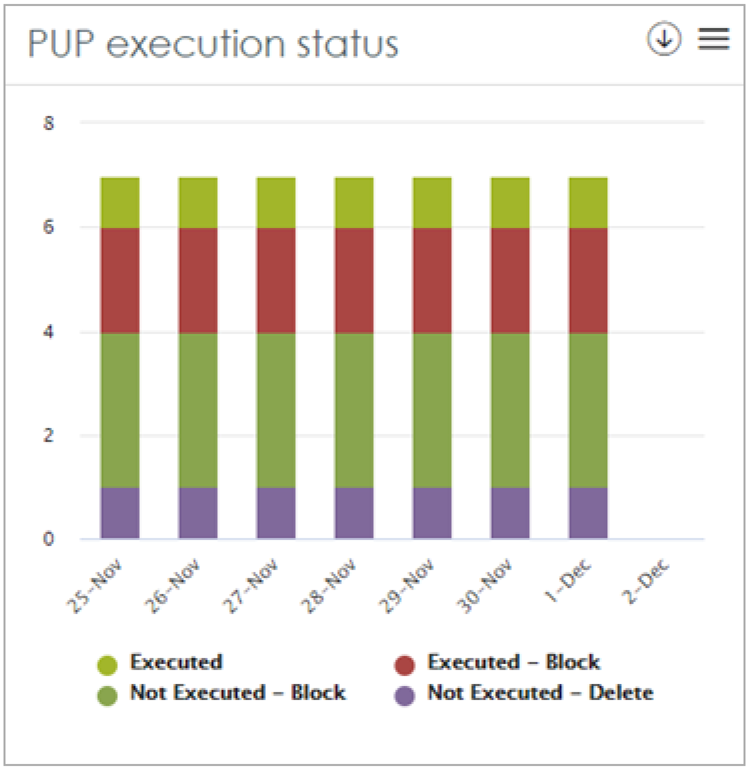
PUPs 49 42 (16.667 %)

Exploits 56 48 (16.667 %)

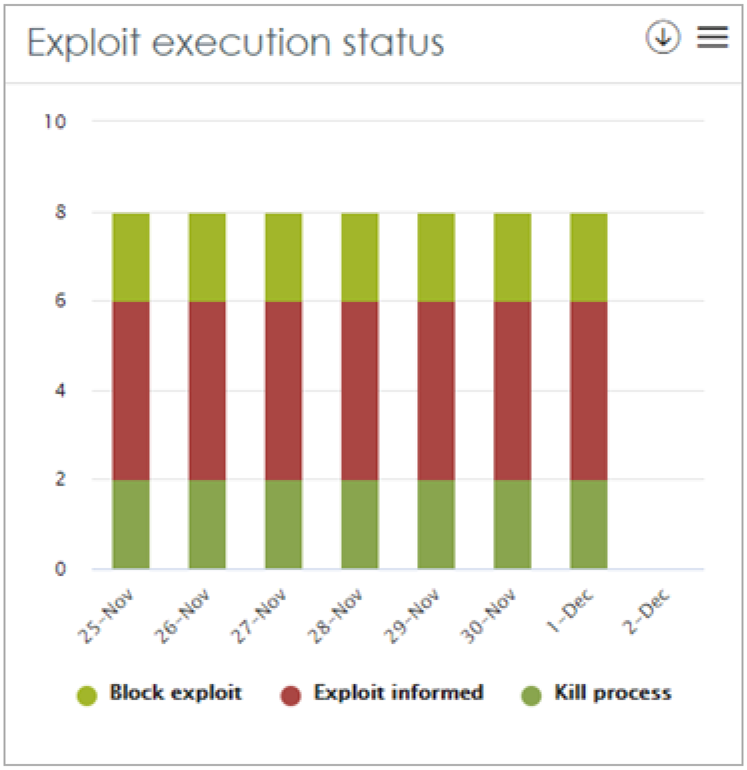
6. In the **Malware Execution Status** tile, review the chart to determine if there is any malware executed in the last 7 days that you should investigate.



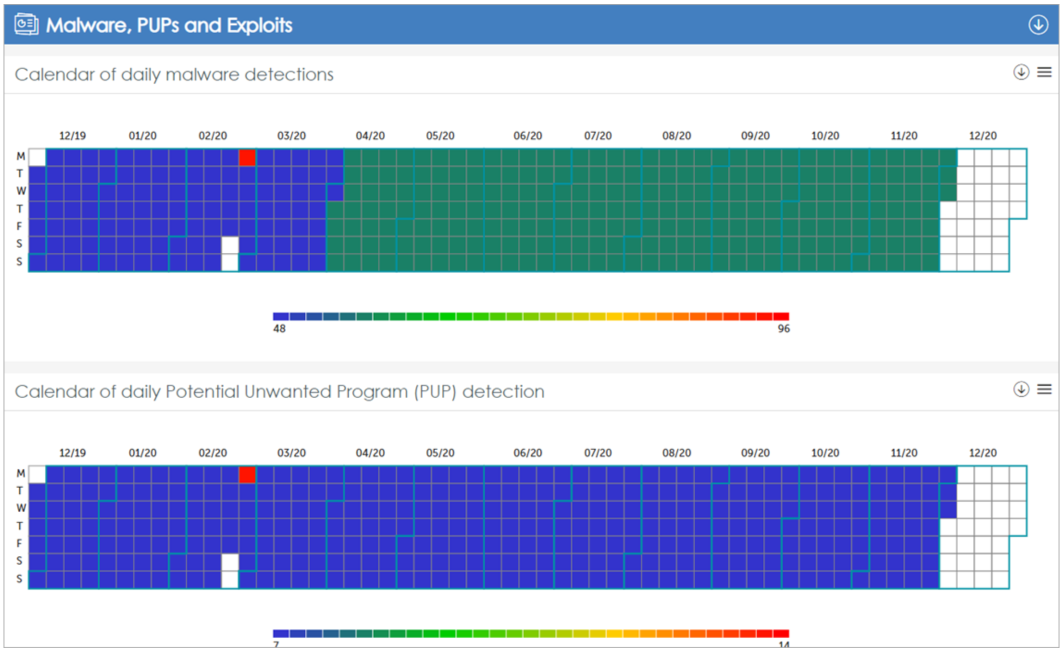
7. In the **PUP Execution Status** tile, review the chart to determine if any there are any PUPs executed in the last 7 days that you should investigate.
   PUPs can lead to data exfiltration, increased network traffic, and injected advertising. Adaptive Defense 360 provides the tools to remove PUPs and increase baseline security and integrity.



8. In the **Exploit Execution Status** tile, review the chart to determine if there are any exploits executed in the last 7 days that you should investigate.
   Hackers often exploit unpatched software. Adaptive Defense 360 includes up-to-date filters to detect possible exploits. The Patch Management tool provides insights into which security patches you can install to prevent future exploitation.

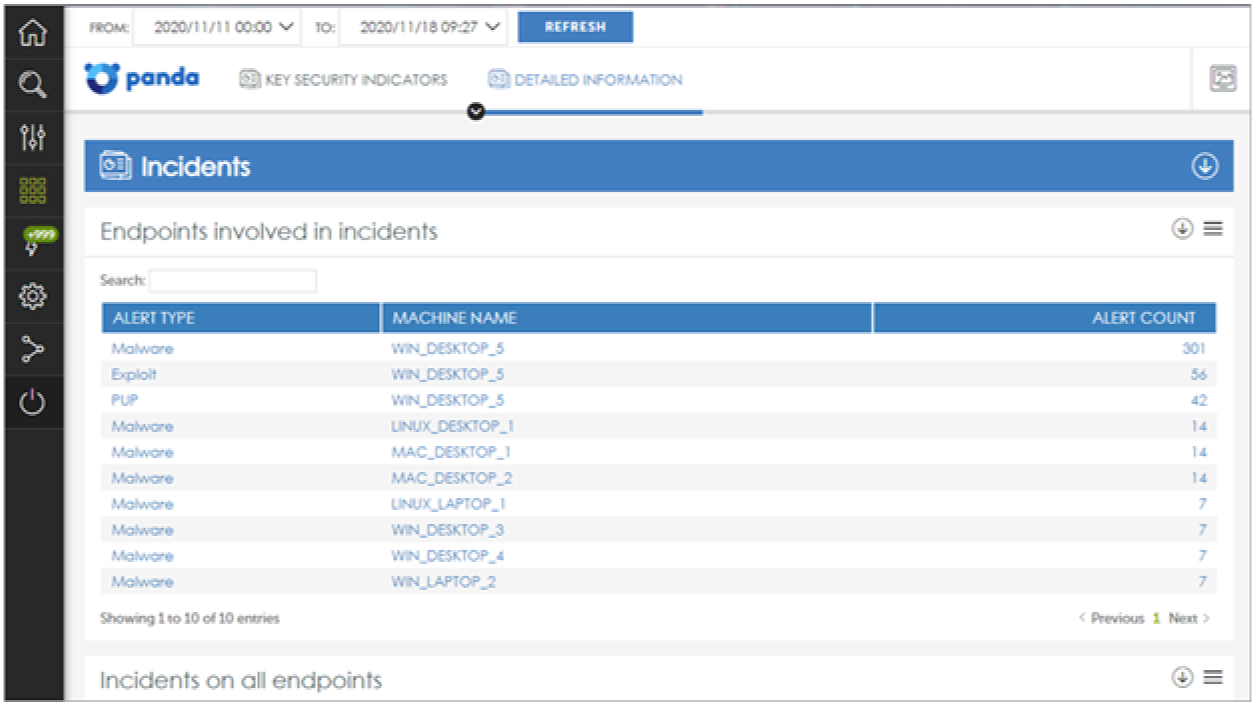


9. In the Malware, PUPs and Exploits section, review the calendars to determine if you should investigate any days.
   The Malware calendar shows the days of the year on which most malware detections occurred on the network. The Exploits calendar shows the days of the year when most exploit detections occurred on the network.



Detailed Information

On the **Detailed Information** page, you can see information about the endpoints involved in a security incident.



Endpoints involved in incidents

Search:

ALERT TYPE	MACHINE NAME	ALERT COUNT
Malware	WIN_DESKTOP_5	301
Exploit	WIN_DESKTOP_5	56
PUP	WIN_DESKTOP_5	42
Malware	LINUX_DESKTOP_1	14
Malware	MAC_DESKTOP_1	14
Malware	MAC_DESKTOP_2	14
Malware	LINUX_LAPTOP_1	7
Malware	WIN_DESKTOP_3	7
Malware	WIN_DESKTOP_4	7
Malware	WIN_LAPTOP_2	7

Showing 1 to 10 of 10 entries

< Previous 1 Next >

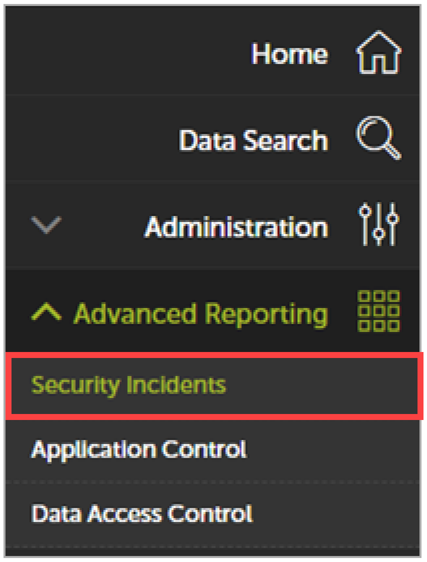
Incidents on all endpoints

Determine the Origin of a Security Threat

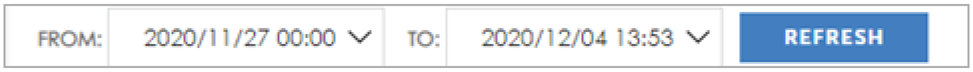
You can filter a data table to determine the origin of a security threat. Alternatively, you can edit the SQL query directly to determine the origin.

To filter the data table to determine the origin of a security threat:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Security Incidents**.

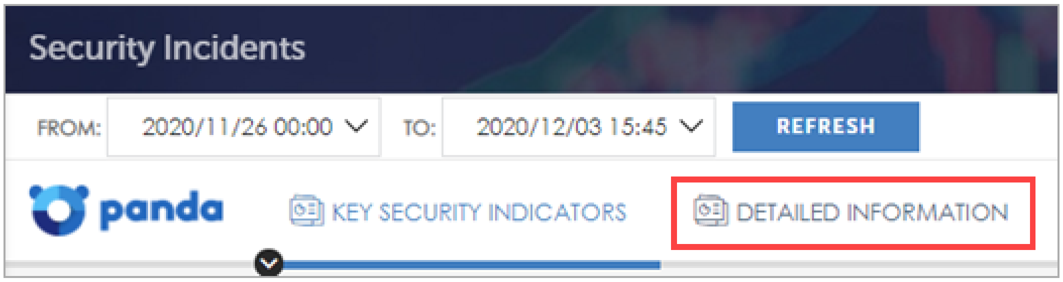


4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. Select **Detailed Information**.

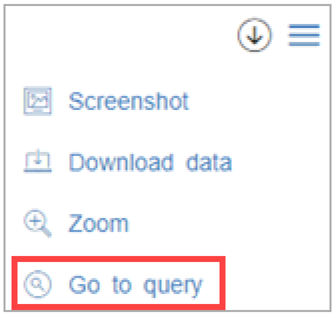


Security Incidents

FROM: 2020/11/26 00:00 TO: 2020/12/03 15:45

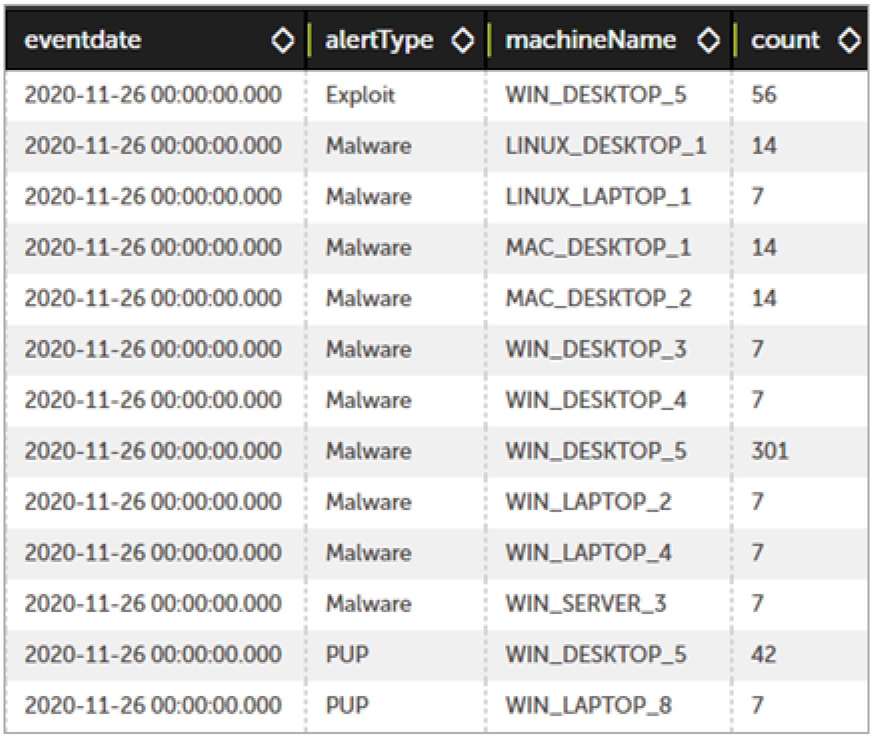
6. Review the list of endpoints in the **Endpoints involved in incidents** tile.

7. To open the corresponding data table, from menu ≡, select **Go to query**.



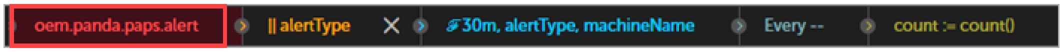
The data table opens.

In the example below, WIN_DESKTOP_5 has the highest number of malware alerts.

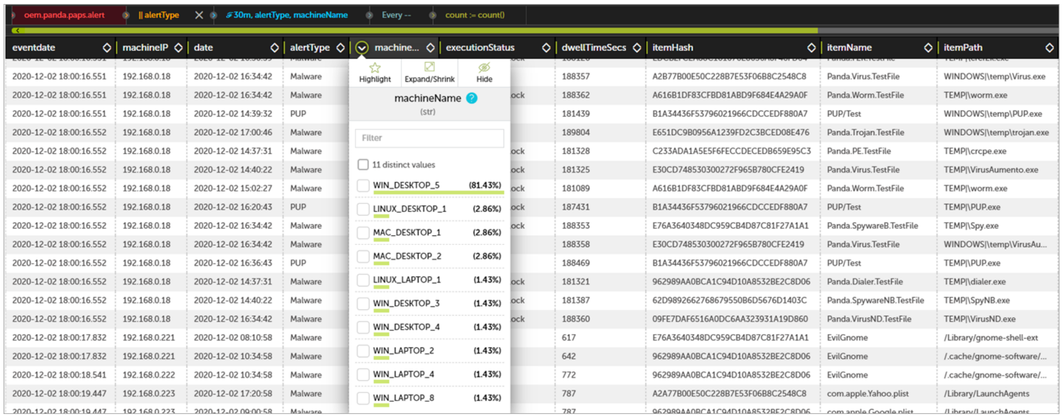


eventdate	alertType	machineName	count
2020-11-26 00:00:00.000	Exploit	WIN_DESKTOP_5	56
2020-11-26 00:00:00.000	Malware	LINUX_DESKTOP_1	14
2020-11-26 00:00:00.000	Malware	LINUX_LAPTOP_1	7
2020-11-26 00:00:00.000	Malware	MAC_DESKTOP_1	14
2020-11-26 00:00:00.000	Malware	MAC_DESKTOP_2	14
2020-11-26 00:00:00.000	Malware	WIN_DESKTOP_3	7
2020-11-26 00:00:00.000	Malware	WIN_DESKTOP_4	7
2020-11-26 00:00:00.000	Malware	WIN_DESKTOP_5	301
2020-11-26 00:00:00.000	Malware	WIN_LAPTOP_2	7
2020-11-26 00:00:00.000	Malware	WIN_LAPTOP_4	7
2020-11-26 00:00:00.000	Malware	WIN_SERVER_3	7
2020-11-26 00:00:00.000	PUP	WIN_DESKTOP_5	42
2020-11-26 00:00:00.000	PUP	WIN_LAPTOP_8	7

8. Above the data table, in the table legend, click **oem.panda.paps.alert**.



9. In the full data table, to filter the table by machine name, click the down arrow ⌄ in the **machineName** column.

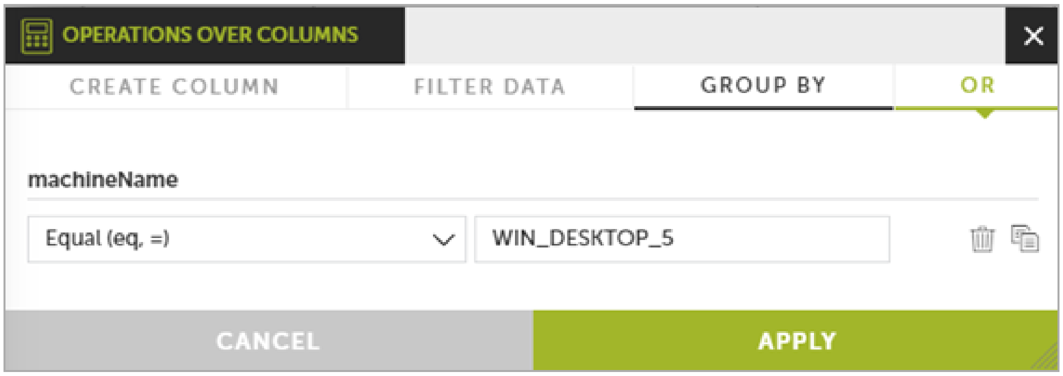


eventdate	machineIP	date	alertType	machine...	executionStatus	dwellTimeSecs	itemHash	itemName	itemPath
2020-12-02 18:00:16.551	192.168.0.18	2020-12-02 16:34:42	Malware			188357	A2B77B00E50C228B7E53F06B8C2548C8	Panda.Virus.TestFile	WINDOWS|\temp\Virus.exe
2020-12-02 18:00:16.551	192.168.0.18	2020-12-02 16:34:42	Malware		ock	188362	A616B1DF83CFBD81ABD9F684E4A29A0F	Panda.Worm.TestFile	TEMP|\worm.exe
2020-12-02 18:00:16.551	192.168.0.18	2020-12-02 14:39:32	PUP			181439	B1A34436F53796021966CDCCEDF880A7	PUP/Test	WINDOWS|\temp\PUP.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 17:00:46	Malware			189804	E651DC9B0956A1239FD2C3BCED08E476	Panda.Trojan.TestFile	WINDOWS|\temp\trojan.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 14:37:31	Malware		ock	181328	C233ADA1A5E5F6FECCDECEDB659E95C3	Panda.PE.TestFile	TEMP|\crcpe.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 14:40:22	Malware		ock	181325	E30CD748530300272F965B780CFE2419	Panda.Virus.TestFile	TEMP|\VirusAumento.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 15:02:27	Malware		ock	181089	A616B1DF83CFBD81ABD9F684E4A29A0F	Panda.Worm.TestFile	TEMP|\worm.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 16:20:43	PUP		ock	187431	B1A34436F53796021966CDCCEDF880A7	PUP/Test	TEMP|\PUP.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 16:34:42	Malware		ock	188353	E76A3640348DC959CB4D87C81F27A1A1	Panda.SpywareB.TestFile	TEMP|\Spy.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 16:34:42	Malware			188358	E30CD748530300272F965B780CFE2419	Panda.Virus.TestFile	WINDOWS|\temp\VirusAu...
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 16:36:43	PUP			188469	B1A34436F53796021966CDCCEDF880A7	PUP/Test	TEMP|\PUP.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 14:37:31	Malware		ock	181321	962989AA0BCA1C94D10A8532BE2C8D06	Panda.Dialer.TestFile	TEMP|\dialer.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 14:40:22	Malware		ock	181387	62D9892662768679550B6D5676D1403C	Panda.SpywareNB.TestFile	TEMP|\SpyNB.exe
2020-12-02 18:00:16.552	192.168.0.18	2020-12-02 16:34:42	Malware		ock	188360	09FE7DAF6516A0DC6AA323931A19D860	Panda.VirusND.TestFile	TEMP|\VirusND.exe
2020-12-02 18:00:17.832	192.168.0.221	2020-12-02 08:10:58	Malware			617	E76A3640348DC959CB4D87C81F27A1A1	EvilGnome	/Library/gnome-shell-ext
2020-12-02 18:00:17.832	192.168.0.221	2020-12-02 10:34:58	Malware			642	962989AA0BCA1C94D10A8532BE2C8D06	EvilGnome	/.cache/gnome-software/...
2020-12-02 18:00:18.541	192.168.0.222	2020-12-02 10:34:58	Malware			772	962989AA0BCA1C94D10A8532BE2C8D06	EvilGnome	/.cache/gnome-software/...
2020-12-02 18:00:19.447	192.168.0.223	2020-12-02 17:20:58	Malware			787	A2A77B00E50C228B7E53F06B8C2548C8	com.apple.Yahoo.plist	/Library/LaunchAgents

☐ 11 distinct values

☐	WIN_DESKTOP_5	(81.43%)
☐	LINUX_DESKTOP_1	(2.86%)
☐	MAC_DESKTOP_1	(2.86%)
☐	MAC_DESKTOP_2	(2.86%)
☐	LINUX_LAPTOP_1	(1.43%)
☐	WIN_DESKTOP_3	(1.43%)
☐	WIN_DESKTOP_4	(1.43%)
☐	WIN_LAPTOP_2	(1.43%)
☐	WIN_LAPTOP_4	(1.43%)
☐	WIN_LAPTOP_8	(1.43%)

10. Select the check box next to a machine name.
The Operations Over Columns dialog box opens.



machineName

Equal (eq, =) WIN_DESKTOP_5

11. Click **Apply**.
12. To filter the **alertType** column by **Malware**, repeat steps 7 – 9.
    The table shows the malware name (itemName) and location (itemPath).
13. Click to add **itemname** and **itempath** columns to the data table.
14. Click **Toggle Query Editor** in the toolbar.
15. Clear the existing code and copy this SQL code in the text box:

```
from oem.panda.paps.alert

where alertType = "Malware" or alertType = "PUP"

or alertType = "Exploit"

group every 30m by alertType, machineName,

itemName, itemPath

every -

select count() as count
```

16. Click **Run**.

Manage Misuse of Corporate Networks and Applications

The Application Control dashboards offer detailed information about the applications installed and executed on endpoints. This might be legitimate software used for malicious actions. You can use Application Control data to identify applications that are unwanted, unauthorized, unlicensed, have known vulnerabilities, consume a high amount of bandwidth, or are scripting, remote access, or system tools.

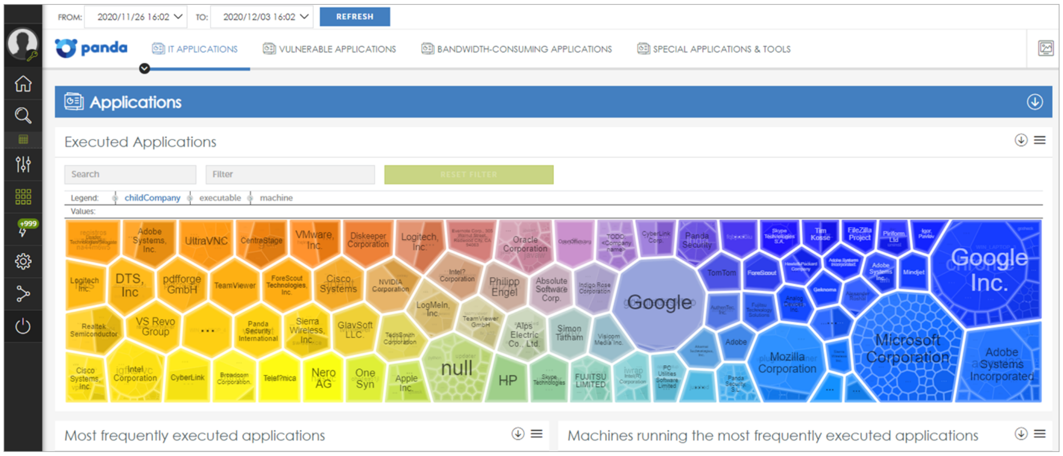
ⓘ For a list of the applications detected by ART, see the Knowledge Base article, Special applications and tools tables in Advanced Reporting Tool.

This section describes how to use ART to track the resource usage patterns of users to enforce and enhance organization security policies. This includes how to:

- Find corporate and non-corporate applications that run on your network.
- Find applications that execute least often in your network , which might indicate that an attacker has run a rare application in your network.
- Find vulnerable applications installed on endpoints that can lead to infection or impact network performance.
- Manage Microsoft Office licenses.
- Identify applications that consume high amounts of bandwidth.

IT Applications

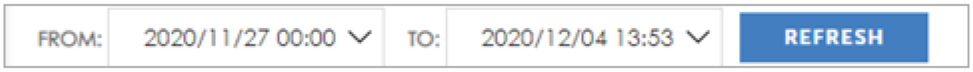
The **IT Applications** page enables you to find out which applications have run on network computers, as well as control the Microsoft Office licenses in use.



View Executed Applications

To view applications that have run on network computers:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.

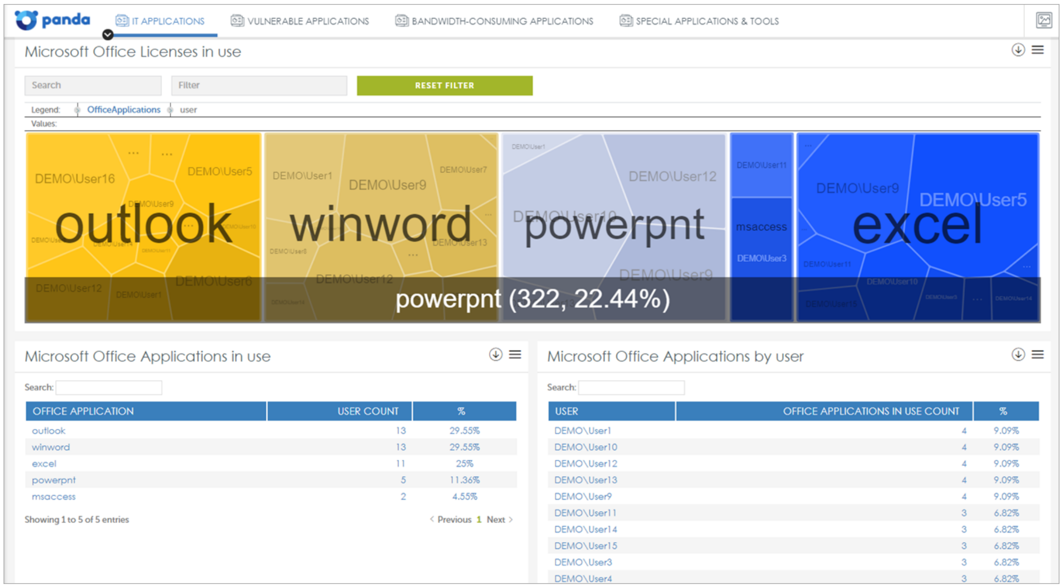

FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53 REFRESH

5. Select **IT Applications**.
6. Review the list of executed applications to determine whether there are applications that have not been validated.

> We recommend that remove any VPN clients that are not validated by the company. Non-validated VPN clients can evade corporate rules and network security, such as firewalls and other filters. VPN clients that run on accounts with extensive permissions might be outdated, which can add to the attack vectors that cyber criminals use. You can use the IT Applications page to find VPN clients.

View Microsoft Office Licenses

Use the **IT Applications** page to view information on the number of Microsoft Office licenses that are in use in the network.



Microsoft Office Licenses in use

Microsoft Office Applications in use

Search:

OFFICE APPLICATION	USER COUNT	%
outlook	13	29.55%
winword	13	29.55%
excel	11	25%
powerpnt	5	11.36%
msaccess	2	4.55%

Showing 1 to 5 of 5 entries

Previous 1 Next

Microsoft Office Applications by user

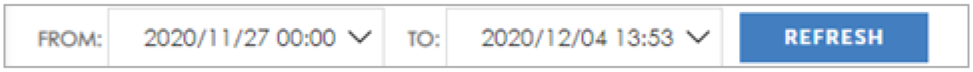
Search:

USER	OFFICE APPLICATIONS IN USE COUNT	%
DEMO\User1	4	9.09%
DEMO\User10	4	9.09%
DEMO\User12	4	9.09%
DEMO\User13	4	9.09%
DEMO\User9	4	9.09%
DEMO\User11	3	6.82%
DEMO\User14	3	6.82%
DEMO\User15	3	6.82%
DEMO\User3	3	6.82%
DEMO\User4	3	6.82%

To view users who use a specific Microsoft application, in the legend bar, drag **user** before **Office Applications**. Or, double-click an application square to view the users of that application.

To view Microsoft Office licenses:

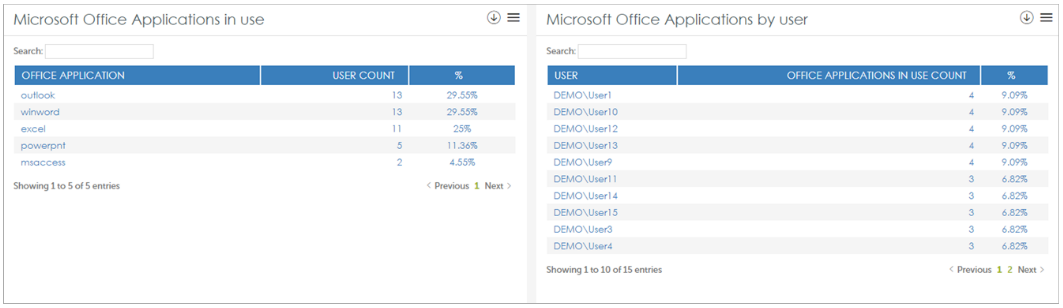
1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00

TO: 2020/12/04 13:53

5. Select **IT Applications**.
6. In the **Microsoft Office Licenses in Use** tile, review the list of Microsoft Office licenses in use on your network.
7. In the **Microsoft Office Applications in Use** tile, review the list of Microsoft Office applications that executed on user computers in your network.



Microsoft Office Applications in use

Search:

OFFICE APPLICATION	USER COUNT	%
outlook	13	29.55%
winword	13	29.55%
excel	11	25%
powerpnt	5	11.36%
msaccess	2	4.55%

Showing 1 to 5 of 5 entries

Microsoft Office Applications by user

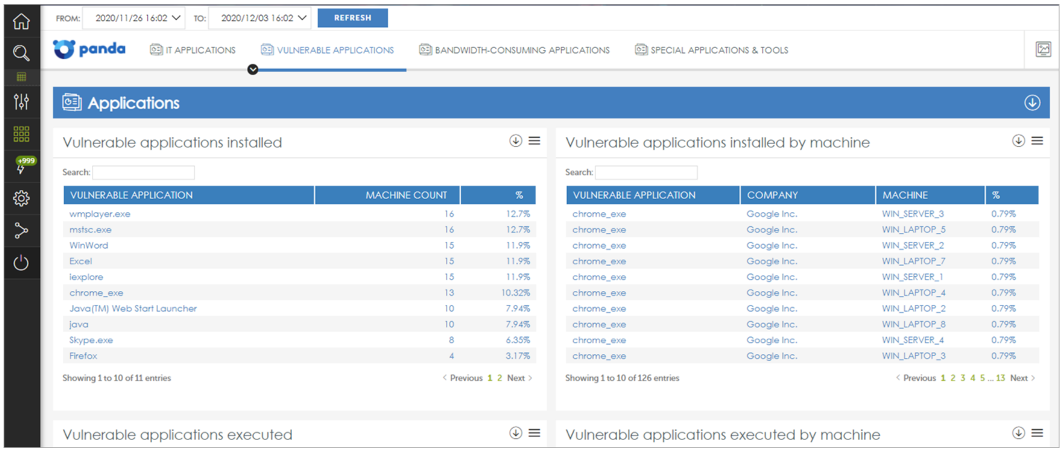
Search:

USER	OFFICE APPLICATIONS IN USE COUNT	%
DEMO\User1	4	9.09%
DEMO\User10	4	9.09%
DEMO\User12	4	9.09%
DEMO\User13	4	9.09%
DEMO\User9	4	9.09%
DEMO\User11	3	6.82%
DEMO\User14	3	6.82%
DEMO\User15	3	6.82%
DEMO\User3	3	6.82%
DEMO\User4	3	6.82%

Showing 1 to 10 of 15 entries

Vulnerable Applications

The **Vulnerable Applications** page enables you to identify vulnerable applications installed and executed on network computers.



FROM: 2020/11/26 16:02 TO: 2020/12/03 16:02

Vulnerable applications installed

Search:

VULNERABLE APPLICATION	MACHINE COUNT	%
wmplayer.exe	16	12.7%
mstsc.exe	16	12.7%
WinWord	15	11.9%
Excel	15	11.9%
iexplore	15	11.9%
chrome_exe	13	10.32%
Java(TM) Web Start Launcher	10	7.94%
java	10	7.94%
Skype.exe	8	6.35%
Firefox	4	3.17%

Showing 1 to 10 of 11 entries

Vulnerable applications installed by machine

Search:

VULNERABLE APPLICATION	COMPANY	MACHINE	%
chrome_exe	Google Inc.	WIN_SERVER_3	0.79%
chrome_exe	Google Inc.	WIN_LAPTOP_5	0.79%
chrome_exe	Google Inc.	WIN_SERVER_2	0.79%
chrome_exe	Google Inc.	WIN_LAPTOP_7	0.79%
chrome_exe	Google Inc.	WIN_SERVER_1	0.79%
chrome_exe	Google Inc.	WIN_LAPTOP_4	0.79%
chrome_exe	Google Inc.	WIN_LAPTOP_2	0.79%
chrome_exe	Google Inc.	WIN_LAPTOP_8	0.79%
chrome_exe	Google Inc.	WIN_SERVER_4	0.79%
chrome_exe	Google Inc.	WIN_LAPTOP_3	0.79%

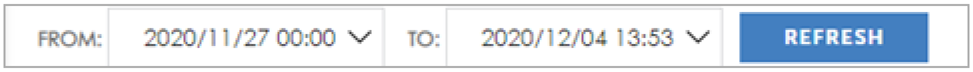
Showing 1 to 10 of 126 entries

Vulnerable applications executed

Vulnerable applications executed by machine

To view vulnerable applications installed and executed in the network:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.

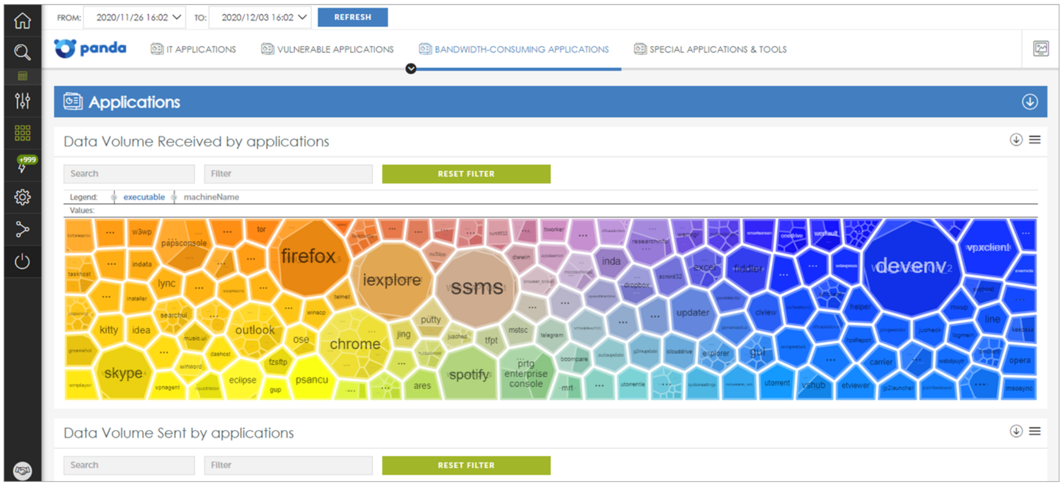


FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. Select **Vulnerable Applications**.
6. Review the **Vulnerable Applications Installed** and **Vulnerable Applications Executed** tiles to help determine which applications to prioritize for software updates.

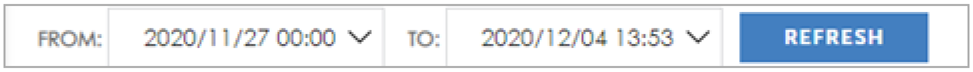
Bandwidth-consuming Applications

When programs download or upload high volumes of data, it can indicate malicious activity or failed application updates that continually download data.


FROM: 2020/11/26 16:02 TO: 2020/12/03 16:02

To view applications that send and receive high amounts of data:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.

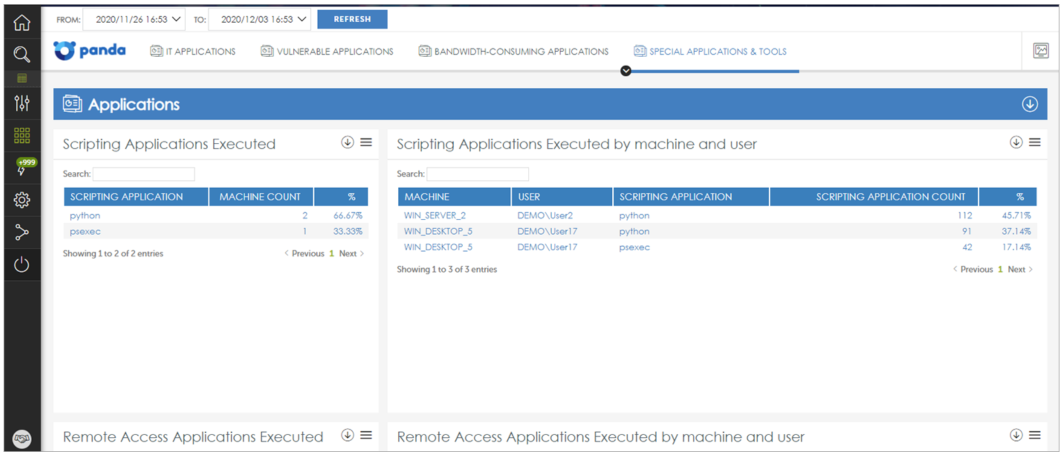

FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. Select **Bandwidth Consuming Applications > Applications**.
   The tiles display the volume and percentage of data received by applications that run on the network. You can use this information to identify applications with above average consumption and optimize bandwidth use across your network. You can also use Data Access Control for detailed information on bandwidth consumption. For more information, see Bandwidth Consumers.
6. In the **Data Volume Received by Applications** tile, review the applications that receive a high amount of data.
   The applications in this section can indicate machines or users that download problematic files. This can be a risk for security, bandwidth usage, as well as a general indication of abnormal system use.
7. In the **Data Volume Sent by Application** tile, review the applications that send a high amount of data.
   An application that sends a high amount of data might indicate data exfiltration.
8. To view users who send high amounts of data, in the legend bar, drag **machineName** before executable.
   Users who send a high amount of traffic might indicate data exfiltration operations. Double-click a machine name to view the executables that sent the data.

Special Applications and Tools

The **Special Applications & Tools** page provides visibility into the executed applications that are not authorized by your organization IT policies. These applications include:

- Script-based applications, such as PowerShell, Linux shell, and Windows cmd shell
- Remote access applications, such as TeamViewer and VNC
- Unwanted freeware applications, such as Torrent



Applications

Scripting Applications Executed

Search:

SCRIPTING APPLICATION	MACHINE COUNT	%
python	2	66.67%
psexec	1	33.33%

Showing 1 to 2 of 2 entries ‹ Previous 1 Next ›

Scripting Applications Executed by machine and user

Search:

MACHINE	USER	SCRIPTING APPLICATION	SCRIPTING APPLICATION COUNT	%
WIN_SERVER_2	DEMO\User2	python	112	45.71%
WIN_DESKTOP_5	DEMO\User17	python	91	37.14%
WIN_DESKTOP_5	DEMO\User17	psexec	42	17.14%

Showing 1 to 3 of 3 entries ‹ Previous 1 Next ›

Remote Access Applications Executed

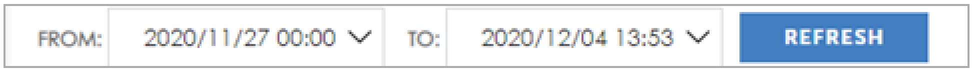
Remote Access Applications Executed by machine and user

View Script-based Applications in Use

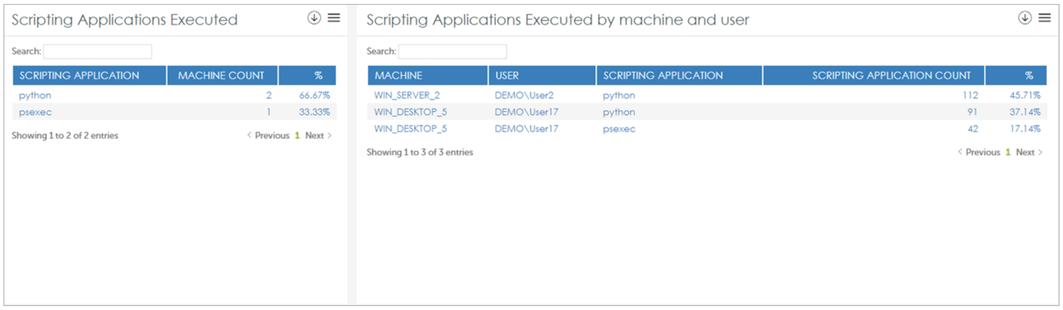
Script-based applications are legitimate software that can be used for malicious actions. It is important to know who uses these applications, and when and where they use them.

To view scripting applications on the network:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.



5. Select **Special Applications & Tools.**
These tiles list vulnerable applications installed or executed on user computers. Use this information to prioritize computers when you update software with known vulnerabilities
6. In the **Scripting Applications Executed** tiles, review the list of applications that specific users ran on specific computers, and how many times the application ran.



Scripting Applications Executed

Search:

SCRIPTING APPLICATION	MACHINE COUNT	%
python	2	66.67%
psexec	1	33.33%

Showing 1 to 2 of 2 entries

Scripting Applications Executed by machine and user

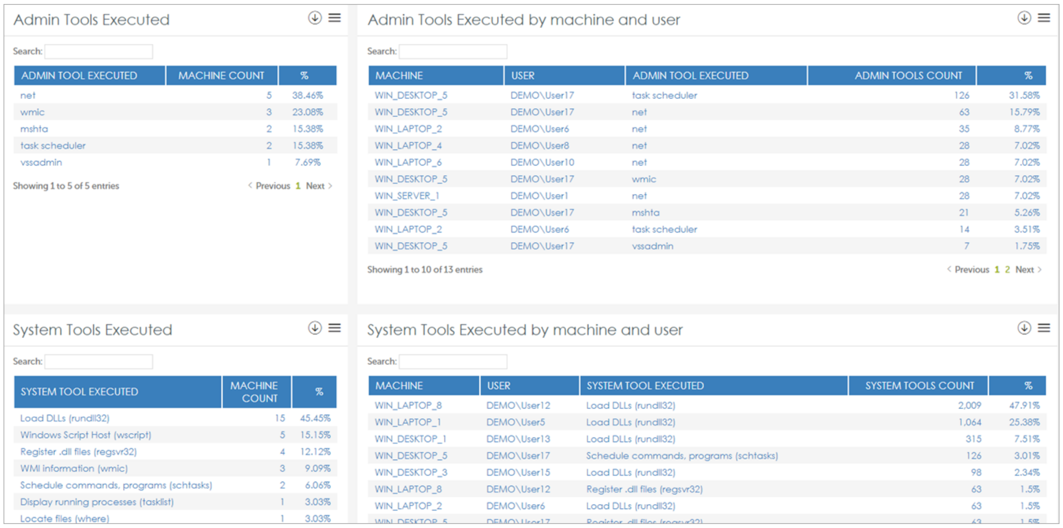
Search:

MACHINE	USER	SCRIPTING APPLICATION	SCRIPTING APPLICATION COUNT	%
WIN_SERVER_2	DEMO\User2	python	112	45.71%
WIN_DESKTOP_5	DEMO\User17	python	91	37.14%
WIN_DESKTOP_5	DEMO\User17	psexec	42	17.14%

Showing 1 to 3 of 3 entries

View Admin and System Tools in Use

Admin and system tools can also be used for malicious actions. It is important to know by who uses these applications, and when and where they use them.



Admin Tools Executed

Search:

ADMIN TOOL EXECUTED	MACHINE COUNT	%
net	5	38.46%
wmic	3	23.08%
mshta	2	15.38%
task scheduler	2	15.38%
vssadmin	1	7.69%

Showing 1 to 5 of 5 entries

Admin Tools Executed by machine and user

Search:

MACHINE	USER	ADMIN TOOL EXECUTED	ADMIN TOOLS COUNT	%
WIN_DESKTOP_5	DEMO\User17	task scheduler	126	31.58%
WIN_DESKTOP_5	DEMO\User17	net	63	15.79%
WIN_LAPTOP_2	DEMO\User6	net	35	8.77%
WIN_LAPTOP_4	DEMO\User8	net	28	7.02%
WIN_LAPTOP_6	DEMO\User10	net	28	7.02%
WIN_DESKTOP_5	DEMO\User17	wmic	28	7.02%
WIN_SERVER_1	DEMO\User1	net	28	7.02%
WIN_DESKTOP_5	DEMO\User17	mshta	21	5.26%
WIN_LAPTOP_2	DEMO\User6	task scheduler	14	3.51%
WIN_DESKTOP_5	DEMO\User17	vssadmin	7	1.75%

Showing 1 to 10 of 13 entries

System Tools Executed

Search:

SYSTEM TOOL EXECUTED	MACHINE COUNT	%
Load DLLs (rundll32)	15	45.45%
Windows Script Host (wscript)	5	15.15%
Register .dll files (regsvr32)	4	12.12%
WMI information (wmic)	3	9.09%
Schedule commands, programs (schtasks)	2	6.06%
Display running processes (tasklist)	1	3.03%
Locate files (where)	1	3.03%

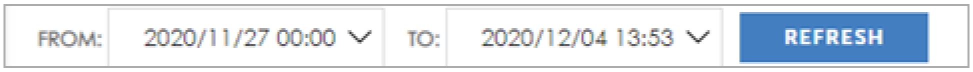
System Tools Executed by machine and user

Search:

MACHINE	USER	SYSTEM TOOL EXECUTED	SYSTEM TOOLS COUNT	%
WIN_LAPTOP_8	DEMO\User12	Load DLLs (rundll32)	2,009	47.91%
WIN_LAPTOP_1	DEMO\User5	Load DLLs (rundll32)	1,064	25.38%
WIN_DESKTOP_1	DEMO\User13	Load DLLs (rundll32)	315	7.51%
WIN_DESKTOP_5	DEMO\User17	Schedule commands, programs (schtasks)	126	3.01%
WIN_DESKTOP_3	DEMO\User15	Load DLLs (rundll32)	98	2.34%
WIN_LAPTOP_8	DEMO\User12	Register .dll files (regsvr32)	63	1.5%
WIN_LAPTOP_2	DEMO\User6	Load DLLs (rundll32)	63	1.5%
WIN_DESKTOP_5	DEMO\User17	Register .dll files (regsvr32)	63	1.5%

To view admin and system tools that run on your network:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

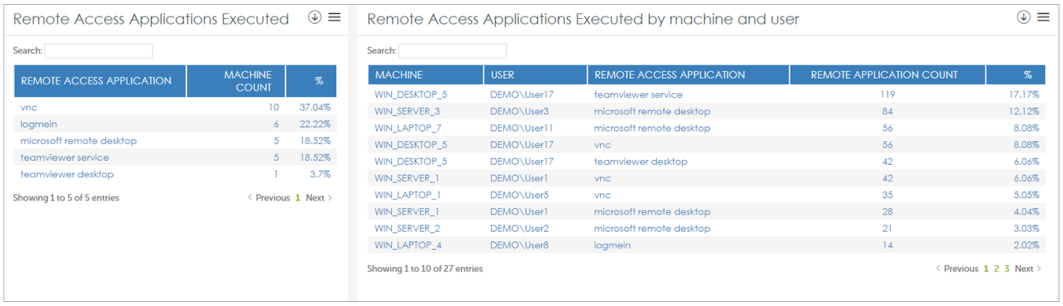
5. Select **Special Applications & Tools**.
6. In the **Admin Tools Executed** tiles, review the admin tools that run across the network to identify tools that are not validated.
7. In the **System Tools Executed** tiles, review the Windows OS utilities that run across the network to identify utilities that are not validated.

8. In the **System Internal Tools Executed** sections, review the Sysinternal tools that run across the network and identify tools that are not validated.
   Sysinternal tools are not included with the Windows OS but are freely available from Microsoft with extra, advanced utilities. Sysinternal tools are sometimes used as part of a malware attack (for example, toolsets).

> For more information on the specific tools detected, see the Support Article, Special applications and tools tables in Advanced Reporting Tool.

View Remote Access Applications

Remote tools are a common attack vector. We recommend that you only use remote tools validated by the company. Limit connectivity to administrators and use a fireware filter, as well as strong passwords. Check for regular use of remote access tools to identify misuse or hacking attacks.



Remote Access Applications Executed

Search:

REMOTE ACCESS APPLICATION	MACHINE COUNT	%
vnc	10	37.04%
logmein	6	22.22%
microsoft remote desktop	5	18.52%
teamviewer service	5	18.52%
teamviewer desktop	1	3.7%

Showing 1 to 5 of 5 entries

Remote Access Applications Executed by machine and user

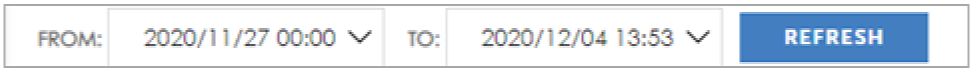
Search:

MACHINE	USER	REMOTE ACCESS APPLICATION	REMOTE APPLICATION COUNT	%
WIN_DESKTOP_5	DEMO\User17	teamviewer service	119	17.17%
WIN_SERVER_3	DEMO\User3	microsoft remote desktop	84	12.12%
WIN_LAPTOP_7	DEMO\User11	microsoft remote desktop	56	8.08%
WIN_DESKTOP_5	DEMO\User17	vnc	56	8.08%
WIN_DESKTOP_5	DEMO\User17	teamviewer desktop	42	6.06%
WIN_SERVER_1	DEMO\User1	vnc	42	6.06%
WIN_LAPTOP_1	DEMO\User5	vnc	35	5.05%
WIN_SERVER_1	DEMO\User1	microsoft remote desktop	28	4.04%
WIN_SERVER_2	DEMO\User2	microsoft remote desktop	21	3.03%
WIN_LAPTOP_4	DEMO\User8	logmein	14	2.02%

Showing 1 to 10 of 27 entries

To view remote access applications:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.



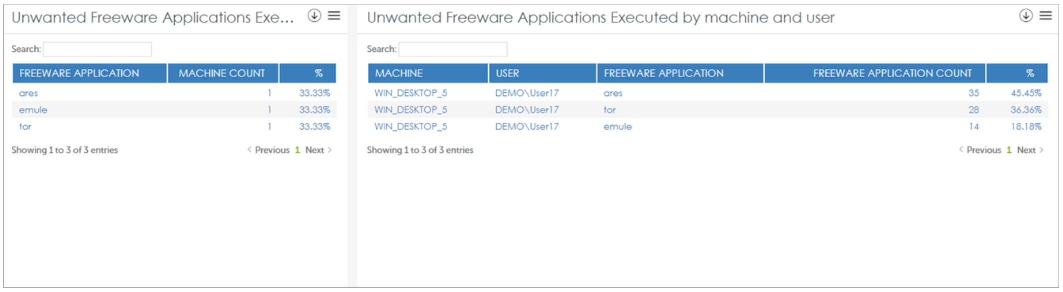
FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. Select **Special Applications & Tools**.
6. In the **Remote Access Applications Executed** tiles, review the list of applications executed by machine and user.

View Unwanted Freeware

Torrent software is not necessarily a risk, but files downloaded from torrent sites might contain malware or malicious content. Traffic through Tor exit nodes indicates the use of Tor browsers in your environment. These exit nodes are risky because traffic that passes through the gateway is difficult to control and can indicate an attempt to hide the activity.

We recommend that you remove Torrent software from your network to prevent the upload and download of copyrighted material, and minimize bandwidth usage. Alternatively, you could actively monitor Tor nodes and files downloaded through torrent applications.



Unwanted Freeware Applications Exe...

Search:

FREEWARE APPLICATION	MACHINE COUNT	%
ares	1	33.33%
emule	1	33.33%
tor	1	33.33%

Showing 1 to 3 of 3 entries

Unwanted Freeware Applications Executed by machine and user

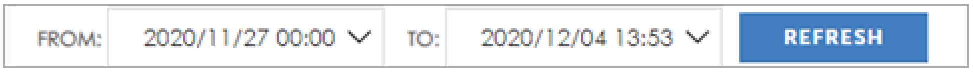
Search:

MACHINE	USER	FREEWARE APPLICATION	FREEWARE APPLICATION COUNT	%
WIN_DESKTOP_5	DEMO\User17	ares	35	45.45%
WIN_DESKTOP_5	DEMO\User17	tor	28	36.36%
WIN_DESKTOP_5	DEMO\User17	emule	14	18.18%

Showing 1 to 3 of 3 entries

To view unwanted freeware such as Torrent:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, select **Advanced Reporting > Application Control**.
4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00

TO: 2020/12/04 13:53

5. Select **Special Applications & Tools**.
6. In the **Unwanted Freeware Applications Executed** tiles, review the list of applications executed by machine and user.

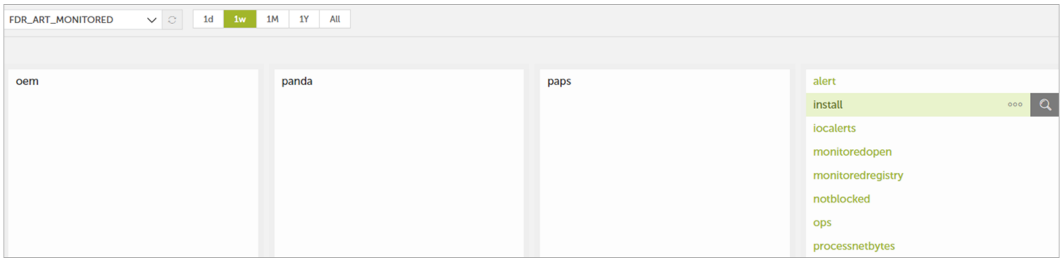
Example: Monitor Microsoft Operating System Use

It is a good idea to minimize the number of different versions of Microsoft Windows in your IT environment. Fewer versions help to reduce the risk of attack (in general, Windows 10 is twice as secure as Windows 7), and make it easier to manage and build policies to protect the operating system.

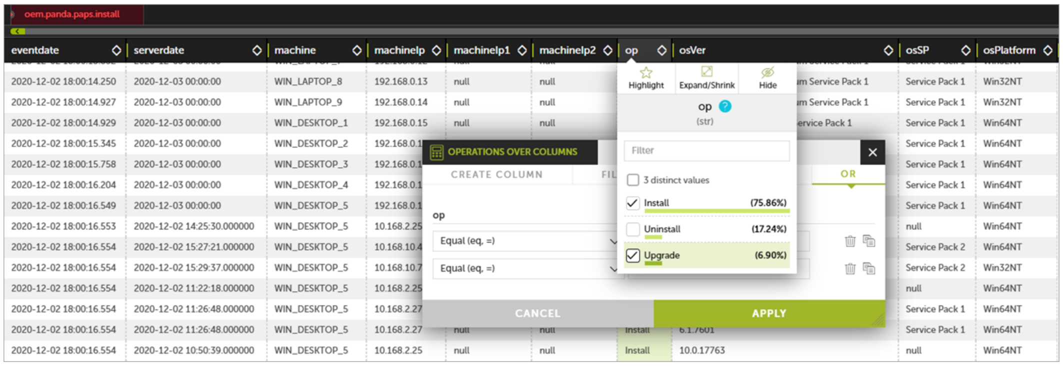
This example describes how to filter and refine a data table to view the versions of Microsoft Windows that are in use, as well as how to generate a visual representation of the data.

To view the Microsoft operating systems in use:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Data Search** 🔍 .
4. Select the **oem.panda.paps.install** table for the time period you want.
   The data table window opens.



5. Filter the **op** column by **Install** and **Upgrade**.

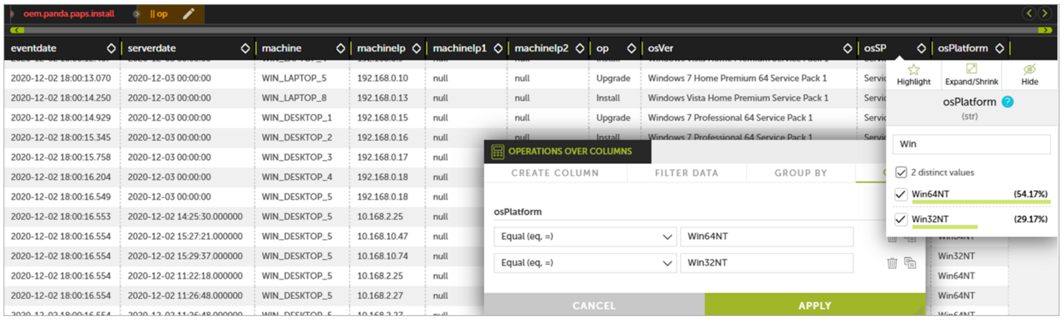


op
Equal (eq, =)
Equal (eq, =)

☐ 3 distinct values
☑ Install (75.86%)
☐ Uninstall (17.24%)
☑ Upgrade (6.90%)

eventdate	serverdate	machine	machineIp	machineIp1	machineIp2	op	osVer	osSP	osPlatform
2020-12-02 18:00:14.250	2020-12-03 00:00:00	WIN_LAPTOP_8	192.168.0.13	null	null		m Service Pack 1	Service Pack 1	Win32NT
2020-12-02 18:00:14.927	2020-12-03 00:00:00	WIN_LAPTOP_9	192.168.0.14	null	null		m Service Pack 1	Service Pack 1	Win32NT
2020-12-02 18:00:14.929	2020-12-03 00:00:00	WIN_DESKTOP_1	192.168.0.15	null	null		ervice Pack 1	Service Pack 1	Win64NT
2020-12-02 18:00:15.345	2020-12-03 00:00:00	WIN_DESKTOP_2	192.168.0.1					Service Pack 1	Win64NT
2020-12-02 18:00:15.758	2020-12-03 00:00:00	WIN_DESKTOP_3	192.168.0.1					Service Pack 1	Win64NT
2020-12-02 18:00:16.204	2020-12-03 00:00:00	WIN_DESKTOP_4	192.168.0.1					Service Pack 1	Win64NT
2020-12-02 18:00:16.549	2020-12-03 00:00:00	WIN_DESKTOP_5	192.168.0.1					Service Pack 1	Win64NT
2020-12-02 18:00:16.553	2020-12-02 14:25:30.000000	WIN_DESKTOP_5	10.168.2.25					null	Win64NT
2020-12-02 18:00:16.554	2020-12-02 15:27:21.000000	WIN_DESKTOP_5	10.168.10.4					Service Pack 2	Win64NT
2020-12-02 18:00:16.554	2020-12-02 15:29:37.000000	WIN_DESKTOP_5	10.168.10.7					Service Pack 2	Win32NT
2020-12-02 18:00:16.554	2020-12-02 11:22:18.000000	WIN_DESKTOP_5	10.168.2.25					null	Win64NT
2020-12-02 18:00:16.554	2020-12-02 11:26:48.000000	WIN_DESKTOP_5	10.168.2.27					Service Pack 1	Win64NT
2020-12-02 18:00:16.554	2020-12-02 11:26:48.000000	WIN_DESKTOP_5	10.168.2.27	null	null	Install	6.1.7601	Service Pack 1	Win64NT
2020-12-02 18:00:16.554	2020-12-02 10:50:39.000000	WIN_DESKTOP_5	10.168.2.25	null	null	Install	10.0.17763	null	Win64NT

6. Filter the **opPlatform** column for platforms that start with **Win**.



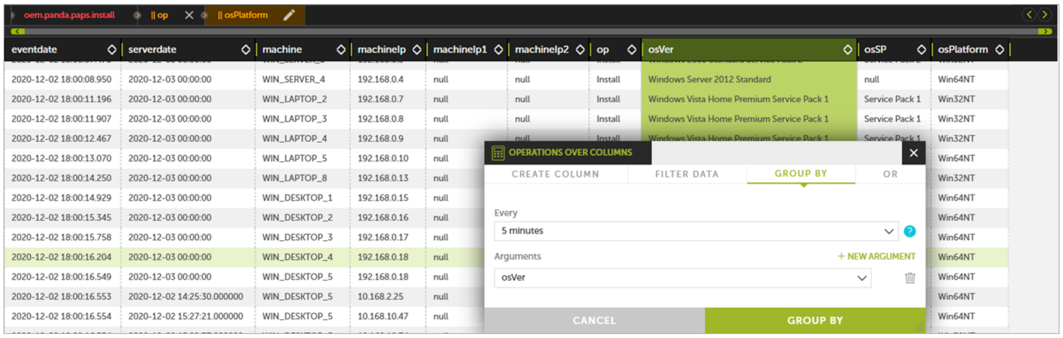
osPlatform
Equal (eq, =) Win64NT
Equal (eq, =) Win32NT

Win
☑ 2 distinct values
☑ Win64NT (54.17%)
☑ Win32NT (29.17%)

eventdate	serverdate	machine	machineIp	machineIp1	machineIp2	op	osVer	osSP	osPlatform
2020-12-02 18:00:13.070	2020-12-03 00:00:00	WIN_LAPTOP_5	192.168.0.10	null	null	Upgrade	Windows 7 Home Premium 64 Service Pack 1	Servic	
2020-12-02 18:00:14.250	2020-12-03 00:00:00	WIN_LAPTOP_8	192.168.0.13	null	null	Install	Windows Vista Home Premium Service Pack 1	Servic	
2020-12-02 18:00:14.929	2020-12-03 00:00:00	WIN_DESKTOP_1	192.168.0.15	null	null	Upgrade	Windows 7 Professional 64 Service Pack 1	Servic	
2020-12-02 18:00:15.345	2020-12-03 00:00:00	WIN_DESKTOP_2	192.168.0.16	null	null	Install	Windows 7 Professional 64 Service Pack 1	Servic	
2020-12-02 18:00:15.758	2020-12-03 00:00:00	WIN_DESKTOP_3	192.168.0.17	null					
2020-12-02 18:00:16.204	2020-12-03 00:00:00	WIN_DESKTOP_4	192.168.0.18	null					
2020-12-02 18:00:16.549	2020-12-03 00:00:00	WIN_DESKTOP_5	192.168.0.18	null					
2020-12-02 18:00:16.553	2020-12-02 14:25:30.000000	WIN_DESKTOP_5	10.168.2.25	null					
2020-12-02 18:00:16.554	2020-12-02 15:27:21.000000	WIN_DESKTOP_5	10.168.10.47	null					
2020-12-02 18:00:16.554	2020-12-02 15:29:37.000000	WIN_DESKTOP_5	10.168.10.74	null					Win32NT
2020-12-02 18:00:16.554	2020-12-02 11:22:18.000000	WIN_DESKTOP_5	10.168.2.25	null					Win64NT
2020-12-02 18:00:16.554	2020-12-02 11:26:48.000000	WIN_DESKTOP_5	10.168.2.27	null					Win64NT

7. Click **Apply**.
8. Select the **osVer** column and click **Group** in the toolbar.

9. Click **New Argument**.
10. From the **Arguments** list, select **osVer**.



eventdate	serverdate	machine	machineIp	machineIp1	machineIp2	op	osVer	osSP	osPlatform
2020-12-02 18:00:08.950	2020-12-03 00:00:00	WIN_SERVER_4	192.168.0.4	null	null	Install	Windows Server 2012 Standard	null	Win64NT
2020-12-02 18:00:11.196	2020-12-03 00:00:00	WIN_LAPTOP_2	192.168.0.7	null	null	Install	Windows Vista Home Premium Service Pack 1	Service Pack 1	Win32NT
2020-12-02 18:00:11.907	2020-12-03 00:00:00	WIN_LAPTOP_3	192.168.0.8	null	null	Install	Windows Vista Home Premium Service Pack 1	Service Pack 1	Win32NT
2020-12-02 18:00:12.467	2020-12-03 00:00:00	WIN_LAPTOP_4	192.168.0.9	null	null	Install	Windows Vista Home Premium Service Pack 1	Service Pack 1	Win32NT
2020-12-02 18:00:13.070	2020-12-03 00:00:00	WIN_LAPTOP_5	192.168.0.10	null					Win64NT
2020-12-02 18:00:14.250	2020-12-03 00:00:00	WIN_LAPTOP_8	192.168.0.13	null					Win32NT
2020-12-02 18:00:14.929	2020-12-03 00:00:00	WIN_DESKTOP_1	192.168.0.15	null					Win64NT
2020-12-02 18:00:15.345	2020-12-03 00:00:00	WIN_DESKTOP_2	192.168.0.16	null					Win64NT
2020-12-02 18:00:15.758	2020-12-03 00:00:00	WIN_DESKTOP_3	192.168.0.17	null					Win64NT
2020-12-02 18:00:16.204	2020-12-03 00:00:00	WIN_DESKTOP_4	192.168.0.18	null					Win64NT
2020-12-02 18:00:16.549	2020-12-03 00:00:00	WIN_DESKTOP_5	192.168.0.18	null					Win64NT
2020-12-02 18:00:16.553	2020-12-02 14:25:30.000000	WIN_DESKTOP_5	10.168.2.25	null					Win64NT
2020-12-02 18:00:16.554	2020-12-02 15:27:21.000000	WIN_DESKTOP_5	10.168.10.47	null					Win64NT

Every
5 minutes

Arguments
osVer

11. Click **Group By**.
12. To create a count of the machines with each OS version, add a Count column:
    a. Click **Add Column** .
    b. Select **Aggregate Function**.
    c. In the **Column name** box, type `count`.
    d. From the **Aggregation** list, select **Count**.
    e. Click **Aggregate Function**.
13. To create a chart of this data:
    a. Click **Options** **> Charts > Plots > Histogram**.
    b. Drag the **osVer** and **Count** columns from the data table into the **Histogram** dialog box.

Manage Access to Critical Business Information

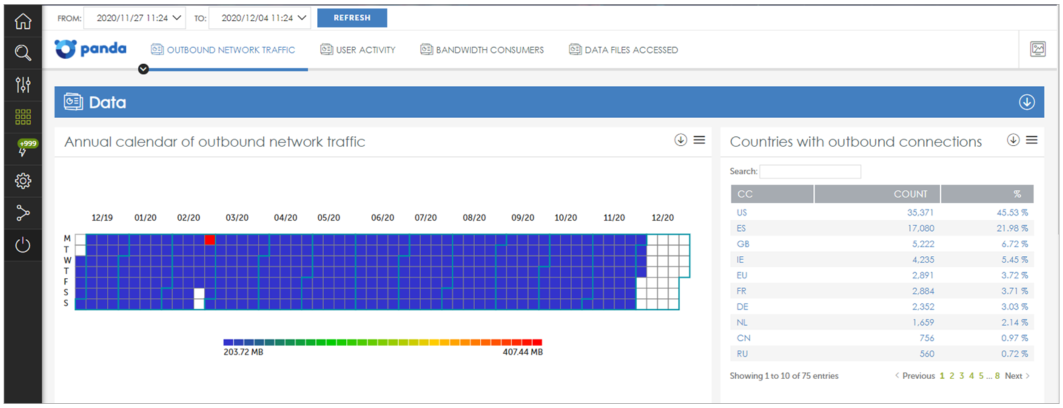
The Data Access Control dashboard displays the data that leaves your network. Data Access Control provides information that enables you to detect data leaks and theft of confidential information, identify high bandwidth consumers, and monitor file access and execution activity.

The dashboard can show you:

- Files that network users most commonly access.
- Calendar charts and maps that show the data sent over the last year.
- Which users access specific computers on the network.
- Countries that receive the highest number of connections from your network, which you can use to identify malicious activity.

Outbound Network Traffic

To minimize the attack surface and avoid exfiltration of data, it is important to know the external ports that outgoing traffic is sent to. Use the **Outbound Network Traffic** page to see where data is sent (and received), and to identify possible data breaches and compromised systems.



FROM: 2020/11/27 11:24 TO: 2020/12/04 11:24

Countries with outbound connections

Search:

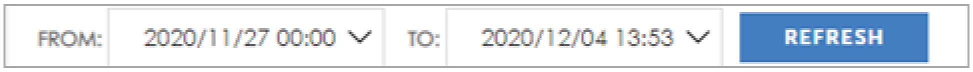
CC	COUNT	%
US	35,371	45.53 %
ES	17,080	21.98 %
GB	5,222	6.72 %
IE	4,235	5.45 %
EU	2,891	3.72 %
FR	2,884	3.71 %
DE	2,352	3.03 %
NL	1,659	2.14 %
CN	756	0.97 %
RU	560	0.72 %

Showing 1 to 10 of 75 entries ‹ Previous 1 2 3 4 5 ... 8 Next ›

> If you do not monitor outgoing traffic on sensitive ports, you could expose the company to potential attacks. We recommend that you close open ports when you do not need them and monitor ports continuously when access is required.

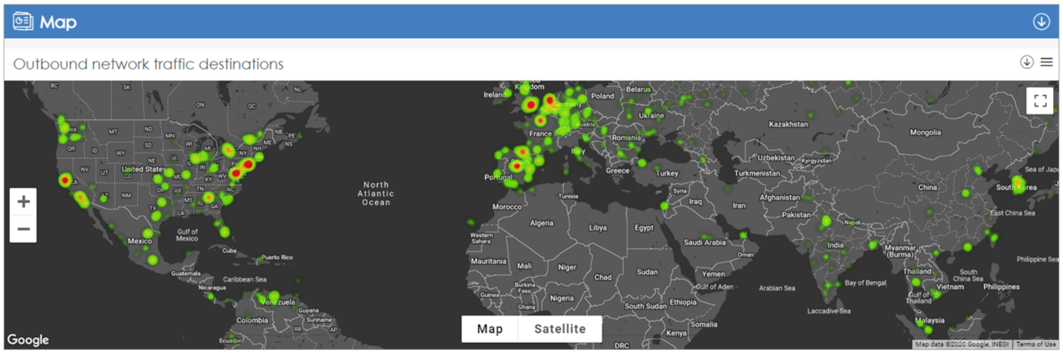
To view outbound network traffic destinations:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Data Access Control**.
4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. On the **Outbound Network Traffic** page, in the **Data** section, review the **Countries with outbound connections** tile.
This tile displays information about the volume of data sent from your network to a country. The charts show the absolute and relative amounts of data transferred. If you do not work with any company in China or Russia, for example, and you have traffic that goes to those countries, it is possible that there is malware exfiltrating data from your machines.
6. In the **Map** section, review the highlighted destinations.
The map shows the destinations where the largest amount of data was sent and helps you to identify abnormal traffic destinations.


Map
Outbound network traffic destinations
North Atlantic Ocean
United States
Mexico
Gulf of Mexico
Cuba
Caribbean Sea
Venezuela
Colombia
Ireland
France
Poland
Belarus
Ukraine
Romania
Italy
Greece
Turkey
Portugal
Morocco
Algeria
Libya
Egypt
Kazakhstan
Mongolia
China
South Korea
India
Iran
Saudi Arabia
+
−
Map
Satellite
Google

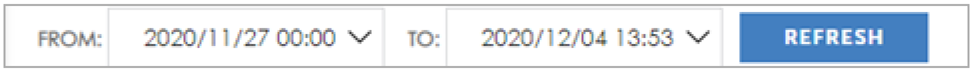
Bandwidth Consumers

Use the **Bandwidth Consumers** page to find applications and users that send large amounts of data. Large amounts of data sent can indicate data exfiltration. Applications that behave in an anomalous way can be a sign of malfunction or compromise. Users who send a high amount of traffic might indicate data exfiltration operations, and can provide early insight into potential user and device misuse.

View High Brandwidth-consuming Application Processes and Users

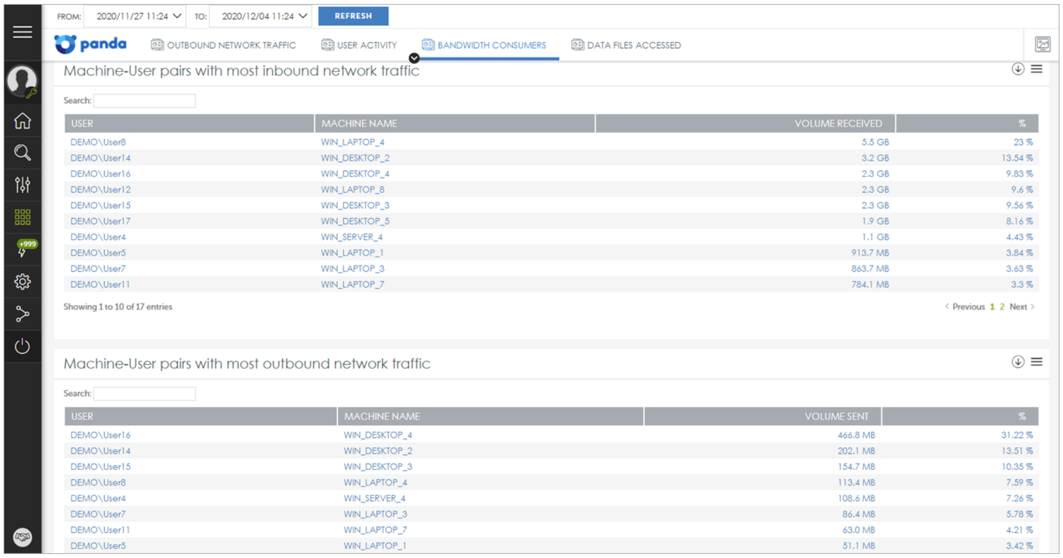
To view application processes and users that generate high inbound and outbound data volume:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Data Access Control**.
4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. Select **Bandwidth Consumers**.
The tables list the application processes and users that used the most inbound and outbound data volume.
6. In the **Applications** section, review the applications that receive a high amount of data.
Applications that receive a high amount of data can indicate machines or users that download problematic files. This can be a risk both when it comes to security but also bandwidth usage, and a general indication of system misuse.
7. In the **Machine-User** section, review the users who send a high amount of data.
High amounts of data can also indicate failed application updates that continually re-download data.



FROM: 2020/11/27 11:24 TO: 2020/12/04 11:24

Machine-User pairs with most inbound network traffic

Search:

USER	MACHINE NAME	VOLUME RECEIVED	%
DEMO\User8	WIN_LAPTOP_4	5.5 GB	23 %
DEMO\User14	WIN_DESKTOP_2	3.2 GB	13.54 %
DEMO\User16	WIN_DESKTOP_4	2.3 GB	9.83 %
DEMO\User12	WIN_LAPTOP_8	2.3 GB	9.6 %
DEMO\User15	WIN_DESKTOP_3	2.3 GB	9.56 %
DEMO\User17	WIN_DESKTOP_5	1.9 GB	8.16 %
DEMO\User4	WIN_SERVER_4	1.1 GB	4.43 %
DEMO\User5	WIN_LAPTOP_1	913.7 MB	3.84 %
DEMO\User7	WIN_LAPTOP_3	863.7 MB	3.63 %
DEMO\User11	WIN_LAPTOP_7	784.1 MB	3.3 %

Showing 1 to 10 of 17 entries

‹ Previous 1 2 Next ›

Machine-User pairs with most outbound network traffic

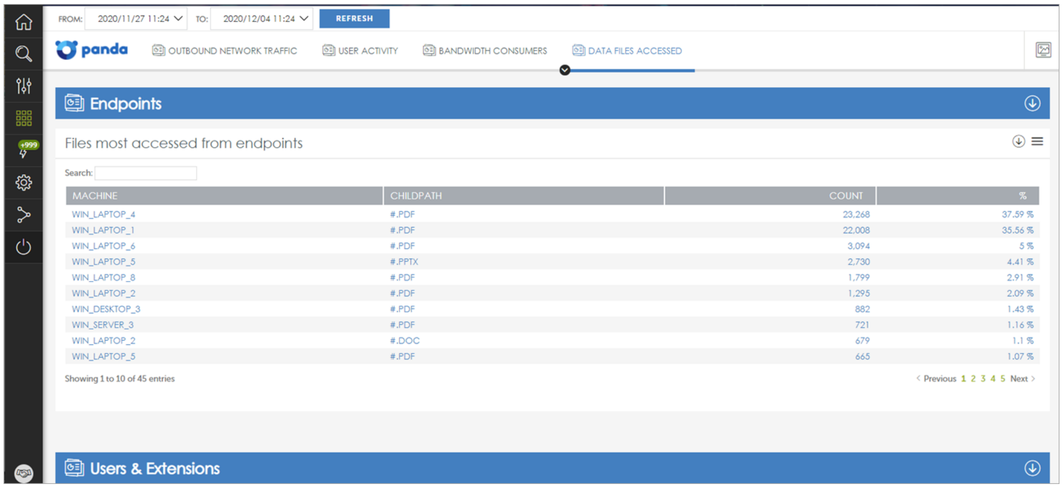
Search:

USER	MACHINE NAME	VOLUME SENT	%
DEMO\User16	WIN_DESKTOP_4	466.8 MB	31.22 %
DEMO\User14	WIN_DESKTOP_2	202.1 MB	13.51 %
DEMO\User15	WIN_DESKTOP_3	154.7 MB	10.35 %
DEMO\User8	WIN_LAPTOP_4	113.4 MB	7.59 %
DEMO\User4	WIN_SERVER_4	108.6 MB	7.26 %
DEMO\User7	WIN_LAPTOP_3	86.4 MB	5.78 %
DEMO\User11	WIN_LAPTOP_7	63.0 MB	4.21 %
DEMO\User5	WIN_LAPTOP_1	51.1 MB	3.42 %

To prevent data breaches or other unknown malicious activity, we recommend that you set an alert to warn you of high amounts of traffic. For information on alarms, see *Configure Real-time Alerts*.

Data Files Accessed

The **Data Files Accessed** page displays the data that leaves your network and enables you to help detect data leaks and theft of confidential information.



FROM: 2020/11/27 11:24 TO: 2020/12/04 11:24

Files most accessed from endpoints

Search:

MACHINE	CHILDPATH	COUNT	%
WIN_LAPTOP_4	#.PDF	23,268	37.59 %
WIN_LAPTOP_1	#.PDF	22,008	35.56 %
WIN_LAPTOP_6	#.PDF	3,094	5 %
WIN_LAPTOP_5	#.PPTX	2,730	4.41 %
WIN_LAPTOP_8	#.PDF	1,799	2.91 %
WIN_LAPTOP_2	#.PDF	1,295	2.09 %
WIN_DESKTOP_3	#.PDF	882	1.43 %
WIN_SERVER_3	#.PDF	721	1.16 %
WIN_LAPTOP_2	#.DOC	679	1.1 %
WIN_LAPTOP_5	#.PDF	665	1.07 %

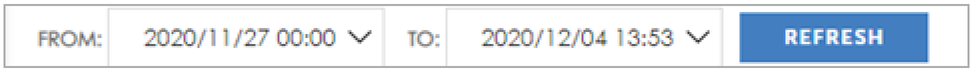
Showing 1 to 10 of 45 entries

‹ Previous 1 2 3 4 5 Next ›

View Data Files Access

To view data files accessed from non-standard means:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Advanced Reporting > Data Access Control**.
4. Select the date range for the data you want to view and click **Refresh**.



FROM: 2020/11/27 00:00 TO: 2020/12/04 13:53

5. Select **Data Files Accessed**.
6. In the **Endpoints** section, review endpoints that accessed files through non-standard means.
   For example, you might view when a PowerPoint (PPT) file was opened through a web browser instead of the PowerPoint application.
7. In the **Users & Extensions** section, review file access and execution statistics by user and file extension.

Real-time Alerts

You can configure real-time alerts based on events that indicate a security breach or an infringement of your corporate data management policy. An alert for anomalous behavior can help prevent an attack in its earliest stage. The alert features in ART include:

- Default alerts that indicate high-risk situations
- The ability to create up to 10 custom alerts based on your own specific criteria
- Several delivery methods to send alerts to recipients (for example, email, HTTP-JSON, Service Desk, Jira, Pushover, PagerDuty, and Slack)
- Anti-flooding settings to prevent alert floods

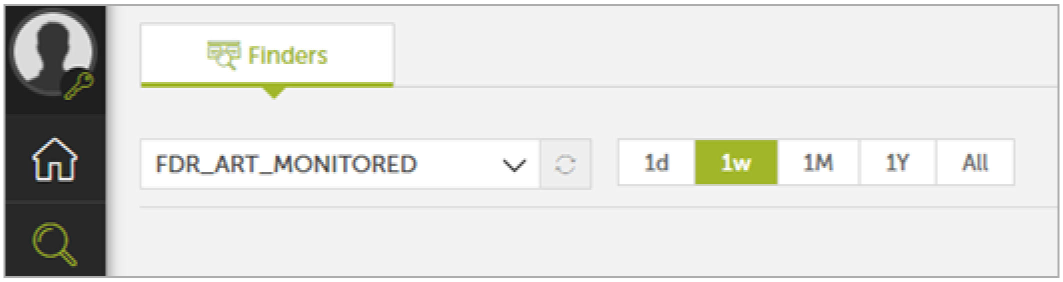
Configure Real-time Alerts

You create an alert from the associated data table. The alert can be configured for frequency, the conditions to generate an alert, and the delivery method.

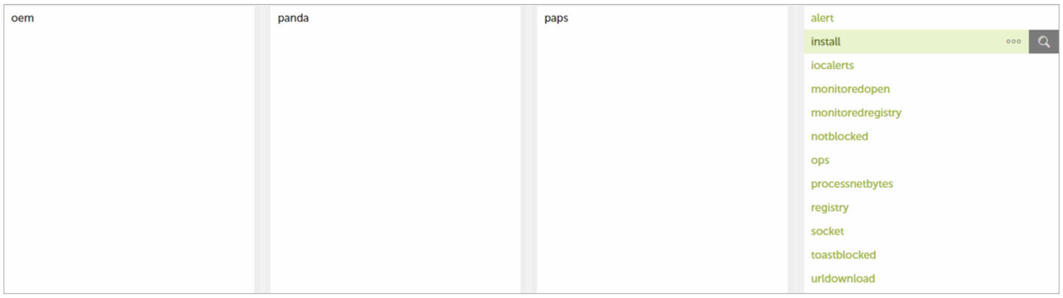
> For detailed information on how to create alerts, see the **Alerts** chapter in the *Advanced Reporting Tools Administration Guide*.

To configure an alert:

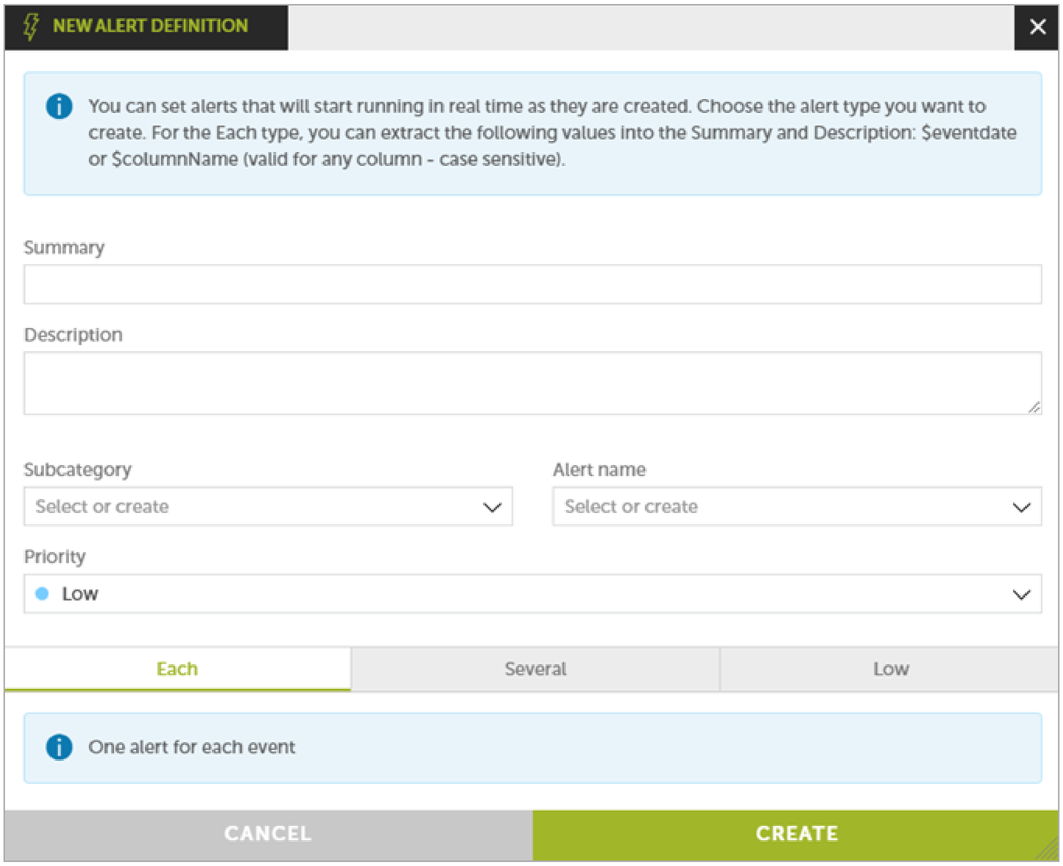
1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, from the navigation menu, select **Data Search** .
4. Select the time period you want to create the alert for.



5. Select the appropriate data table.
   *For information on the available data tables and fields, see the **Knowledge Table** chapter in the Advanced Reporting Tool Administration Guide.*



6. Apply filters and data transformations to generate the information table you want.
   *The legend bar lists the fields displayed in the data table. You can click **Toggle Query Editor** to display the exact settings of the data source that feeds the data table, including the specified time interval. You can experiment with multiple variations of the chart using the SQL statement as a starting point. For sample SQL queries, see Appendix: Sample SQL Query Text.*
7. In the toolbar, click **New Alert Definition** .
   The New Alert Definition dialog box opens.



You can set alerts that will start running in real time as they are created. Choose the alert type you want to create. For the Each type, you can extract the following values into the Summary and Description: $eventdate or $columnName (valid for any column - case sensitive).

Summary

Description

Subcategory: Select or create

Alert name: Select or create

Priority: ● Low

One alert for each event

8. Type a **Summary** and **Description** for the alert.
9. Type or select a **Subcategory** for the alert.
10. Type or select an **Alert name**.
11. To specify the alert frequency, select a tab.
    - To generate an alert for each event entry in the table, select **Each**.
    - To generate a single alert for number of events (**Threshold**) during the specified time **Period**, select **Several**.
    - To generate a single alert when the number of events received (**Threshold**) is less than indicated for the specified time **Period**, select **Low**.
12. Create post filters, if required.
    Post filters enable you to edit the features of the generated alerts before they are sent, as well as delete them if they meet specified criteria. For more information, see ***Creating Post Filters*** *in the Advanced Reporting Tool Administration Guide.*
13. Specify the delivery conditions.
    Delivery conditions include the delivery schedule and method. For more information, see ***Creating Delivery Conditions*** *in the Advanced Reporting Tool Administration Guide.*
14. Create an anti-flooding policy, if required.
    An anti-flooding policy allows complete, temporary suspension of alert generation when the rate of alerts exceeds a threshold defined by the administrator. For more information, see ***Creating Anti-flooding Policies*** *in the Advanced Reporting Tool Administration Guide.*
15. Create a new delivery policy and assign it to the alert you created.
    Alert policies, also called sending policies, define how the alerts are sent. For more information, see ***Creating Alert Policies*** *in the Advanced Reporting Tool Administration Guide.*

Example: Create Alerts for RDP Sessions

Remote tools are a common attack vector. This example creates an alert to check for regular use of remote access tools and to provide early insight into misuse or hacking attacks.

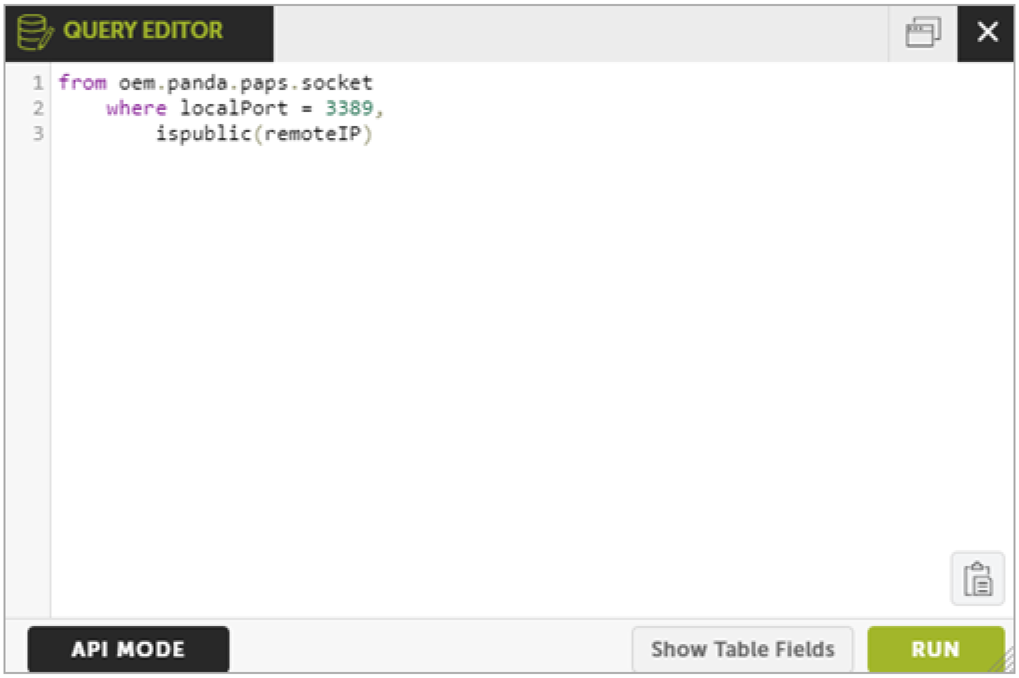
To configure alerts for RDP sessions that occur in a 10-minute period:

1. In the Adaptive Defense 360 console, select **Status**.
2. From the navigation menu, select **Advanced Visualization Tool**.
3. In the window that opens, in the left pane, click **Data Search** .
4. Select the **oem.panda.paps.socket** table for the time period you want.
5. In the toolbar, select **Toggle Query Editor** .
6. Paste this code into the text box:

```
from oem.panda.paps.socket

where localPort = 3389,

ispublic(remoteIP)
```



```
from oem.panda.paps.socket
    where localPort = 3389,
        ispublic(remoteIP)
```

7. Click **Run**.
   Confirm that the data table shows the information you want. For more sample SQL queries, see Appendix: Sample SQL Query Text.
8. Click **New Alert Definition** in the toolbar.
9. Specify the alert parameters to include in the alert (for example, in the email subject line or body).
   a. In the **Summary** text box, type a brief name for the alert.
   b. In the **Description** text box, type a description or add information fields from the data table.
      For example, if the data table includes an eventdate column, type $eventdate to add the date to the Description.
   c. From the **Subcategory** list, select or type a subcategory for the alert.

   d. From the **Alert name** list, select or type a name for the alert.
   e. From the **Priority** list, select a priority level for the alert.

10. To trigger an alert when a specified number of events occur within a specified time period, click **Several**.
    This type of alert can be useful to monitor for potentially malicious activity and to be informed when a threshold is exceeded.
11. From the **Period** drop-down list, select **10m**.
12. In the **Threshold** text box, type the number of times an event will occur before an alert is sent.
    For example, if you type 3, then when an RDP session starts 3 times or more on port 3389 during the 10-minute period, an alert is sent at the end of the 10-minute period.
13. Click **Create**.
14. Create post filters, if required.
    *For more information, see **Creating Post Filters** in the Advanced Reporting Tool Administration Guide.*
15. Specify the delivery method.
    *For more information, see **Creating Delivery Conditions** in the Advanced Reporting Tool Administration Guide.*
16. Create an anti-flooding policy, if required.
    *For more information, see **Creating Anti-flooding Policies** in the Advanced Reporting Tool Administration Guide.*
17. Create a new delivery policy and assign it to the alert you created.
    *For more information, see **Creating Alert Policies** in the Advanced Reporting Tool Administration Guide.*

ⓘ For information on how to disable predefined alerts, see the Support Center article, How to modify and disable the Advanced Reporting Tool predefined alerts.

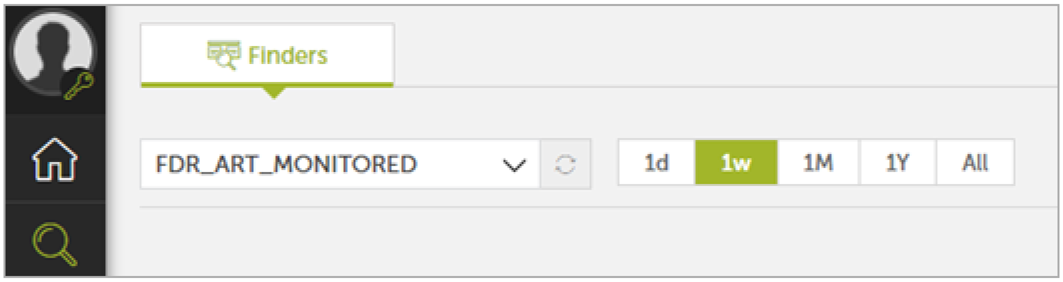
Appendix: Sample SQL Query Text

Panda Adaptive Defense collects information and sends it to the Advanced Reporting Tools service, where it is organized in to data tables. Each line of a table is an event monitored by Panda Adaptive Defense. The tables contain a series of specific fields, as well as common fields that appear in all of the tables and provide information such as when the event occurred, the computer where it was detected, the computer IP address, etc. This appendix provides sample SQL query text that you can use to filter the data in these tables.

> ⓘ For information on the available data tables and fields, see the **Knowledge Table** chapter in the *Advanced Reporting Tool Administration Guide*.

To use sample SQL query text:

1. Select **Data Search** 🔍.
2. Select the appropriate table for the time period you want.
   For example, to create a query to show remote desktop connections detected to or from an external IP address, select the oem.panda.paps.socket table.



3. In the toolbar, click **Toggle Query Editor** .
4. Clear the existing query from the editor text box.
5. Paste the sample code in the text box.
6. Click **Run**.

Remote Desktop Connection (Port 3389) Detected To or From External IP

Remote Desktop Services that are open without proper security measures are at a high risk of attack. Attackers take advantage of this through Brute Force attacks or they enter the network with stolen credentials. Many ransomware attacks start through open Remote Desktop Services.

> We recommend that you set proper security measures to prevent attacks through these services.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket

where localPort = 3389,

ispublic(remoteIP)
```

Top 5 Data Volume Received by Applications in Bytes (1 Week)

When you keep track of traffic consumed by each application, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.processnetbytes

Sample Code

```
from oem.panda.paps.processnetbytes where endswith(path,".exe")

group every 30m by path

every 0

select peek(path, re("\\\\(\\w+.\\w+)$"), 0) as executable

select sum(bytesReceived) as bytesReceived,

bytesReceived > 1073741824 as `+1G`,

bytesReceived > 2147483648 as `+2G`,

bytesReceived > 3221225472 as `+3G`,

bytesReceived > 4294967296 as `+4G`,
bytesReceived > 5368709120 as `+5G`,

bytesReceived > 6442450944 as `+6G`,

bytesReceived > 7516192768 as `+7G`,

bytesReceived > 8589934592 as `+8G`,

bytesReceived > 9663676416 as `+9G`,

bytesReceived > 10737418240 as `+10G`
```

Top 5 Data Volume Sent by Applications in Bytes (1 Week)

When you keep track of traffic sent per application, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.processnetbytes

Sample Code

```
from oem.panda.paps.processnetbytes where endswith(path,".exe") GOOD

group every 30m by path

every 0

select peek(path, re("\\\\(\\w+.\\w+)$"), 0) as executable

select sum(bytesSent) as bytesSent,

bytesSent > 1073741824 as `+1G`,

bytesSent > 2147483648 as `+2G`,

bytesSent > 3221225472 as `+3G`,

bytesSent > 4294967296 as `+4G`,

bytesSent > 5368709120 as `+5G`,

bytesSent > 6442450944 as `+6G`,

bytesSent > 7516192768 as `+7G`,

bytesSent > 8589934592 as `+8G`,

bytesSent > 9663676416 as `+9G`,

bytesSent > 10737418240 as `+10G`
```

Top 5 Data Volume Received by Machine in Bytes (1 Week)

When you keep track of downloaded traffic per application, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.processnetbytes

Sample Code

```
from oem.panda.paps.processnetbytes

group every 30m by machineName

every 0

select sum(bytesReceived) as bytesReceived,

bytesReceived > 1073741824 as `+1G`,

bytesReceived > 2147483648 as `+2G`,

bytesReceived > 3221225472 as `+3G`,

bytesReceived > 4294967296 as `+4G`,

bytesReceived > 5368709120 as `+5G`,

bytesReceived > 6442450944 as `+6G`,

bytesReceived > 7516192768 as `+7G`,

bytesReceived > 8589934592 as `+8G`,

bytesReceived > 9663676416 as `+9G`,

bytesReceived > 10737418240 as `+10G`
```

Top 5 Data Volume Sent by Machine in Bytes (1 Week)

When you keep track of uploaded traffic per application, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.processnetbytes

Sample Code

```
from oem.panda.paps.processnetbytes
group every 30m by machineName
every 0
select sum(bytesSent) as bytesSent,
bytesSent > 1073741824 as `+1G`,
bytesSent > 2147483648 as `+2G`,
bytesSent > 3221225472 as `+3G`,
bytesSent > 4294967296 as `+4G`,
bytesSent > 5368709120 as `+5G`,
bytesSent > 6442450944 as `+6G`,
bytesSent > 7516192768 as `+7G`,
bytesSent > 8589934592 as `+8G`,
bytesSent > 9663676416 as `+9G`,
bytesSent > 10737418240 as `+10G`
```

Top 5 Data Volume Sent by User in Bytes (1 Week)

When you keep track of uploaded traffic per user, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.processnetbytes

Sample Code

```
from oem.panda.paps.processnetbytes
group every 30m by user
every 0
select sum(bytesSent) as bytesSent,
bytesSent > 1073741824 as `+1G`,
bytesSent > 2147483648 as `+2G`,
bytesSent > 3221225472 as `+3G`,
bytesSent > 4294967296 as `+4G`,
bytesSent > 5368709120 as `+5G`,
bytesSent > 6442450944 as `+6G`,
bytesSent > 7516192768 as `+7G`,
bytesSent > 8589934592 as `+8G`,
bytesSent > 9663676416 as `+9G`,
bytesSent > 10737418240 as `+10G`
```

Top 5 Data Volume Received by User in Bytes (1 Week)

When you keep track of downloaded traffic per user, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.processnetbytes

Sample Code

```
from oem.panda.paps.processnetbytes
group every 30m by user
every 0
select sum(bytesReceived) as bytesReceived,
bytesReceived > 1073741824 as `+1G`,
bytesReceived > 2147483648 as `+2G`,
bytesReceived > 3221225472 as `+3G`,
bytesReceived > 4294967296 as `+4G`,
bytesReceived > 5368709120 as `+5G`,
bytesReceived > 6442450944 as `+6G`,
bytesReceived > 7516192768 as `+7G`,
bytesReceived > 8589934592 as `+8G`,
bytesReceived > 9663676416 as `+9G`,
bytesReceived > 10737418240 as `+10G`
```

Top 5 TCP Communication Ports Used to External IPs (Download)

When you keep track of TCP ports used for upload to external IP addresses, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket

where ispublic(remoteIP)

group every 30m by protocol, localPort, direction

every 0

select count() as count,

count > 100 as `+100_times`,

count > 500 as `+500_times`,

count > 1000 as `+1000_times`,

count > 2000 as `+2000_times`,

count > 5000 as `+5000_times`,

count > 10000 as `+10000_times`

where protocol = "TCP"

where direction = "Down"
```

Top 5 TCP Communication Ports Used to Upload to External IPs

When you keep track of TCP ports used to upload to external IP addresses, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

> We recommend that you monitor and set active alerts if processes consume more data than normal. This will help you to identify many different problems and act if needed.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket
where ispublic(remoteIP)
group every 30m by protocol, localPort, direction
every 0
select count() as count,
count > 100 as `+100_times`,
count > 500 as `+500_times`,
count > 1000 as `+1000_times`,
count > 2000 as `+2000_times`,
count > 5000 as `+5000_times`,
count > 10000 as `+10000_times`
where protocol = "TCP"
where direction = "Up"
```

Top 5 UDP Communication Ports Used to Download to External IPs

When you keep track of UDP ports used to download to external IP addresses, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket
where ispublic(remoteIP)
group every 30m by protocol, localPort, direction
every 0
select count() as count,
count > 100 as `+100_times`,
count > 500 as `+500_times`,
count > 1000 as `+1000_times`,
count > 2000 as `+2000_times`,
count > 5000 as `+5000_times`,
count > 10000 as `+10000_times`
where protocol = "UDP"
where direction = "Down"
```

Top 5 UDP Communication Ports Used to Upload to External IPs

When you keep track of UDP ports used to upload to external IP addresses, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket
where ispublic(remoteIP)
group every 30m by protocol, localPort, direction
every 0
select count() as count,
count > 100 as `+100_times`,
count > 500 as `+500_times`,
count > 1000 as `+1000_times`,
count > 2000 as `+2000_times`,
count > 5000 as `+5000_times`,
count > 10000 as `+10000_times`
where protocol = "UDP"
where direction = "Up"
```

Top 10 Countries and Ports (Download 1 Week)

When you keep track of the top countries and ports used for downloads, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket where ispublic(remoteIP)
select mmcountry(remoteIP) as CC
where isnotnull(CC)
group every 30m by CC, localPort, protocol, direction
```

```
every 0
select count() as count,
count > 100 as `+100`,
count > 300 as `+300`,
count > 500 as `+500`,
count > 800 as `+800`,
count > 1000 as `+1000`,
count > 1500 as `+1500`,
count > 2000 as `+2000`,
count > 5000 as `+5000`,
count > 10000 as `+10000`,
count > 15000 as `+15000`,
count > 20000 as `+20000`
where direction = "Down"
```

Top 10 Countries and Ports (Upload 1 Week)

When you keep track of the top countries and ports used for uploads, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.socket

Sample Code

```
from oem.panda.paps.socket where ispublic(remoteIP)
select mmcountry(remoteIP) as CC
where isnotnull(CC)
group every 30m by CC, localPort, protocol, direction
every 0
select count() as count,
count > 1 as `+1`,
count > 50 as `+50`,
count > 100 as `+100`,
count > 300 as `+300`,
count > 500 as `+500`,
count > 800 as `+800`,
count > 1000 as `+1000`,
count > 1500 as `+1500`,
count > 2000 as `+2000`,
count > 5000 as `+5000`,
count > 10000 as `+10000`,
count > 15000 as `+15000`,
count > 20000 as `+20000`
where direction = "Up"
```

Total Download Count of Executable Files (.EXE in 1 Week)

When you keep track of the top executable files that users download, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.urldownload

Sample Code

```
from oem.panda.paps.urldownload
where endswith(url, ".exe")
group every 30m
every 0
select count() as count
```

Total Download Count of Compressed Format Files (.ZIP, .RAR , .7Z in 1 Week)

When you keep track of the top compressed files that users download, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.urldownload

Sample Code

```
from oem.panda.paps.urldownload
where has(url, ".zip", ".rar", ".7z")
group every 30m
every 0
select count() as count
```

Total Download Count of Office Documents (.DOC* , .XLS* , .PPT* , .OCT)

When you keep track of the top Office document file types that users download, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.urldownload

Sample Code

```
from oem.panda.paps.urldownload

where has(url, ".doc", ".xls", ".ppt" , ".oct")

group every 30m

every 0

select count() as count
```

Torrent Activity Detected

When you keep track of user Torrent activity, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.urldownload

Sample Code

```
from oem.panda.paps.urldownload

where url -> "torrent"

group every 30m

every 0

select count() as count
```

Malware and Potential Unwanted Programs (PUP) in Numbers (1 Week)

When you keep track of the malware and PUPs per week, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.alert

Sample Code

```
from oem.panda.paps.alert

group every 30m by alertType, executionStatus

every 0

select count() as count
```

Vulnerable Applications or Outdated Software Executed

When you keep track of the vulnerable applications or outdated software that users use, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.ops

Sample Code

```
from oem.panda.paps.ops where isnotnull(ocsVer), endswith(childPath, ".exe") select subs(childPath, re(".*\\\\"), template("")) as executablename, lower(executablename) as executablename2, split(executablename2, ".exe", 0) as executable

group every 30m

every 0

select count() as count
```

Number of Possible Vulnerable Applications Detected

When you keep track of the possible vulnerable applications used, it helps you to quickly identify misuse, application errors, possible data exfiltration, and more.

Table

oem.panda.paps.vulnerableappsfound

Sample Code

```
from oem.panda.paps.vulnerableappsfound

group every 30m by companyName

every 0

select count() as count
```