# Forcepoint FlexEdge Secure SD-WAN

## E-Mail Virenfilterung Server Firewall

**Report period**
From: 2024-10-01 00:00:00+0200
To: 2024-11-01 00:00:00+0100

Forcepoint

# Table of Contents

**Report run by**
jens

**SD-WAN Manager Console version**
7.1.4, build 11432

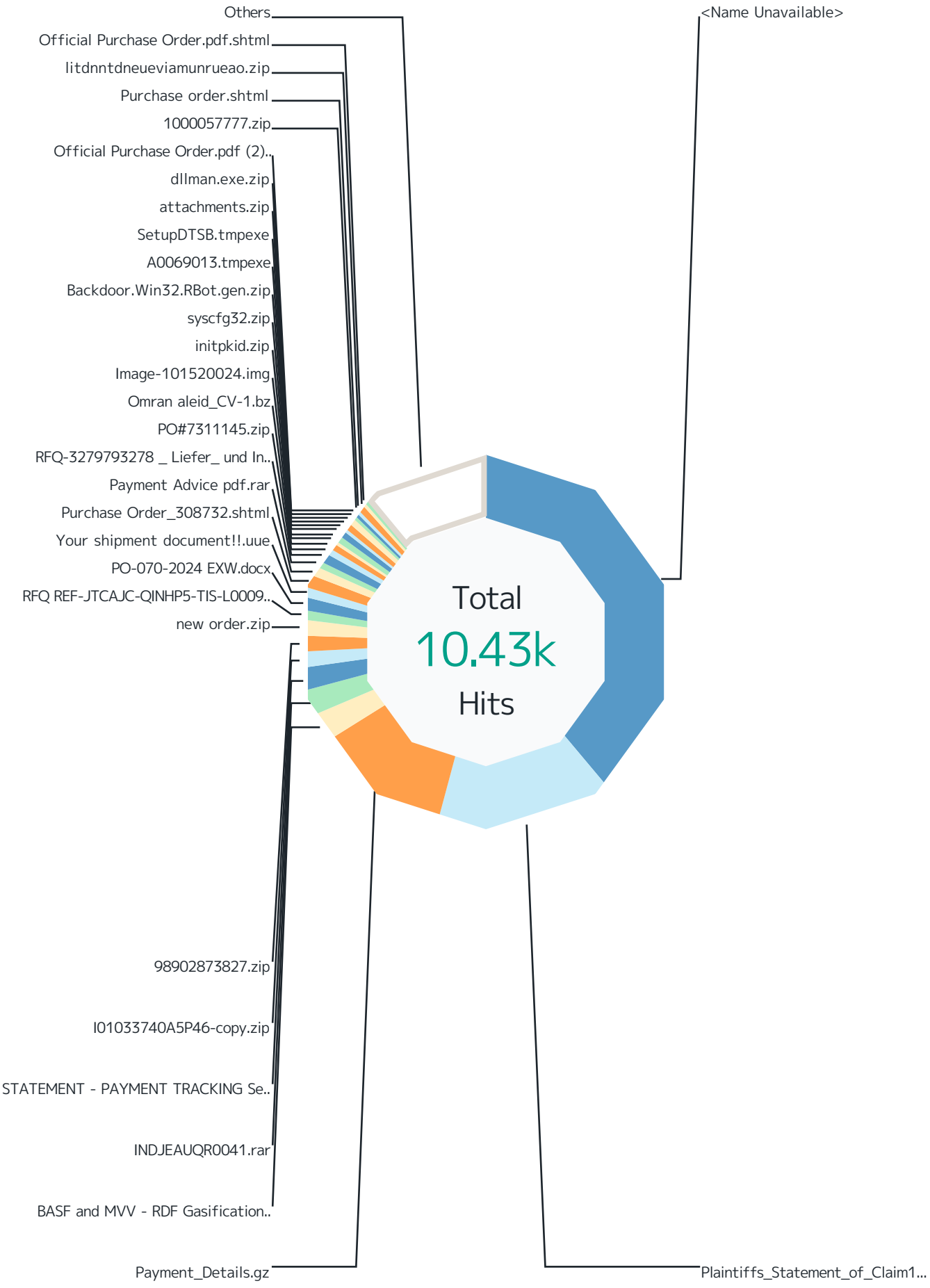
**Update version**
1794

**Report started**
2024-11-02 09:39:36+0100

**Report run time**
03:33:11

**Filters used**
Match All

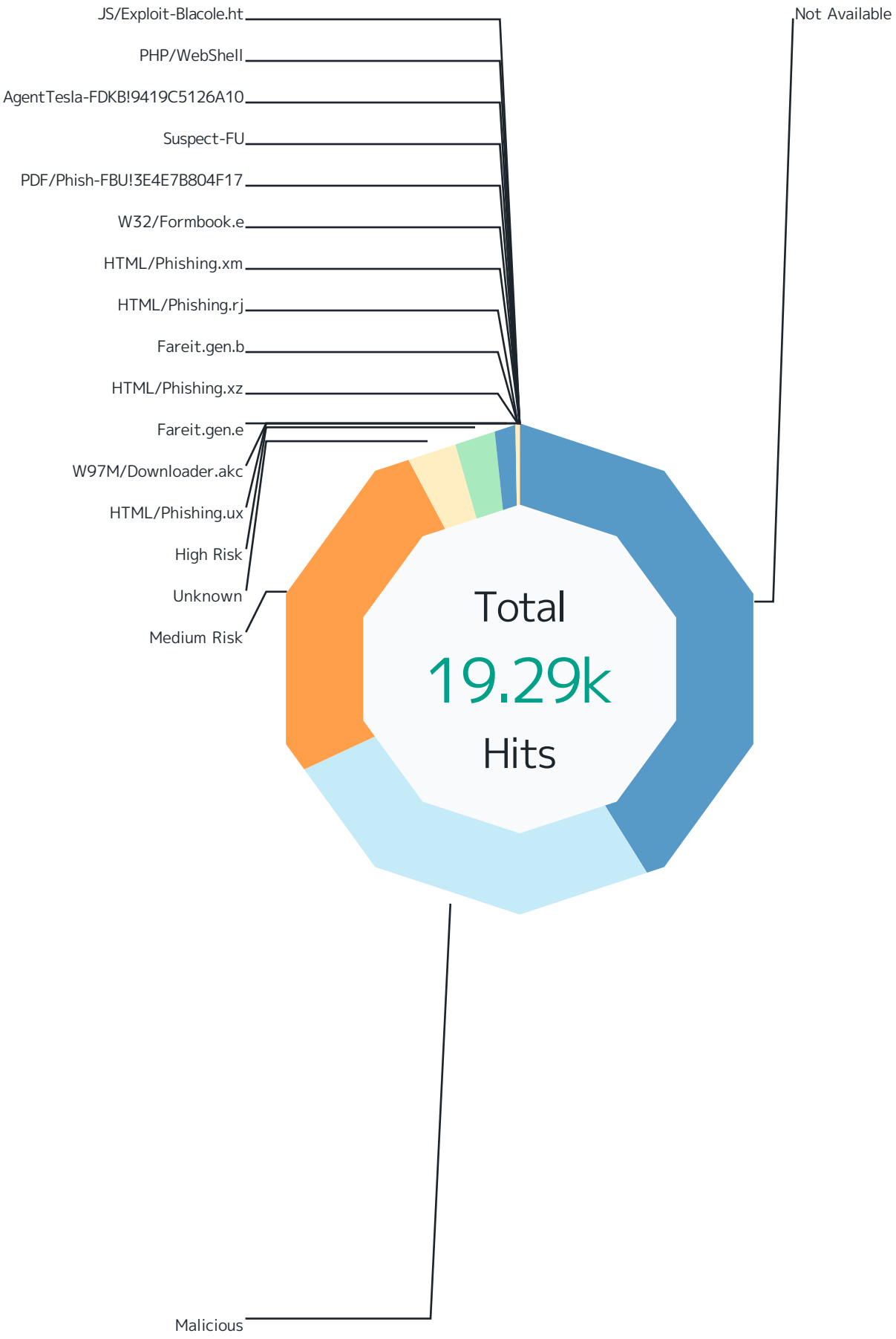
# Virenfilterung MXe



| Records by file name | Hits | % |
|---|---|---|
| <Name Unavailable> | 4.06k | 39.0 % |
| Plaintiffs_Statement_of_Claim1.zip | 1.58k | 15.2 % |
| Payment_Details.gz | 1.25k | 11.9 % |
| BASF and MVV - RDF Gasification Study - Final (241007).zip | 268 | 2.6 % |
| INDJEAUQR0041.rar | 216 | 2.1 % |
| STATEMENT - PAYMENT TRACKING Sept 2024.docx | 201 | 1.9 % |
| I01033740A5P46-copy.zip | 163 | 1.6 % |
| 98902873827.zip | 142 | 1.4 % |
| new order.zip | 129 | 1.2 % |
| RFQ REF-JTCAJC-QINHP5-TIS-L0009- (AL DHAFRA) AL JABER - SUPPLY.zip | 110 | 1.1 % |
| PO-070-2024 EXW.docx | 103 | 1.0 % |
| Your shipment document!!.uue | 96 | 0.9 % |
| Purchase Order_308732.shtml | 94 | 0.9 % |
| Payment Advice pdf.rar | 90 | 0.9 % |
| RFQ-3279793278 _ Liefer_ und Installationsarbeiten _ fur das Al-Delta-Projekt #Ausschreibung 2883.. | 79 | 0.8 % |
| PO#7311145.zip | 76 | 0.7 % |
| Omran aleid_CV-1.bz | 57 | 0.5 % |
| Image-101520024.img | 51 | 0.5 % |
| initpkid.zip | 48 | 0.5 % |
| syscfg32.zip | 48 | 0.5 % |
| Backdoor.Win32.RBot.gen.zip | 48 | 0.5 % |
| A0069013.tmpexe | 48 | 0.5 % |
| SetupDTSB.tmpexe | 48 | 0.5 % |
| attachments.zip | 46 | 0.4 % |
| dllman.exe.zip | 42 | 0.4 % |
| Official Purchase Order.pdf (2).shtml | 38 | 0.4 % |
| 1000057777.zip | 33 | 0.3 % |
| Purchase order.shtml | 33 | 0.3 % |
| litdnntdneueviamunrueao.zip | 32 | 0.3 % |
| Official Purchase Order.pdf.shtml | 32 | 0.3 % |
| Others | 1.16k | 11.2 % |
| **Total** | **10.43k** | **100 %** |

## Top File Types by Scan Result

Top 10 file types by scan result.


JS/Exploit-Blacole.ht
PHP/WebShell
AgentTesla-FDKB!9419C5126A10
Suspect-FU
PDF/Phish-FBU!3E4E7B804F17
W32/Formbook.e
HTML/Phishing.xm
HTML/Phishing.rj
Fareit.gen.b
HTML/Phishing.xz
Fareit.gen.e
W97M/Downloader.akc
HTML/Phishing.ux
High Risk
Unknown
Medium Risk
Not Available
Malicious
Total
19.29k
Hits

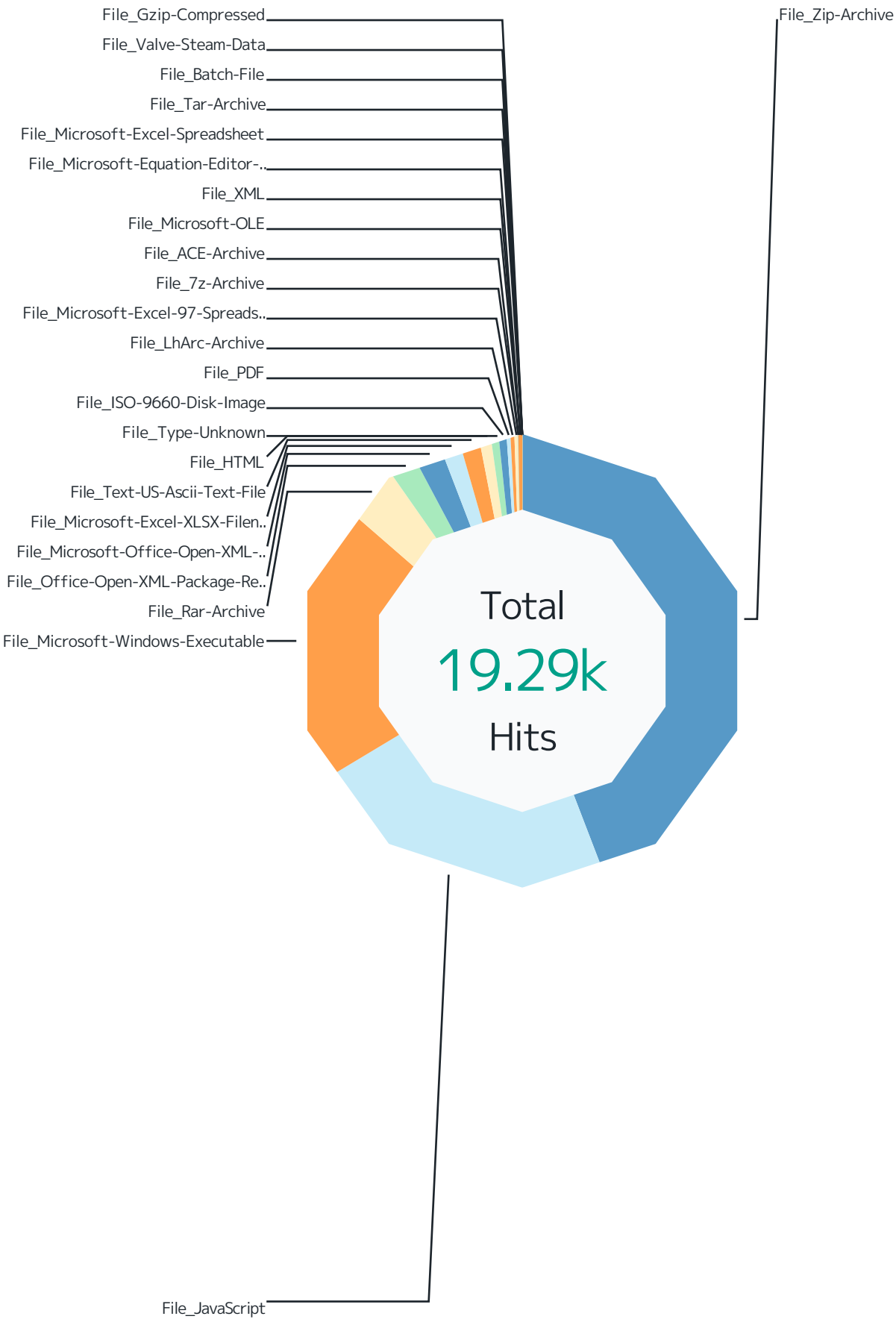
| Scan Result | Hits | % |
|---|---|---|
| **Not Available** | **7.93k** | **41.1 %** |
| File_Zip-Archive | 7.62k | 39.5 % |
| File_Microsoft-Office-Open-XML-Document | 279 | 1.4 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 30 | 0.2 % |
| File_Microsoft-Excel-Spreadsheet | 3 | 0.0 % |
| **Malicious** | **5.19k** | **26.9 %** |
| File_Microsoft-Windows-Executable | 3.68k | 19.1 % |
| File_Rar-Archive | 612 | 3.2 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 270 | 1.4 % |
| File_Zip-Archive | 169 | 0.9 % |
| File_HTML | 98 | 0.5 % |
| File_Type-Unknown | 97 | 0.5 % |
| File_ISO-9660-Disk-Image | 72 | 0.4 % |
| File_Microsoft-Office-Open-XML-Document | 53 | 0.3 % |
| File_Office-Open-XML-Package-Relations-Item | 32 | 0.2 % |
| File_LhArc-Archive | 30 | 0.2 % |
| File_Text-US-Ascii-Text-File | 20 | 0.1 % |
| File_Microsoft-Excel-97-Spreadsheet | 20 | 0.1 % |
| File_7z-Archive | 14 | 0.1 % |
| File_Microsoft-OLE | 9 | 0.0 % |
| File_PDF | 3 | 0.0 % |
| File_Microsoft-Excel-Spreadsheet | 3 | 0.0 % |
| File_Tar-Archive | 3 | 0.0 % |
| File_Batch-File | 3 | 0.0 % |
| File_JavaScript | 1 | 0.0 % |
| File_Valve-Steam-Data | 1 | 0.0 % |
| **Medium Risk** | **4.66k** | **24.1 %** |
| File_JavaScript | 4.28k | 22.2 % |
| File_Office-Open-XML-Package-Relations-Item | 201 | 1.0 % |
| File_Microsoft-Windows-Executable | 55 | 0.3 % |
| File_HTML | 41 | 0.2 % |
| File_PDF | 33 | 0.2 % |
| File_ISO-9660-Disk-Image | 18 | 0.1 % |
| File_Rar-Archive | 12 | 0.1 % |
| File_XML | 9 | 0.0 % |
| File_Microsoft-Office-Open-XML-Document | 6 | 0.0 % |
| File_Zip-Archive | 1 | 0.0 % |
| File_Type-Unknown | 1 | 0.0 % |
| **Unknown** | **643** | **3.3 %** |

| Scan Result | Hits | % |
|---|---|---|
| File_Zip-Archive | 635 | 3.3 % |
| File_Microsoft-Office-Open-XML-Document | 6 | 0.0 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 2 | 0.0 % |
| **High Risk** | **572** | **3.0 %** |
| File_Microsoft-Windows-Executable | 146 | 0.8 % |
| File_Office-Open-XML-Package-Relations-Item | 131 | 0.7 % |
| File_Rar-Archive | 130 | 0.7 % |
| File_Zip-Archive | 71 | 0.4 % |
| File_LhArc-Archive | 22 | 0.1 % |
| File_PDF | 20 | 0.1 % |
| File_JavaScript | 19 | 0.1 % |
| File_HTML | 14 | 0.1 % |
| File_Type-Unknown | 10 | 0.1 % |
| File_Microsoft-Equation-Editor-Document | 6 | 0.0 % |
| File_7z-Archive | 2 | 0.0 % |
| File_ISO-9660-Disk-Image | 1 | 0.0 % |
| **HTML/Phishing.ux** | **239** | **1.2 %** |
| File_Text-US-Ascii-Text-File | 239 | 1.2 % |
| **W97M/Downloader.akc** | **15** | **0.1 %** |
| File_Microsoft-Excel-97-Spreadsheet | 15 | 0.1 % |
| **Fareit.gen.e** | **9** | **0.0 %** |
| File_ACE-Archive | 9 | 0.0 % |
| **HTML/Phishing.xz** | **8** | **0.0 %** |
| File_HTML | 8 | 0.0 % |
| **Fareit.gen.b** | **6** | **0.0 %** |
| File_ACE-Archive | 6 | 0.0 % |
| **HTML/Phishing.rj** | **6** | **0.0 %** |
| File_Text-US-Ascii-Text-File | 6 | 0.0 % |
| **HTML/Phishing.xm** | **4** | **0.0 %** |
| File_HTML | 4 | 0.0 % |
| **W32/Formbook.e** | **3** | **0.0 %** |
| File_Rar-Archive | 3 | 0.0 % |
| **PDF/Phish-FBU!3E4E7B804F17** | **1** | **0.0 %** |
| File_PDF | 1 | 0.0 % |
| **Suspect-FU** | **1** | **0.0 %** |
| File_Zip-Archive | 1 | 0.0 % |
| **AgentTesla-FDKB!9419C5126A10** | **1** | **0.0 %** |
| File_Zip-Archive | 1 | 0.0 % |
| **PHP/WebShell** | **1** | **0.0 %** |

| Scan Result | Hits | % |
|---|---|---|
| File_Gzip-Compressed | 1 | 0.0 % |
| **JS/Exploit-Blacole.ht** | **1** | **0.0 %** |
| File_JavaScript | 1 | 0.0 % |
| **Total** | **19.29k** | **100 %** |

## Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.


File_Gzip-Compressed
File_Valve-Steam-Data
File_Batch-File
File_Tar-Archive
File_Microsoft-Excel-Spreadsheet
File_Microsoft-Equation-Editor-..
File_XML
File_Microsoft-OLE
File_ACE-Archive
File_7z-Archive
File_Microsoft-Excel-97-Spreads..
File_LhArc-Archive
File_PDF
File_ISO-9660-Disk-Image
File_Type-Unknown
File_HTML
File_Text-US-Ascii-Text-File
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-Office-Open-XML-..
File_Office-Open-XML-Package-Re..
File_Rar-Archive
File_Microsoft-Windows-Executable
File_Zip-Archive
Total
19.29k
Hits
File_JavaScript

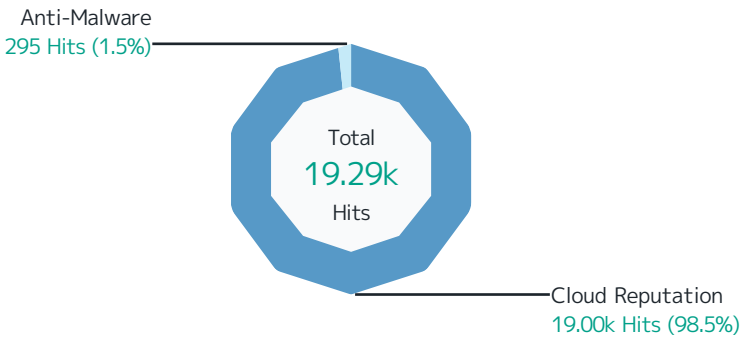
| Responding Scanner | Hits | % |
|---|---|---|
| **File_Zip-Archive** | **8.50k** | **44.1 %** |
| Not Available | 7.62k | 39.5 % |
| Unknown | 635 | 3.3 % |
| Malicious | 169 | 0.9 % |
| High Risk | 71 | 0.4 % |
| Medium Risk | 1 | 0.0 % |
| Suspect-FU | 1 | 0.0 % |
| AgentTesla-FDKB!9419C5126A10 | 1 | 0.0 % |
| **File_JavaScript** | **4.30k** | **22.3 %** |
| Medium Risk | 4.28k | 22.2 % |
| High Risk | 19 | 0.1 % |
| Malicious | 1 | 0.0 % |
| JS/Exploit-Blacole.ht | 1 | 0.0 % |
| **File_Microsoft-Windows-Executable** | **3.88k** | **20.1 %** |
| Malicious | 3.68k | 19.1 % |
| High Risk | 146 | 0.8 % |
| Medium Risk | 55 | 0.3 % |
| **File_Rar-Archive** | **757** | **3.9 %** |
| Malicious | 612 | 3.2 % |
| High Risk | 130 | 0.7 % |
| Medium Risk | 12 | 0.1 % |
| W32/Formbook.e | 3 | 0.0 % |
| **File_Office-Open-XML-Package-Relations-Item** | **364** | **1.9 %** |
| Medium Risk | 201 | 1.0 % |
| High Risk | 131 | 0.7 % |
| Malicious | 32 | 0.2 % |
| **File_Microsoft-Office-Open-XML-Document** | **344** | **1.8 %** |
| Not Available | 279 | 1.4 % |
| Malicious | 53 | 0.3 % |
| Medium Risk | 6 | 0.0 % |
| Unknown | 6 | 0.0 % |
| **File_Microsoft-Excel-XLSX-Filename-Extension** | **302** | **1.6 %** |
| Malicious | 270 | 1.4 % |
| Not Available | 30 | 0.2 % |
| Unknown | 2 | 0.0 % |
| **File_Text-US-Ascii-Text-File** | **265** | **1.4 %** |
| HTML/Phishing.ux | 239 | 1.2 % |
| Malicious | 20 | 0.1 % |
| HTML/Phishing.rj | 6 | 0.0 % |

| Responding Scanner | Hits | % |
|---|---|---|
| **File_HTML** | **165** | **0.9 %** |
| Malicious | 98 | 0.5 % |
| Medium Risk | 41 | 0.2 % |
| High Risk | 14 | 0.1 % |
| HTML/Phishing.xz | 8 | 0.0 % |
| HTML/Phishing.xm | 4 | 0.0 % |
| **File_Type-Unknown** | **108** | **0.6 %** |
| Malicious | 97 | 0.5 % |
| High Risk | 10 | 0.1 % |
| Medium Risk | 1 | 0.0 % |
| **File_ISO-9660-Disk-Image** | **91** | **0.5 %** |
| Malicious | 72 | 0.4 % |
| Medium Risk | 18 | 0.1 % |
| High Risk | 1 | 0.0 % |
| **File_PDF** | **57** | **0.3 %** |
| Medium Risk | 33 | 0.2 % |
| High Risk | 20 | 0.1 % |
| Malicious | 3 | 0.0 % |
| PDF/Phish-FBU!3E4E7B804F17 | 1 | 0.0 % |
| **File_LhArc-Archive** | **52** | **0.3 %** |
| Malicious | 30 | 0.2 % |
| High Risk | 22 | 0.1 % |
| **File_Microsoft-Excel-97-Spreadsheet** | **35** | **0.2 %** |
| Malicious | 20 | 0.1 % |
| W97M/Downloader.akc | 15 | 0.1 % |
| **File_7z-Archive** | **16** | **0.1 %** |
| Malicious | 14 | 0.1 % |
| High Risk | 2 | 0.0 % |
| **File_ACE-Archive** | **15** | **0.1 %** |
| Fareit.gen.e | 9 | 0.0 % |
| Fareit.gen.b | 6 | 0.0 % |
| **File_Microsoft-OLE** | **9** | **0.0 %** |
| Malicious | 9 | 0.0 % |
| **File_XML** | **9** | **0.0 %** |
| Medium Risk | 9 | 0.0 % |
| **File_Microsoft-Equation-Editor-Document** | **6** | **0.0 %** |
| High Risk | 6 | 0.0 % |
| **File_Microsoft-Excel-Spreadsheet** | **6** | **0.0 %** |
| Not Available | 3 | 0.0 % |

| Responding Scanner | Hits | % |
|---|---|---|
| Malicious | 3 | 0.0 % |
| **File_Tar-Archive** | **3** | **0.0 %** |
| Malicious | 3 | 0.0 % |
| **File_Batch-File** | **3** | **0.0 %** |
| Malicious | 3 | 0.0 % |
| **File_Valve-Steam-Data** | **1** | **0.0 %** |
| Malicious | 1 | 0.0 % |
| **File_Gzip-Compressed** | **1** | **0.0 %** |
| PHP/WebShell | 1 | 0.0 % |
| **Total** | **19.29k** | **100 %** |

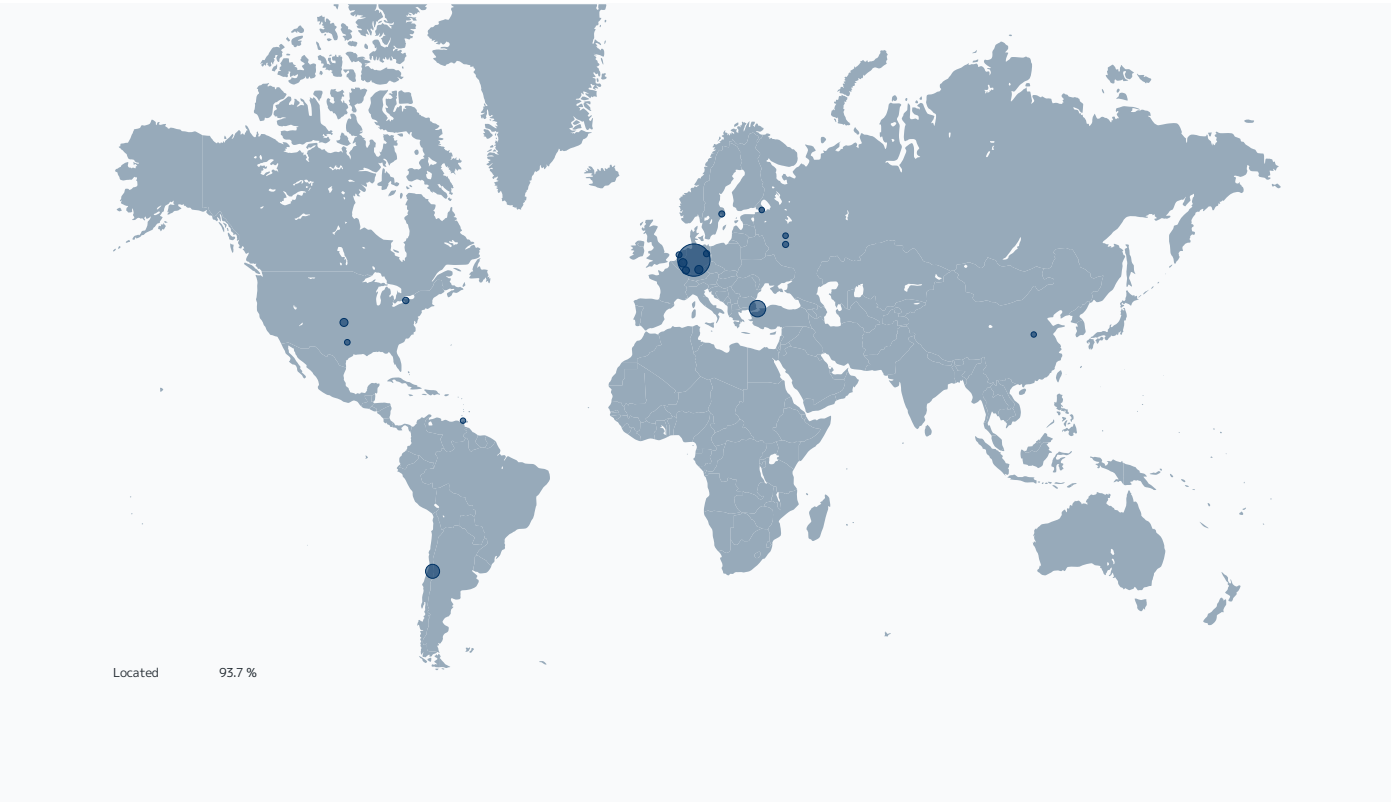
# Top File Types by Responding Scanner

Top 10 file types by responding scanner.



| Responding Scanner | Hits | % |
|---|---|---|
| **Cloud Reputation** | **19.00k** | **98.5 %** |
| File_Zip-Archive | 8.50k | 44.0 % |
| File_JavaScript | 4.30k | 22.3 % |
| File_Microsoft-Windows-Executable | 3.88k | 20.1 % |
| File_Rar-Archive | 754 | 3.9 % |
| File_Office-Open-XML-Package-Relations-Item | 364 | 1.9 % |
| File_Microsoft-Office-Open-XML-Document | 344 | 1.8 % |
| File_Microsoft-Excel-XLSX-Filename-Extension | 302 | 1.6 % |
| File_HTML | 153 | 0.8 % |
| File_Type-Unknown | 108 | 0.6 % |
| File_ISO-9660-Disk-Image | 91 | 0.5 % |
| File_PDF | 56 | 0.3 % |
| File_LhArc-Archive | 52 | 0.3 % |
| File_Text-US-Ascii-Text-File | 20 | 0.1 % |
| File_Microsoft-Excel-97-Spreadsheet | 20 | 0.1 % |
| File_7z-Archive | 16 | 0.1 % |
| File_Microsoft-OLE | 9 | 0.0 % |
| File_XML | 9 | 0.0 % |
| File_Microsoft-Equation-Editor-Document | 6 | 0.0 % |
| File_Microsoft-Excel-Spreadsheet | 6 | 0.0 % |
| File_Tar-Archive | 3 | 0.0 % |
| File_Batch-File | 3 | 0.0 % |
| File_Valve-Steam-Data | 1 | 0.0 % |
| **Anti-Malware** | **295** | **1.5 %** |
| File_Text-US-Ascii-Text-File | 245 | 1.3 % |
| File_Microsoft-Excel-97-Spreadsheet | 15 | 0.1 % |
| File_ACE-Archive | 15 | 0.1 % |
| File_HTML | 12 | 0.1 % |
| File_Rar-Archive | 3 | 0.0 % |
| File_Zip-Archive | 2 | 0.0 % |
| File_JavaScript | 1 | 0.0 % |
| File_PDF | 1 | 0.0 % |
| File_Gzip-Compressed | 1 | 0.0 % |
| **Total** | **19.29k** | **100 %** |

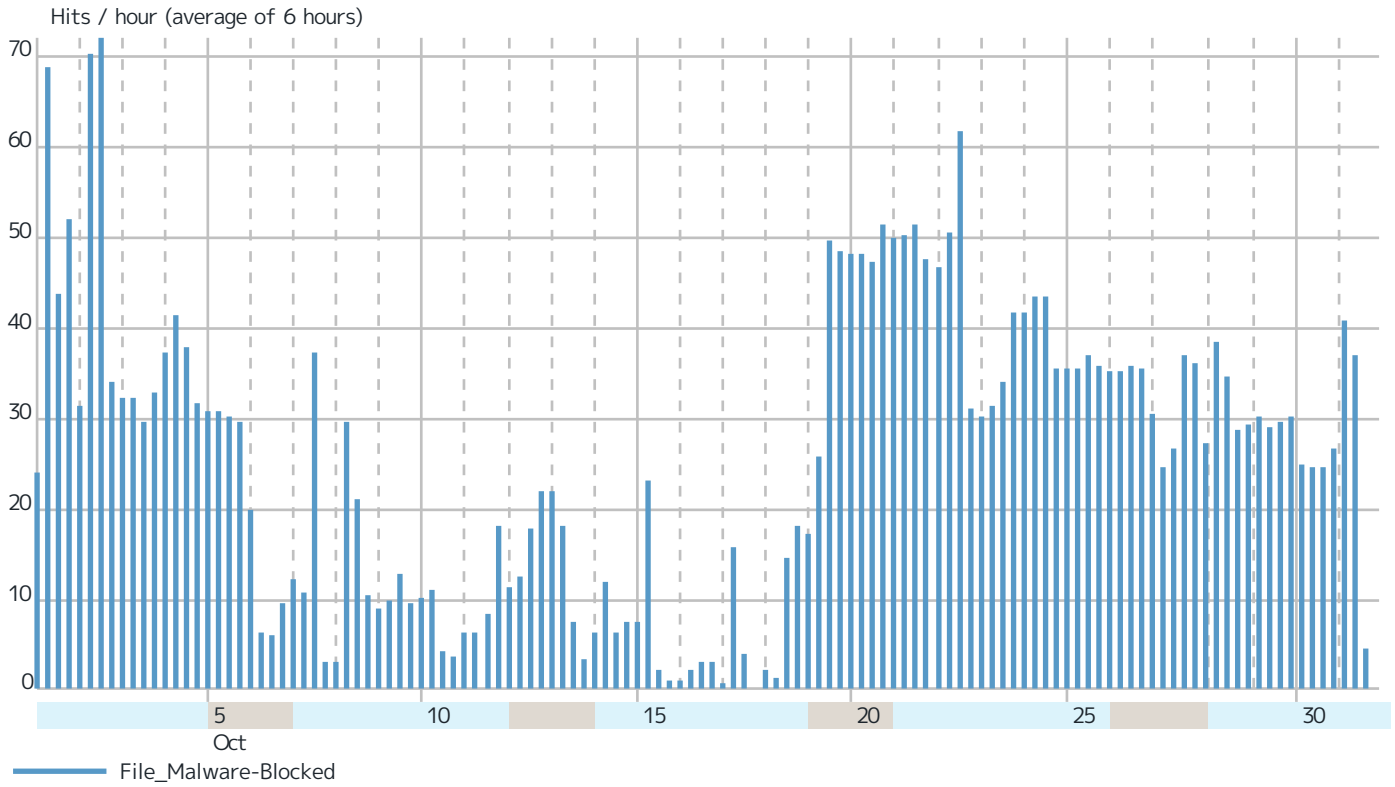
# Virenfilterung SRC IPs



| Records by src IP | | Hits | % |
|---|---|---|---|
| 89.107.187.19 | Germany | 7.38k | 38.3 % |
| 46.31.145.93 | Türkiye | 3.17k | 16.4 % |
| 38.7.201.35 | Santiago, Chile | 2.49k | 12.9 % |
| 94.100.132.209 | Saarbrücken, Germany | 536 | 2.8 % |
| 2a00:8a60:1:11::1005 | RWTH Aachen | 466 | 2.4 % |
| 159.183.93.69 | United States | 402 | 2.1 % |
| 188.68.63.98 | Nuremberg, Germany | 326 | 1.7 % |
| 185.244.194.184 | Nuremberg, Germany | 326 | 1.7 % |
| 136.243.49.10 | Berlin, Germany | 284 | 1.5 % |
| 91.195.205.100 | Tula, Russia | 258 | 1.3 % |
| 82.165.122.100 | Germany | 232 | 1.2 % |
| 193.42.39.230 | Stockholm, Sweden | 220 | 1.1 % |
| 172.245.244.79 | Buffalo, New York 14205, United States | 217 | 1.1 % |
| 37.120.175.171 | Nuremberg, Germany | 192 | 1.0 % |
| 2a00:8a60:1:11::1008 | RWTH Aachen | 182 | 0.9 % |
| 209.59.151.195 | United States | 152 | 0.8 % |
| 168.245.45.241 | United States | 148 | 0.8 % |
| 2a00:8a60:1:11::1007 | RWTH Aachen | 126 | 0.7 % |
| 172.245.225.48 | Dallas, Texas 75270, United States | 123 | 0.6 % |
| 91.224.62.122 | Russia | 114 | 0.6 % |
| 2a00:8a60:1:11::1006 | RWTH Aachen | 110 | 0.6 % |
| 23.94.177.42 | Buffalo, New York 14205, United States | 109 | 0.6 % |
| 72.11.156.199 | Amsterdam, The Netherlands | 104 | 0.5 % |
| 173.205.83.80 | Amsterdam, The Netherlands | 96 | 0.5 % |
| 194.87.68.202 | St Petersburg, Russia | 79 | 0.4 % |
| 181.188.28.140 | D'Abadie, Trinidad and Tobago | 60 | 0.3 % |
| 36.133.149.24 | China | 50 | 0.3 % |
| 159.183.98.52 | United States | 50 | 0.3 % |
| 5.230.34.191 | Germany | 42 | 0.2 % |
| 108.163.248.27 | United States | 37 | 0.2 % |
| Others | | 1.22k | 6.3 % |
| **Total** | | **19.29k** | **100 %** |

# SMTP Virus Filtering by Time

Top 10 file filtering situations on a timeline.



# About the FlexEdge Secure SD-WAN

Forcepoint FlexEdge Secure SD-WAN enables distributed organizations to improve application performance, simplify network management, and increase security— ensuring users can safely access any application from anywhere. By combining multi-link networking and intrusion prevention with zero-touch deployment and updating, it provides centralized visibility and control with high performance that scales to thousands of sites. When used with the Forcepoint ONE SSE platform, FlexEdge Secure SD-WAN delivers true SASE and secure branch solutions that boost productivity, cut costs, reduce risk, and streamline compliance.

For further information visit forcepoint.com/product/secure-sd-wan.

Forcepoint

**forcepoint.com**

## About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.