Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2021-08-01 00:00:00
To: 2021-09-01 00:00:00

Report

Report run by
jens

SMC version
6.10.2, build 11131

Update version
1382

Report started
2021-09-01 04:33:21

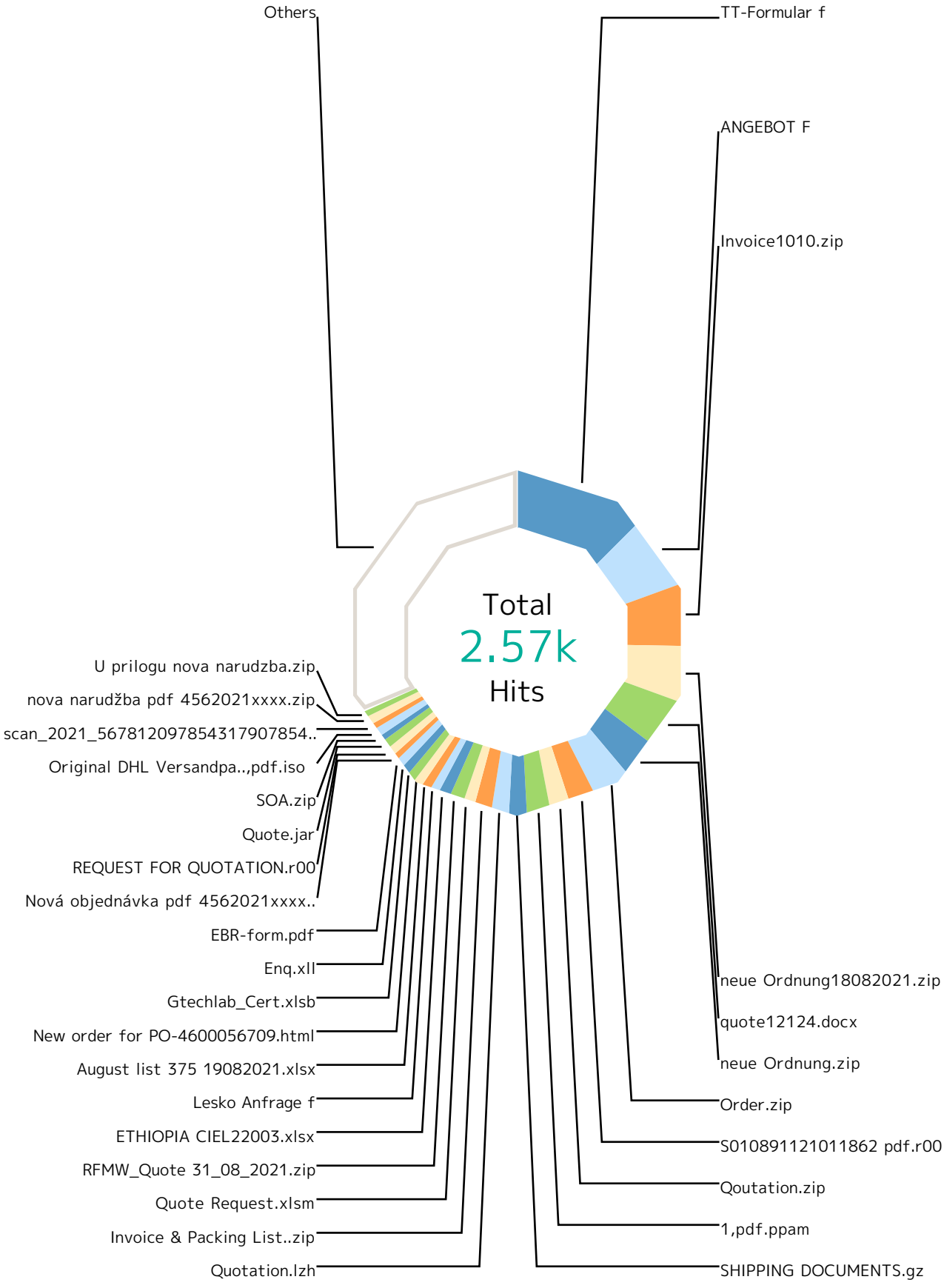
Report run time
01:33:43

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



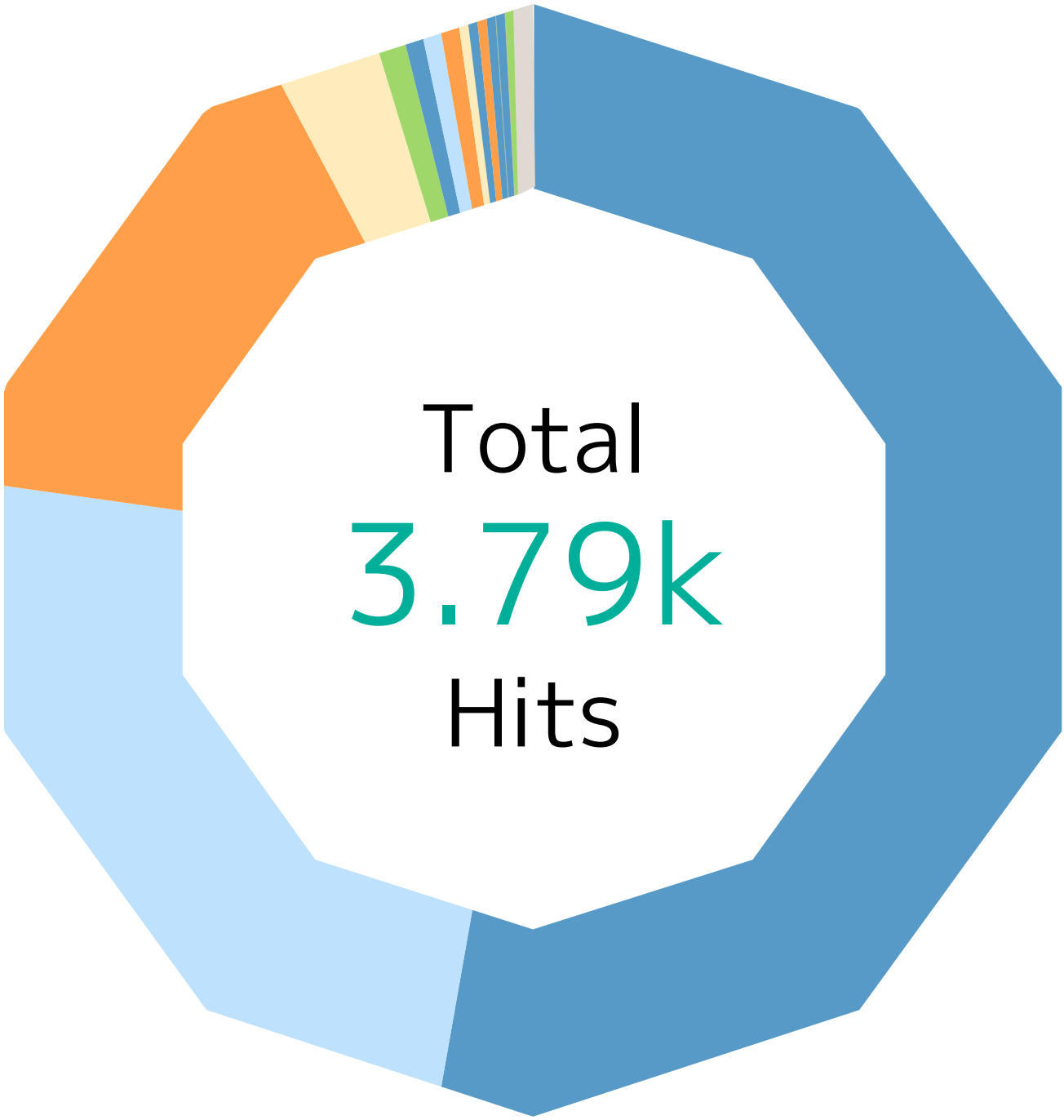
Report

Records by file name	Hits	%
TT-Formular f	321	12.5 %
ANGEBOT F	180	7.0 %
Invoice1010.zip	148	5.8 %
neue Ordnung18082021.zip	138	5.4 %
quote12124.docx	122	4.7 %
neue Ordnung.zip	93	3.6 %
Order.zip	92	3.6 %
S010891121011862 pdf.r00	61	2.4 %
Qoutation.zip	53	2.1 %
1,pdf.ppam	52	2.0 %
SHIPPING DOCUMENTS.gz	46	1.8 %
Quotation.lzh	44	1.7 %
Invoice & Packing List..zip	38	1.5 %
Quote Request.xlsm	35	1.4 %
RFMW_Quote 31_08_2021.zip	34	1.3 %
ETHIOPIA CIEL22003.xlsx	24	0.9 %
Lesko Anfrage f	24	0.9 %
August list 375 19082021.xlsx	23	0.9 %
New order for PO-4600056709.html	22	0.9 %
Gtechlab_Cert.xlsb	21	0.8 %
Enq.xll	20	0.8 %
EBR-form.pdf	20	0.8 %
Nová objednávka pdf 4562021xxxx.zip	19	0.7 %
REQUEST FOR QUOTATION.r00	19	0.7 %
Quote.jar	18	0.7 %
SOA.zip	18	0.7 %
Original DHL Versandpapiere 57635553_021,pdf.iso	18	0.7 %
scan_2021_567812097854317907854.rar	18	0.7 %
nova narudžba pdf 4562021xxxx.zip	18	0.7 %
U prilogu nova narudzba.zip	17	0.7 %
Others	813	31.6 %
Total	**2.57k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
3.79k
Hits

Report

Scan Result	Hits	%
Malicious	**2.00k**	**52.8 %**
File_Microsoft-Windows-Executable	879	23.2 %
File_ISO-9660-Disk-Image	367	9.7 %
File_Zip-Archive	259	6.8 %
File_Rar-Archive	248	6.5 %
File_Office-Open-XML-Package-Relations-Item	97	2.6 %
File_Microsoft-OLE	75	2.0 %
File_Type-Unknown	23	0.6 %
File_Microsoft-Excel-97-Spreadsheet	13	0.3 %
File_Microsoft-Excel-XLSX-Filename-Extension	11	0.3 %
File_Microsoft-Equation-Editor-Document	10	0.3 %
File_ACE-Archive	7	0.2 %
File_JavaScript	3	0.1 %
File_Java-Archive	3	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.1 %
File_LhArc-Archive	1	0.0 %
File_XML	1	0.0 %
File_Microsoft-Cabinet-Archive	1	0.0 %
Not Available	**922**	**24.3 %**
File_Zip-Archive	817	21.6 %
File_Microsoft-Office-Open-XML-Document	43	1.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	32	0.8 %
File_Java-Archive	15	0.4 %
File_Microsoft-Excel-XLSX-Filename-Extension	12	0.3 %
File_Microsoft-Excel-Spreadsheet	3	0.1 %
High Risk	**566**	**14.9 %**
File_LhArc-Archive	181	4.8 %
File_Rar-Archive	99	2.6 %
File_ISO-9660-Disk-Image	64	1.7 %
File_Microsoft-Windows-Executable	59	1.6 %
File_Zip-Archive	37	1.0 %
File_Type-Unknown	32	0.8 %
File_Office-Open-XML-Package-Relations-Item	25	0.7 %
File_Tar-Archive	24	0.6 %
File_7z-Archive	14	0.4 %
File_Generic-OLE-Package	12	0.3 %

Report

Scan Result	Hits	%
File_Microsoft-OLE	9	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
File_PDF	2	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.1 %
File_Microsoft-Equation-Editor-Document	2	0.1 %
Medium Risk	**125**	**3.3 %**
File_Generic-OLE-Package	23	0.6 %
File_JavaScript	22	0.6 %
File_PDF	19	0.5 %
File_Microsoft-Windows-Executable	16	0.4 %
File_Java-Class	15	0.4 %
File_PNG-Image	10	0.3 %
File_ISO-9660-Disk-Image	6	0.2 %
File_Rar-Archive	5	0.1 %
File_Type-Unknown	3	0.1 %
File_XML	3	0.1 %
File_Zip-Archive	2	0.1 %
File_Office-Open-XML-Application-Properties-Part	1	0.0 %
Exploit-GBT!599926F98361	**24**	**0.6 %**
File_Microsoft-Excel-XLSX-Filename-Extension	24	0.6 %
Exploit-GBT!6F2A99B836F3	**23**	**0.6 %**
File_Microsoft-Excel-XLSX-Filename-Extension	23	0.6 %
HTML/Phishing.ge	**21**	**0.6 %**
File_HTML	21	0.6 %
Unknown	**17**	**0.4 %**
File_Zip-Archive	16	0.4 %
File_Microsoft-Excel-XLSB-Filename-Extension	1	0.0 %
HTML/Phish-SiteFraud.ag	**12**	**0.3 %**
File_JavaScript	12	0.3 %
W97M/Downloader.djz	**8**	**0.2 %**
File_Microsoft-Excel-97-Spreadsheet	8	0.2 %
W32/Mydoom.t@MM!zip	**6**	**0.2 %**
File_Zip-Archive	6	0.2 %
AgentTesla-FCTJ!191CD9D202C1	**5**	**0.1 %**
File_Zip-Archive	5	0.1 %
Exploit-GBT!AD9F1173F687	**4**	**0.1 %**

Report

Scan Result	Hits	%
File_Microsoft-Excel-XLSX-Filename-Extension	4	0.1 %
W32/Mydoom.c.n@MM	**3**	**0.1 %**
File_Zip-Archive	2	0.1 %
File_Self-Extracting-Zip-Archive	1	0.0 %
GenericRXOY-KS!B7D638FC7027	**3**	**0.1 %**
File_Zip-Archive	3	0.1 %
AgentTesla-FCTJ!AE816C20AFF5	**3**	**0.1 %**
File_Type-Unknown	3	0.1 %
Dropper-FIY!3F55DBFE3CDB	**2**	**0.1 %**
File_ISO-9660-Disk-Image	2	0.1 %
Downloader-FCEV!DBEBFF454BEF	**2**	**0.1 %**
File_Microsoft-Excel-Spreadsheet	2	0.1 %
Trojan-FTMC!1A56CF92DCCF	**2**	**0.1 %**
File_Rar-Archive	2	0.1 %
Fareit-FCVN!1CD1FF507EDE	**2**	**0.1 %**
File_ISO-9660-Disk-Image	2	0.1 %
Fareit.gen.a	**2**	**0.1 %**
File_ACE-Archive	2	0.1 %
Downloader-FCEV!E6B26E288C1A	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCEV!21D08A88BA3C	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCEV!6CF8DE277ACD	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCEV!EA90B1CE7383	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCEV!05DAC619CA2A	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
PWS-FCXS!5261B690A9C6	**1**	**0.0 %**
File_Type-Unknown	1	0.0 %
Downloader-FCEV!5F839EFDB2D7	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCEV!9CD88D7A79E8	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %
Downloader-FCEV!D3A21FEB4953	**1**	**0.0 %**
File_Microsoft-Excel-Spreadsheet	1	0.0 %

Report

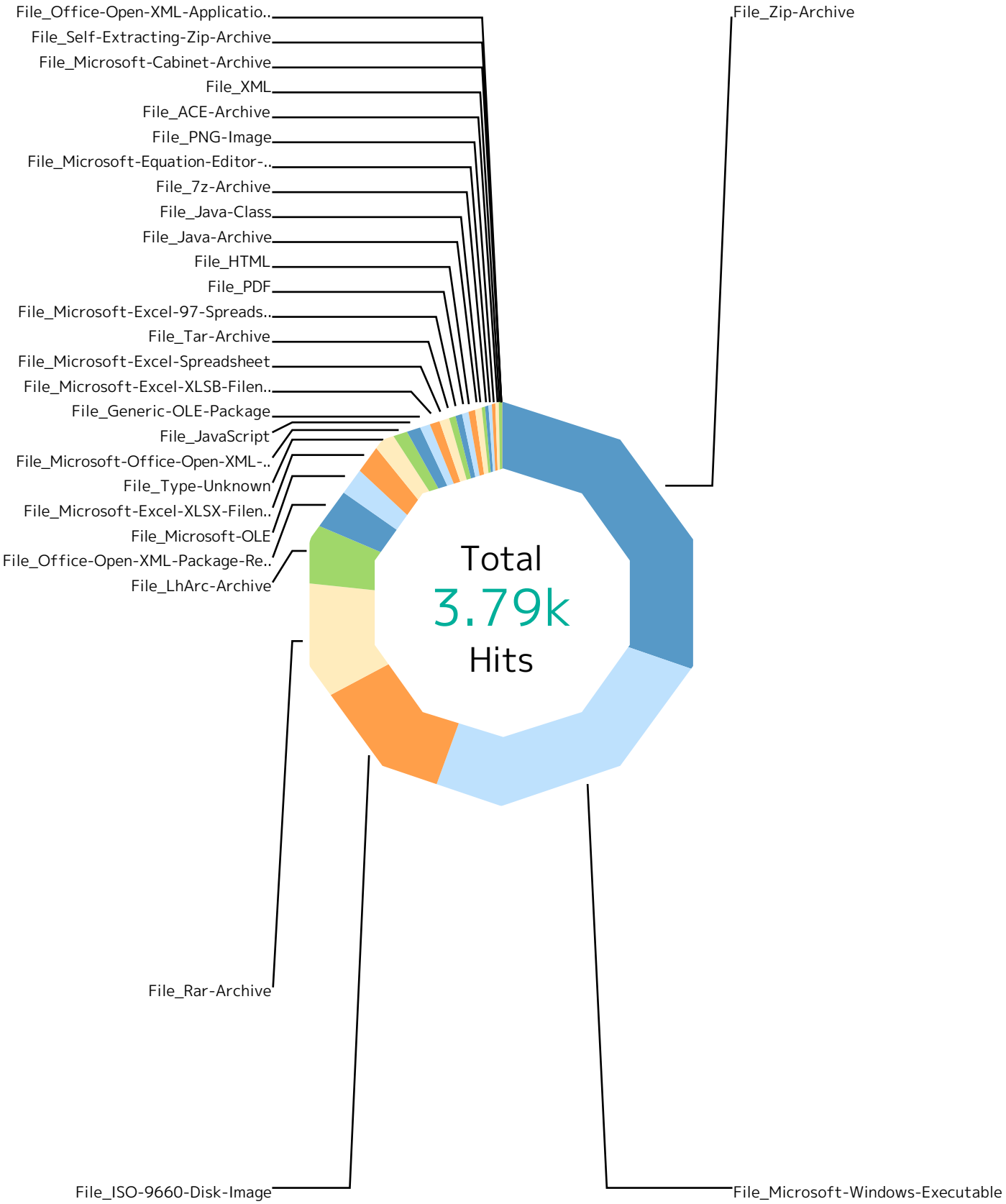
Scan Result	Hits	%
Others	26	0.7 %
Total	**3.79k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Office-Open-XML-Applicatio..
File_Self-Extracting-Zip-Archive
File_Microsoft-Cabinet-Archive
File_XML
File_ACE-Archive
File_PNG-Image
File_Microsoft-Equation-Editor-..
File_7z-Archive
File_Java-Class
File_Java-Archive
File_HTML
File_PDF
File_Microsoft-Excel-97-Spreads..
File_Tar-Archive
File_Microsoft-Excel-Spreadsheet
File_Microsoft-Excel-XLSB-Filen..
File_Generic-OLE-Package
File_JavaScript
File_Microsoft-Office-Open-XML-..
File_Type-Unknown
File_Microsoft-Excel-XLSX-Filen..
File_Microsoft-OLE
File_Office-Open-XML-Package-Re..
File_LhArc-Archive
File_Zip-Archive
Total
3.79k
Hits
File_Rar-Archive
File_ISO-9660-Disk-Image
File_Microsoft-Windows-Executable

Report

Responding Scanner	Hits	%
File_Zip-Archive	**1.15k**	**30.3 %**
Not Available	817	21.6 %
Malicious	259	6.8 %
High Risk	37	1.0 %
Unknown	16	0.4 %
W32/Mydoom.t@MM!zip	6	0.2 %
AgentTesla-FCTJ!191CD9D202C1	5	0.1 %
GenericRXOY-KS!B7D638FC7027	3	0.1 %
Medium Risk	2	0.1 %
W32/Mydoom.c.n@MM	2	0.1 %
Generic Malware.a!zip	1	0.0 %
File_Microsoft-Windows-Executable	**954**	**25.2 %**
Malicious	879	23.2 %
High Risk	59	1.6 %
Medium Risk	16	0.4 %
File_ISO-9660-Disk-Image	**446**	**11.8 %**
Malicious	367	9.7 %
High Risk	64	1.7 %
Medium Risk	6	0.2 %
Dropper-FIY!3F55DBFE3CDB	2	0.1 %
Fareit-FCVN!1CD1FF507EDE	2	0.1 %
Fareit-FCVN!83C6782F13EA	1	0.0 %
GenericRXKB-XS!D8EC77D36B62	1	0.0 %
Fareit-FDBI!39C6FE67D2AE	1	0.0 %
DistTrack!F8466F282D70	1	0.0 %
Fareit-FCVN!AFA5FC0CC169	1	0.0 %
File_Rar-Archive	**354**	**9.3 %**
Malicious	248	6.5 %
High Risk	99	2.6 %
Medium Risk	5	0.1 %
Trojan-FTMC!1A56CF92DCCF	2	0.1 %
File_LhArc-Archive	**183**	**4.8 %**
High Risk	181	4.8 %
Malicious	1	0.0 %
GenericRXLS-VV!FD5BEEE3F5BC	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**122**	**3.2 %**

Report

Responding Scanner	Hits	%
Malicious	97	2.6 %
High Risk	25	0.7 %
File_Microsoft-OLE	**84**	**2.2 %**
Malicious	75	2.0 %
High Risk	9	0.2 %
File_Microsoft-Excel-XLSX-Filename-Extension	**83**	**2.2 %**
Exploit-GBT!599926F98361	24	0.6 %
Exploit-GBT!6F2A99B836F3	23	0.6 %
Not Available	12	0.3 %
Malicious	11	0.3 %
High Risk	4	0.1 %
Exploit-GBT!AD9F1173F687	4	0.1 %
Exploit-FYV!B486866CA27C	1	0.0 %
Exploit-GBT!FFC358B4252F	1	0.0 %
Exploit-GBT!513C60017D4B	1	0.0 %
Exploit-GBT!2E47A80BF01B	1	0.0 %
Exploit-GBT!752F9D854C5C	1	0.0 %
File_Type-Unknown	**65**	**1.7 %**
High Risk	32	0.8 %
Malicious	23	0.6 %
Medium Risk	3	0.1 %
AgentTesla-FCTJ!AE816C20AFF5	3	0.1 %
PWS-FCXS!5261B690A9C6	1	0.0 %
GenericRXOY-KS!48D3FB98743A	1	0.0 %
AgentTesla-FDBQ!42DC7DED1F29	1	0.0 %
AgentTesla-FDAW!6AE942AA130A	1	0.0 %
File_Microsoft-Office-Open-XML-Document	**43**	**1.1 %**
Not Available	43	1.1 %
File_JavaScript	**37**	**1.0 %**
Medium Risk	22	0.6 %
HTML/Phish-SiteFraud.ag	12	0.3 %
Malicious	3	0.1 %
File_Generic-OLE-Package	**35**	**0.9 %**
Medium Risk	23	0.6 %
High Risk	12	0.3 %
File_Microsoft-Excel-XLSB-Filename-Extension	**33**	**0.9 %**

Report

Responding Scanner	Hits	%
Not Available	32	0.8 %
Unknown	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**27**	**0.7 %**
Not Available	3	0.1 %
Malicious	2	0.1 %
High Risk	2	0.1 %
Downloader-FCEV!DBEBFF454BEF	2	0.1 %
Downloader-FCEV!21D08A88BA3C	1	0.0 %
Downloader-FCEV!E6B26E288C1A	1	0.0 %
Downloader-FCEV!6CF8DE277ACD	1	0.0 %
Downloader-FCEV!EA90B1CE7383	1	0.0 %
Downloader-FCEV!05DAC619CA2A	1	0.0 %
Downloader-FCEV!5F839EFDB2D7	1	0.0 %
Downloader-FCEV!9CD88D7A79E8	1	0.0 %
Downloader-FCEV!D3A21FEB4953	1	0.0 %
Downloader-FCEV!C94DD15011AC	1	0.0 %
Downloader-FCEV!B09EEBC45CF9	1	0.0 %
Downloader-FCEV!6799222378F1	1	0.0 %
Downloader-FCEV!743DB171FF1D	1	0.0 %
Downloader-FCEV!542816EF4AD1	1	0.0 %
Downloader-FCEV!3D431FEE5CCF	1	0.0 %
Downloader-FCEV!1E63069DFD07	1	0.0 %
Downloader-FCEV!0CF6170099A5	1	0.0 %
Downloader-FCEV!E871D3A64C81	1	0.0 %
Downloader-FCEV!3D410E43F5F1	1	0.0 %
File_Tar-Archive	**24**	**0.6 %**
High Risk	24	0.6 %
File_Microsoft-Excel-97-Spreadsheet	**21**	**0.6 %**
Malicious	13	0.3 %
W97M/Downloader.djz	8	0.2 %
File_PDF	**21**	**0.6 %**
Medium Risk	19	0.5 %
High Risk	2	0.1 %
File_HTML	**21**	**0.6 %**
HTML/Phishing.ge	21	0.6 %
File_Java-Archive	**18**	**0.5 %**

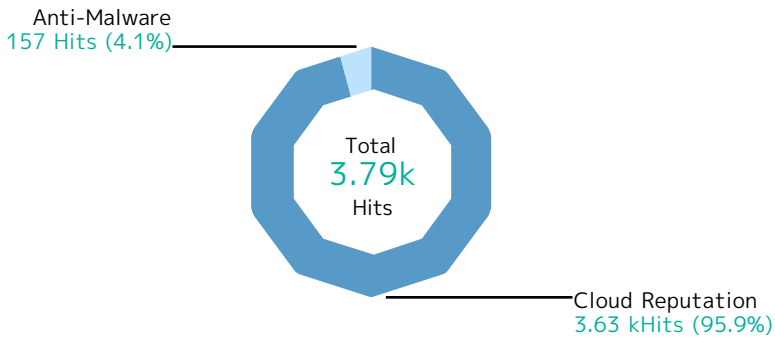
Report

Responding Scanner	Hits	%
Not Available	15	0.4 %
Malicious	3	0.1 %
File_Java-Class	**15**	**0.4 %**
Medium Risk	15	0.4 %
File_7z-Archive	**14**	**0.4 %**
High Risk	14	0.4 %
File_Microsoft-Equation-Editor-Document	**12**	**0.3 %**
Malicious	10	0.3 %
High Risk	2	0.1 %
File_PNG-Image	**10**	**0.3 %**
Medium Risk	10	0.3 %
File_ACE-Archive	**10**	**0.3 %**
Malicious	7	0.2 %
Fareit.gen.a	2	0.1 %
Fareit.gen.e	1	0.0 %
File_XML	**4**	**0.1 %**
Medium Risk	3	0.1 %
Malicious	1	0.0 %
File_Microsoft-Cabinet-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
File_Self-Extracting-Zip-Archive	**1**	**0.0 %**
W32/Mydoom.c.n@MM	1	0.0 %
File_Office-Open-XML-Application-Properties-Part	**1**	**0.0 %**
Medium Risk	1	0.0 %
Total	**3.79k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

Responding Scanner	Hits	%
Cloud Reputation	**3.63k**	**95.9 %**
File_Zip-Archive	1.13k	29.9 %
File_Microsoft-Windows-Executable	954	25.2 %
File_ISO-9660-Disk-Image	437	11.5 %
File_Rar-Archive	352	9.3 %
File_LhArc-Archive	182	4.8 %
File_Office-Open-XML-Package-Relations-Item	122	3.2 %
File_Microsoft-OLE	84	2.2 %
File_Type-Unknown	58	1.5 %
File_Microsoft-Office-Open-XML-Document	43	1.1 %
File_Generic-OLE-Package	35	0.9 %
File_Microsoft-Excel-XLSB-Filename-Extension	33	0.9 %
File_Microsoft-Excel-XLSX-Filename-Extension	27	0.7 %
File_JavaScript	25	0.7 %
File_Tar-Archive	24	0.6 %
File_PDF	21	0.6 %
File_Java-Archive	18	0.5 %
File_Java-Class	15	0.4 %
File_7z-Archive	14	0.4 %
File_Microsoft-Excel-97-Spreadsheet	13	0.3 %
File_Microsoft-Equation-Editor-Document	12	0.3 %
File_PNG-Image	10	0.3 %
File_Microsoft-Excel-Spreadsheet	7	0.2 %
File_ACE-Archive	7	0.2 %
File_XML	4	0.1 %
File_Microsoft-Cabinet-Archive	1	0.0 %
File_Office-Open-XML-Application-Properties-Part	1	0.0 %
Anti-Malware	**157**	**4.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	56	1.5 %
File_HTML	21	0.6 %
File_Microsoft-Excel-Spreadsheet	20	0.5 %
File_Zip-Archive	17	0.4 %
File_JavaScript	12	0.3 %
File_ISO-9660-Disk-Image	9	0.2 %
File_Microsoft-Excel-97-Spreadsheet	8	0.2 %
File_Type-Unknown	7	0.2 %

Report

Responding Scanner	Hits	%
File_ACE-Archive	3	0.1 %
File_Rar-Archive	2	0.1 %
File_LhArc-Archive	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
Total	**3.79k**	**100 %**

Report

Virenfilterung SRC IPs

Located 80.7 %

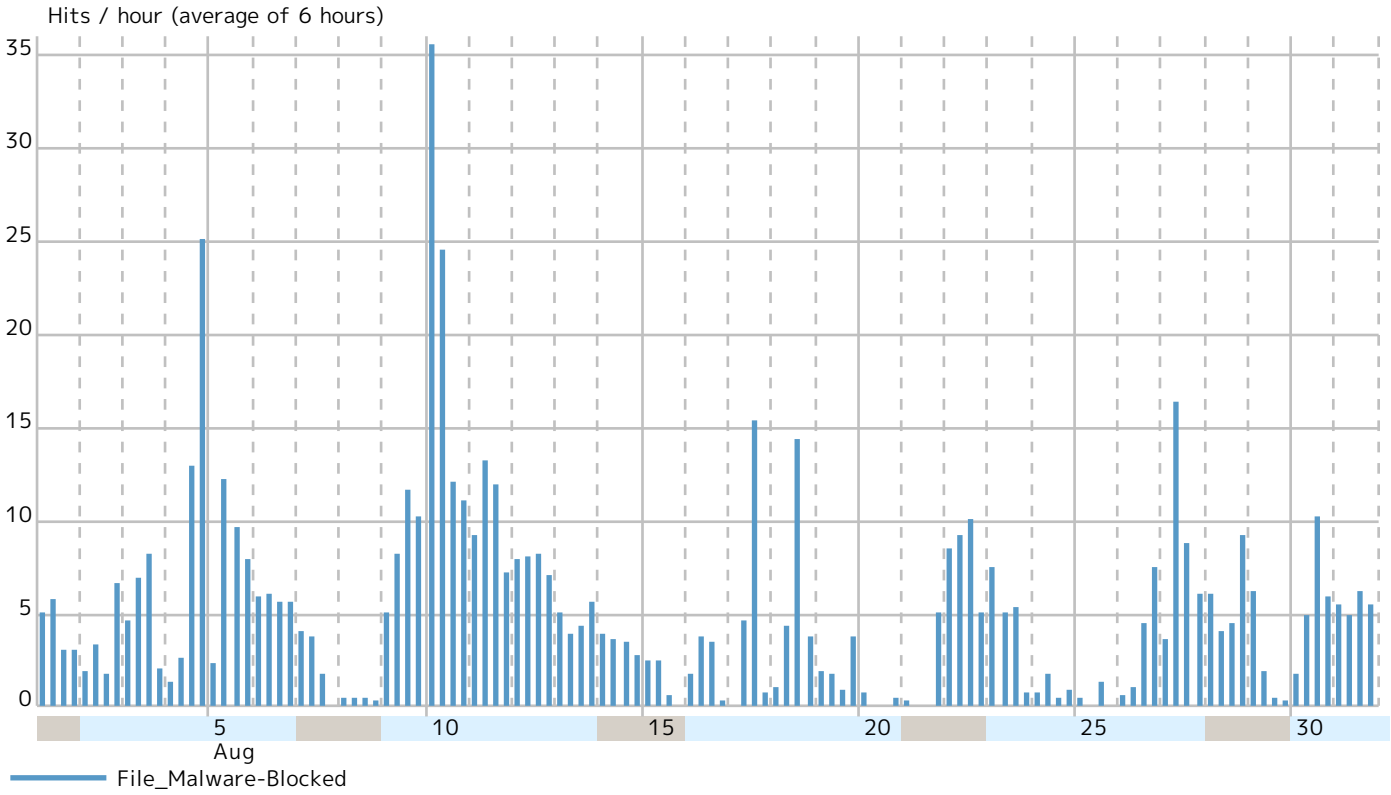
Report

Records by src IP		Hits	%
62.183.109.36	Astrakhan, Russia	707	18.7 %
203.96.177.206	Sydney, Australia	321	8.5 %
194.16.92.203	Sweden	296	7.8 %
211.115.111.12	South Korea	244	6.4 %
103.18.28.202	Indonesia	184	4.9 %
161.35.237.227	Santa Clara, California 95054, United States	180	4.8 %
185.33.234.169	Turkey	122	3.2 %
180.250.242.185	Kediri, Indonesia	104	2.7 %
117.53.155.171	Malaysia	79	2.1 %
46.183.223.59	Moscow, Russia	76	2.0 %
46.183.221.107	Moscow, Russia	72	1.9 %
103.82.21.142	Vietnam	70	1.8 %
93.91.112.112	Tver, Russia	64	1.7 %
139.59.34.136	Bengaluru, India	62	1.6 %
103.133.108.231	Bac Ninh, Vietnam	61	1.6 %
46.183.223.63	Moscow, Russia	47	1.2 %
195.130.35.141	Sarajevo, Bosnia and Herzegovina	38	1.0 %
103.167.84.45	Vietnam	34	0.9 %
45.137.22.114	Bangladesh	30	0.8 %
161.35.196.30	Frankfurt am Main, Germany	30	0.8 %
176.119.30.55	Ukraine	28	0.7 %
91.247.145.78	Germany	28	0.7 %
172.107.237.55	Amsterdam, Netherlands	25	0.7 %
157.245.109.27	Bengaluru, India	24	0.6 %
45.137.22.132	Bangladesh	24	0.6 %
64.44.168.121	Jacksonville, Florida 32255, United States	22	0.6 %
165.227.84.15	North Bergen, New Jersey 07047, United States	22	0.6 %
69.61.36.237	United States	21	0.6 %
104.168.215.144	United States	20	0.5 %
209.182.205.119	United States	20	0.5 %
Others		732	19.3 %
Total		**3.79k**	**100 %**

Report

SMTP Virus Filtering by Time

Top 10 file filtering situations on a timeline.



About NGFW

Forcepoint Next-Generation Firewall (NGFW) protects enterprise networks while giving organizations back time to focus on their business. With it, even thousands of firewalls can be deployed and centrally managed from a single pane of glass. Uniquely built for performance and high availability, Forcepoint firewalls are resilient at all levels – links, clusters and management – and can be updated without downtime. Forcepoint NGFW combines smart, easy-to-comprehend policies with the industry's leading defenses against Advanced Evasion Techniques to deliver superior networking and security.

For further information, product demonstrations, how-to guides & videos, best practices and 3rd party reports, visit forcepoint.com/NGFW

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint human point system delivers risk-adaptive protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.