Forcepoint

NGFW Security Management Center

E-Mail Virenfilterung Server Firewall

Report period

From: 2021-10-01 00:00:00
To: 2021-11-01 00:00:00

Report

Report run by
jens

SMC version
6.10.3, build 11135

Update version
1398

Report started
2021-11-02 07:48:09

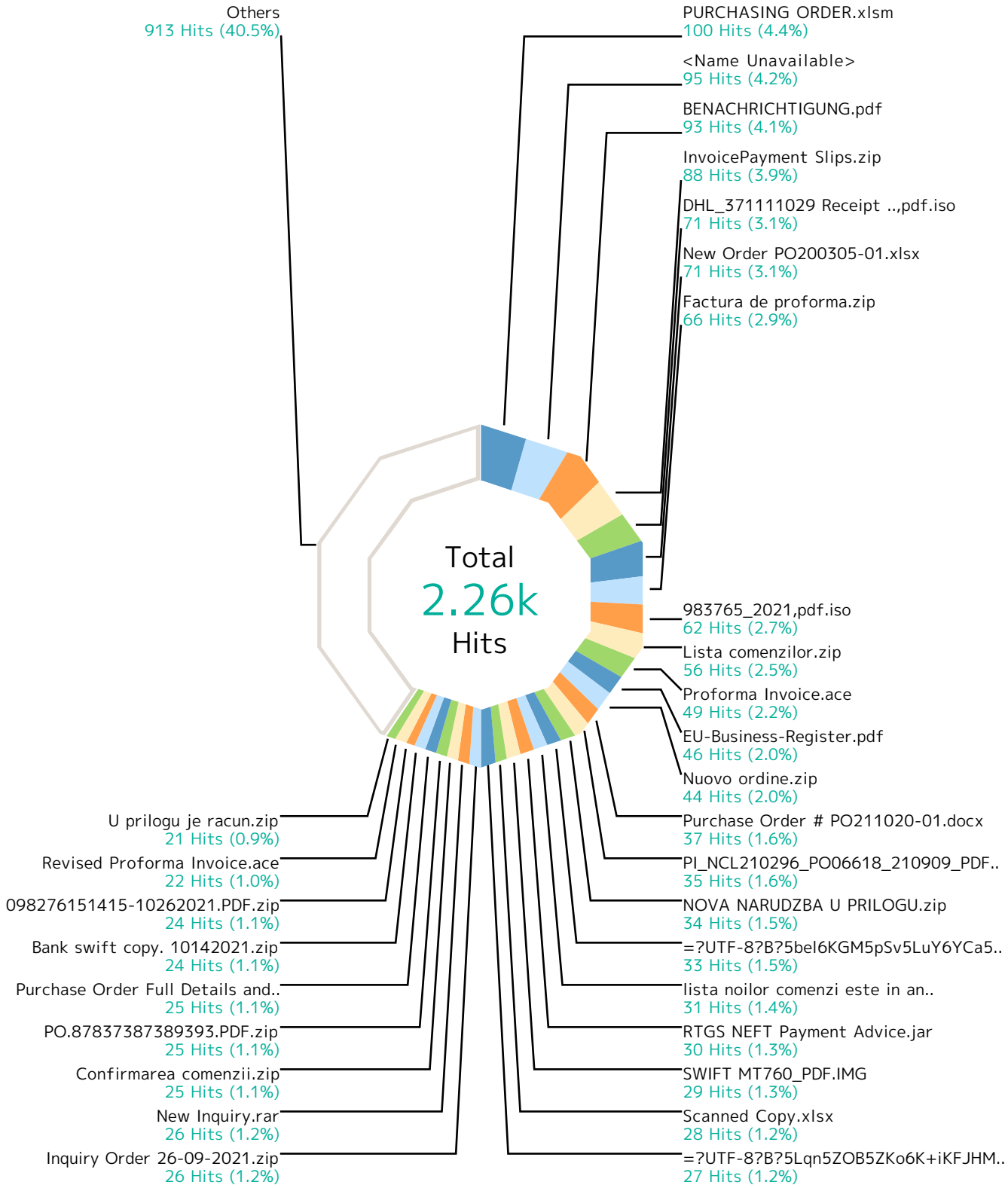
Report run time
01:21:26

Filters used
Match All

Table of Contents

Report

Virenfilterung MXe



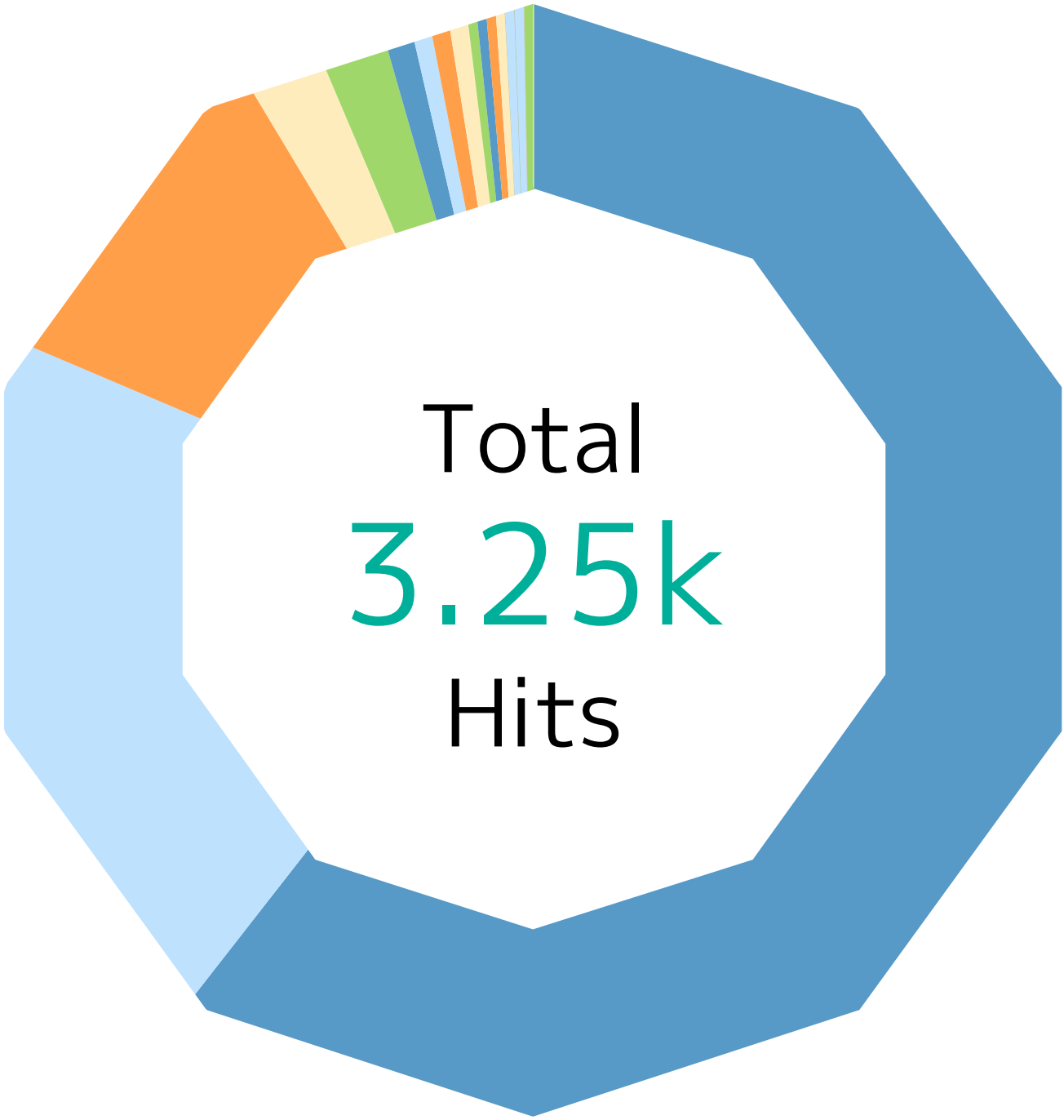
Report

Records by file name	Hits	%
PURCHASING ORDER.xlsm	100	4.4 %
<Name Unavailable>	95	4.2 %
BENACHRICHTIGUNG.pdf	93	4.1 %
InvoicePayment Slips.zip	88	3.9 %
DHL_371111029 Receipt Document,pdf.iso	71	3.1 %
New Order PO200305-01.xlsx	71	3.1 %
Factura de proforma.zip	66	2.9 %
983765_2021,pdf.iso	62	2.7 %
Lista comenzilor.zip	56	2.5 %
Proforma Invoice.ace	49	2.2 %
EU-Business-Register.pdf	46	2.0 %
Nuovo ordine.zip	44	2.0 %
Purchase Order # PO211020-01.docx	37	1.6 %
PI_NCL210296_PO06618_210909_PDF.IMG	35	1.6 %
NOVA NARUDZBA U PRILOGU.zip	34	1.5 %
=?UTF-8?B?5bel6KGM5pSv5LuY6YCa55+IIC0gSUNCQyBQYXItZW50IEFkdmIjZSAoUmVmIE1UMTAzODU3NDg0NzIpLmRvY3g=?=	33	1.5 %
lista noilor comenzi este in anexa.zip	31	1.4 %
RTGS NEFT Payment Advice.jar	30	1.3 %
SWIFT MT760_PDF.IMG	29	1.3 %
Scanned Copy.xlsx	28	1.2 %
=?UTF-8?B?5Lqn5ZOB5ZKo6K+iKFJHMjVMR1NKKS56aXA=?=	27	1.2 %
Inquiry Order 26-09-2021.zip	26	1.2 %
New Inquiry.rar	26	1.2 %
Confirmarea comenzii.zip	25	1.1 %
PO.87837387389393.PDF.zip	25	1.1 %
Purchase Order Full Details and Description PDF.ace	25	1.1 %
Bank swift copy. 10142021.zip	24	1.1 %
098276151415-10262021.PDF.zip	24	1.1 %
Revised Proforma Invoice.ace	22	1.0 %
U prilogu je racun.zip	21	0.9 %
Others	913	40.5 %
Total	**2.26k**	**100 %**

Report

Top File Types by Scan Result

Top 10 file types by scan result.


Total
3.25k
Hits

Report

Scan Result	Hits	%
Malicious	**1.97k**	**60.6 %**
File_Microsoft-Windows-Executable	747	23.0 %
File_ISO-9660-Disk-Image	228	7.0 %
File_Zip-Archive	221	6.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	146	4.5 %
File_Microsoft-OLE	114	3.5 %
File_Rar-Archive	103	3.2 %
File_ACE-Archive	98	3.0 %
File_Microsoft-Excel-97-Spreadsheet	89	2.7 %
File_Office-Open-XML-Package-Relations-Item	56	1.7 %
File_PDF	41	1.3 %
File_Java-Archive	38	1.2 %
File_Microsoft-Equation-Editor-Document	23	0.7 %
File_Type-Unknown	21	0.6 %
File_Microsoft-Cabinet-Archive	21	0.6 %
File_RTF	7	0.2 %
File_Microsoft-Office-Open-XML-Document	6	0.2 %
File_7z-Archive	3	0.1 %
File_Microsoft-Excel-Spreadsheet	2	0.1 %
File_LhArc-Archive	1	0.0 %
File_Microsoft-Excel-XLSB-Filename-Extension	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
Not Available	**677**	**20.8 %**
File_Zip-Archive	487	15.0 %
File_Microsoft-Excel-Spreadsheet	110	3.4 %
File_Microsoft-Office-Open-XML-Document	57	1.8 %
File_Microsoft-Excel-XLSX-Filename-Extension	23	0.7 %
High Risk	**328**	**10.1 %**
File_PDF	93	2.9 %
File_Rar-Archive	88	2.7 %
File_Zip-Archive	36	1.1 %
File_ISO-9660-Disk-Image	34	1.0 %
File_Microsoft-Windows-Executable	30	0.9 %
File_Office-Open-XML-Package-Relations-Item	17	0.5 %
File_LhArc-Archive	8	0.2 %
File_Microsoft-Excel-Spreadsheet	4	0.1 %

Report

Scan Result	Hits	%
File_Microsoft-Office-Open-XML-Document	4	0.1 %
File_7z-Archive	4	0.1 %
File_Type-Unknown	3	0.1 %
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
File_ACE-Archive	2	0.1 %
File_Microsoft-OLE	1	0.0 %
File_HTML	1	0.0 %
File_Tar-Archive	1	0.0 %
Medium Risk	**70**	**2.2 %**
File_Zip-Archive	12	0.4 %
File_Type-Unknown	12	0.4 %
File_PDF	11	0.3 %
File_HTML	10	0.3 %
File_Microsoft-Windows-Executable	8	0.2 %
File_Rar-Archive	5	0.2 %
File_Microsoft-Excel-97-Spreadsheet	5	0.2 %
File_Microsoft-Office-Open-XML-Document	5	0.2 %
File_ISO-9660-Disk-Image	1	0.0 %
File_Microsoft-OLE	1	0.0 %
Unknown	**58**	**1.8 %**
File_Zip-Archive	58	1.8 %
Fareit.gen.a	**30**	**0.9 %**
File_ACE-Archive	30	0.9 %
Exploit-CVE2017-11882.yx	**22**	**0.7 %**
File_Microsoft-Excel-XLSX-Filename-Extension	21	0.6 %
File_Microsoft-Office-Open-XML-Document	1	0.0 %
HTML/Phishing.ge	**19**	**0.6 %**
File_HTML	19	0.6 %
Fareit-FCVN!6A4F90CAB77A	**14**	**0.4 %**
File_ISO-9660-Disk-Image	14	0.4 %
Exploit-GBT!54EA30653905	**9**	**0.3 %**
File_Microsoft-Excel-XLSX-Filename-Extension	9	0.3 %
Fareit.gen.e	**8**	**0.2 %**
File_ACE-Archive	8	0.2 %
Exploit-GDJ!A1FCD26F412F	**5**	**0.2 %**
File_Microsoft-Excel-XLSX-Filename-Extension	5	0.2 %

Report

Scan Result	Hits	%
HTML/Phishing.iy	**5**	**0.2 %**
File_HTML	5	0.2 %
Suspect-BW!EFE074C271F0	**5**	**0.2 %**
File_Zip-Archive	5	0.2 %
AgentTesla-FDAK!88EB10863F66	**4**	**0.1 %**
File_Rar-Archive	4	0.1 %
HTML/Phishing.is	**3**	**0.1 %**
File_HTML	3	0.1 %
GenericRXPZ-RR!C67962F854AE	**2**	**0.1 %**
File_Zip-Archive	2	0.1 %
PWS-FCZF!D03CC6BB0B84	**2**	**0.1 %**
File_Rar-Archive	2	0.1 %
GuLoader-FDDN!12DCE249E7EC	**2**	**0.1 %**
File_Zip-Archive	2	0.1 %
Exploit-GBT!5D4AEC4ED6DB	**2**	**0.1 %**
File_Microsoft-Excel-XLSX-Filename-Extension	2	0.1 %
X97M/Downloader.ky	**2**	**0.1 %**
File_Microsoft-Excel-XLSB-Filename-Extension	2	0.1 %
HTML/Phishing.hh	**2**	**0.1 %**
File_HTML	2	0.1 %
VBS/Psyme.a	**1**	**0.0 %**
File_Tar-Archive	1	0.0 %
GuLoader-FDDN!3DBF52BEF094	**1**	**0.0 %**
File_Type-Unknown	1	0.0 %
PWS-FCZF!22872F4D32C9	**1**	**0.0 %**
File_Zip-Archive	1	0.0 %
AgentTesla-FDAR!B7CD3C89BF36	**1**	**0.0 %**
File_ISO-9660-Disk-Image	1	0.0 %
Exploit-GDR!9ABCA342D134	**1**	**0.0 %**
File_Microsoft-Office-Open-XML-Document	1	0.0 %
GuLoader-FDDL!AE7621BD98AE	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %
Exploit-GBT!80DF6C3CA720	**1**	**0.0 %**
File_Microsoft-Excel-XLSX-Filename-Extension	1	0.0 %
PWS-FCZF!95FCDE9E18CF	**1**	**0.0 %**
File_Rar-Archive	1	0.0 %

Report

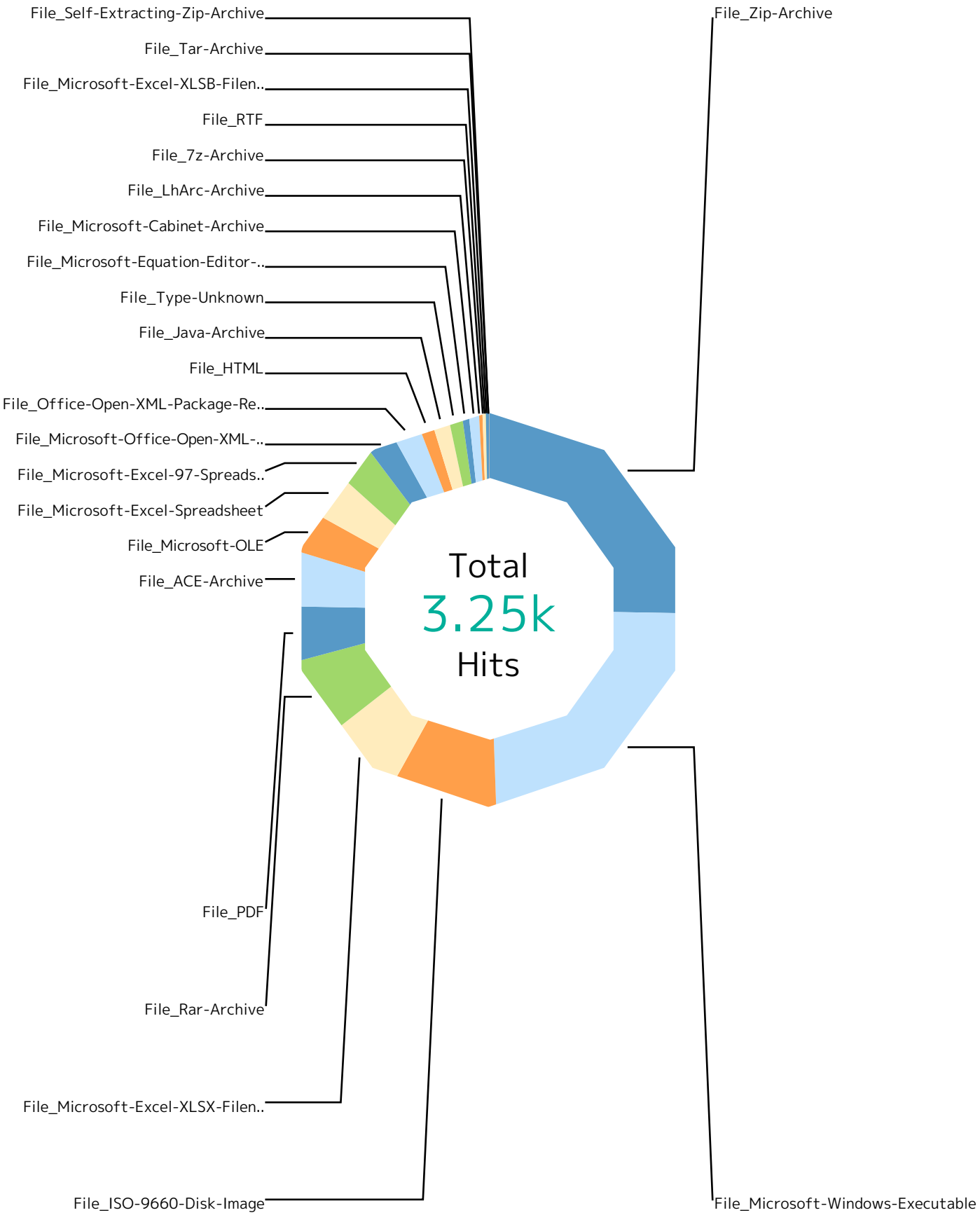
Scan Result	Hits	%
Others	4	0.1 %
Total	**3.25k**	**100 %**

Report

Top Scan Results by Responding Scanner

Top 10 file filtering scan results by responding scanner.

Report


File_Self-Extracting-Zip-Archive
File_Tar-Archive
File_Microsoft-Excel-XLSB-Filen..
File_RTF
File_7z-Archive
File_LhArc-Archive
File_Microsoft-Cabinet-Archive
File_Microsoft-Equation-Editor-..
File_Type-Unknown
File_Java-Archive
File_HTML
File_Office-Open-XML-Package-Re..
File_Microsoft-Office-Open-XML-..
File_Microsoft-Excel-97-Spreads..
File_Microsoft-Excel-Spreadsheet
File_Microsoft-OLE
File_ACE-Archive
File_PDF
File_Rar-Archive
File_Microsoft-Excel-XLSX-Filen..
File_ISO-9660-Disk-Image
File_Zip-Archive
File_Microsoft-Windows-Executable
Total
3.25k
Hits

Report

Responding Scanner	Hits	%
File_Zip-Archive	**824**	**25.4 %**
Not Available	487	15.0 %
Malicious	221	6.8 %
Unknown	58	1.8 %
High Risk	36	1.1 %
Medium Risk	12	0.4 %
Suspect-BW!EFE074C271F0	5	0.2 %
GenericRXPZ-RR!C67962F854AE	2	0.1 %
GuLoader-FDDN!12DCE249E7EC	2	0.1 %
PWS-FCZF!22872F4D32C9	1	0.0 %
File_Microsoft-Windows-Executable	**785**	**24.2 %**
Malicious	747	23.0 %
High Risk	30	0.9 %
Medium Risk	8	0.2 %
File_ISO-9660-Disk-Image	**278**	**8.6 %**
Malicious	228	7.0 %
High Risk	34	1.0 %
Fareit-FCVN!6A4F90CAB77A	14	0.4 %
Medium Risk	1	0.0 %
AgentTesla-FDAR!B7CD3C89BF36	1	0.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	**210**	**6.5 %**
Malicious	146	4.5 %
Not Available	23	0.7 %
Exploit-CVE2017-11882.yx	21	0.6 %
Exploit-GBT!54EA30653905	9	0.3 %
Exploit-GDJ!A1FCD26F412F	5	0.2 %
High Risk	2	0.1 %
Exploit-GBT!5D4AEC4ED6DB	2	0.1 %
Exploit-GBT!80DF6C3CA720	1	0.0 %
Exploit-GBT!68AD94204E88	1	0.0 %
File_Rar-Archive	**205**	**6.3 %**
Malicious	103	3.2 %
High Risk	88	2.7 %
Medium Risk	5	0.2 %
AgentTesla-FDAK!88EB10863F66	4	0.1 %
PWS-FCZF!D03CC6BB0B84	2	0.1 %

Report

Responding Scanner	Hits	%
GuLoader-FDDL!AE7621BD98AE	1	0.0 %
PWS-FCZF!95FCDE9E18CF	1	0.0 %
AgentTesla-FDAK!83AE9EB1E48D	1	0.0 %
File_PDF	**145**	**4.5 %**
High Risk	93	2.9 %
Malicious	41	1.3 %
Medium Risk	11	0.3 %
File_ACE-Archive	**138**	**4.2 %**
Malicious	98	3.0 %
Fareit.gen.a	30	0.9 %
Fareit.gen.e	8	0.2 %
High Risk	2	0.1 %
File_Microsoft-OLE	**116**	**3.6 %**
Malicious	114	3.5 %
High Risk	1	0.0 %
Medium Risk	1	0.0 %
File_Microsoft-Excel-Spreadsheet	**116**	**3.6 %**
Not Available	110	3.4 %
High Risk	4	0.1 %
Malicious	2	0.1 %
File_Microsoft-Excel-97-Spreadsheet	**94**	**2.9 %**
Malicious	89	2.7 %
Medium Risk	5	0.2 %
File_Microsoft-Office-Open-XML-Document	**74**	**2.3 %**
Not Available	57	1.8 %
Malicious	6	0.2 %
Medium Risk	5	0.2 %
High Risk	4	0.1 %
Exploit-CVE2017-11882.yx	1	0.0 %
Exploit-GDR!9ABCA342D134	1	0.0 %
File_Office-Open-XML-Package-Relations-Item	**73**	**2.2 %**
Malicious	56	1.7 %
High Risk	17	0.5 %
File_HTML	**41**	**1.3 %**
HTML/Phishing.ge	19	0.6 %
Medium Risk	10	0.3 %

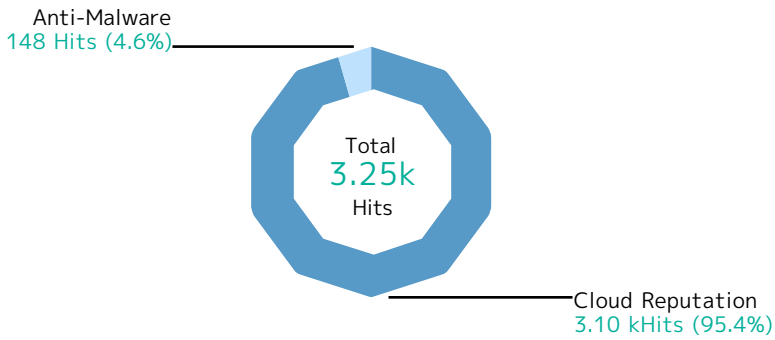
Report

Responding Scanner	Hits	%
HTML/Phishing.iy	5	0.2 %
HTML/Phishing.is	3	0.1 %
HTML/Phishing.hh	2	0.1 %
High Risk	1	0.0 %
HTML/Phishing.jt	1	0.0 %
File_Java-Archive	**38**	**1.2 %**
Malicious	38	1.2 %
File_Type-Unknown	**37**	**1.1 %**
Malicious	21	0.6 %
Medium Risk	12	0.4 %
High Risk	3	0.1 %
GuLoader-FDDN!3DBF52BEF094	1	0.0 %
File_Microsoft-Equation-Editor-Document	**23**	**0.7 %**
Malicious	23	0.7 %
File_Microsoft-Cabinet-Archive	**21**	**0.6 %**
Malicious	21	0.6 %
File_LhArc-Archive	**9**	**0.3 %**
High Risk	8	0.2 %
Malicious	1	0.0 %
File_7z-Archive	**8**	**0.2 %**
High Risk	4	0.1 %
Malicious	3	0.1 %
GenericRXQK-ZC!27A9E4F59F07	1	0.0 %
File_RTF	**7**	**0.2 %**
Malicious	7	0.2 %
File_Microsoft-Excel-XLSB-Filename-Extension	**3**	**0.1 %**
X97M/Downloader.ky	2	0.1 %
Malicious	1	0.0 %
File_Tar-Archive	**2**	**0.1 %**
High Risk	1	0.0 %
VBS/Psyme.a	1	0.0 %
File_Self-Extracting-Zip-Archive	**1**	**0.0 %**
Malicious	1	0.0 %
Total	**3.25k**	**100 %**

Report

Top File Types by Responding Scanner

Top 10 file types by responding scanner.



Report

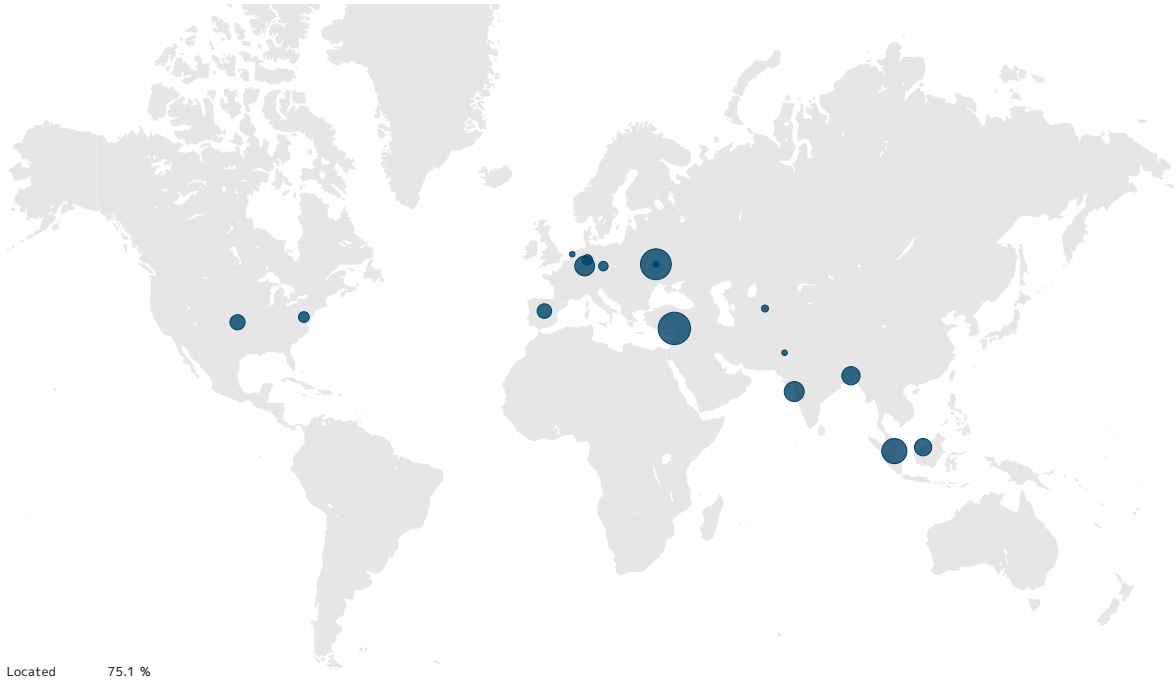
Responding Scanner	Hits	%
Cloud Reputation	**3.10k**	**95.4 %**
File_Zip-Archive	814	25.1 %
File_Microsoft-Windows-Executable	785	24.2 %
File_ISO-9660-Disk-Image	263	8.1 %
File_Rar-Archive	196	6.0 %
File_Microsoft-Excel-XLSX-Filename-Extension	171	5.3 %
File_PDF	145	4.5 %
File_Microsoft-OLE	116	3.6 %
File_Microsoft-Excel-Spreadsheet	116	3.6 %
File_ACE-Archive	100	3.1 %
File_Microsoft-Excel-97-Spreadsheet	94	2.9 %
File_Office-Open-XML-Package-Relations-Item	73	2.2 %
File_Microsoft-Office-Open-XML-Document	72	2.2 %
File_Java-Archive	38	1.2 %
File_Type-Unknown	36	1.1 %
File_Microsoft-Equation-Editor-Document	23	0.7 %
File_Microsoft-Cabinet-Archive	21	0.6 %
File_HTML	11	0.3 %
File_LhArc-Archive	9	0.3 %
File_7z-Archive	7	0.2 %
File_RTF	7	0.2 %
File_Microsoft-Excel-XLSB-Filename-Extension	1	0.0 %
File_Tar-Archive	1	0.0 %
File_Self-Extracting-Zip-Archive	1	0.0 %
Anti-Malware	**148**	**4.6 %**
File_Microsoft-Excel-XLSX-Filename-Extension	39	1.2 %
File_ACE-Archive	38	1.2 %
File_HTML	30	0.9 %
File_ISO-9660-Disk-Image	15	0.5 %
File_Zip-Archive	10	0.3 %
File_Rar-Archive	9	0.3 %
File_Microsoft-Office-Open-XML-Document	2	0.1 %
File_Microsoft-Excel-XLSB-Filename-Extension	2	0.1 %
File_Type-Unknown	1	0.0 %
File_7z-Archive	1	0.0 %
File_Tar-Archive	1	0.0 %

Report

Responding Scanner	Hits	%
Total	**3.25k**	**100 %**

Report

Virenfilterung SRC IPs



Located 75.1 %

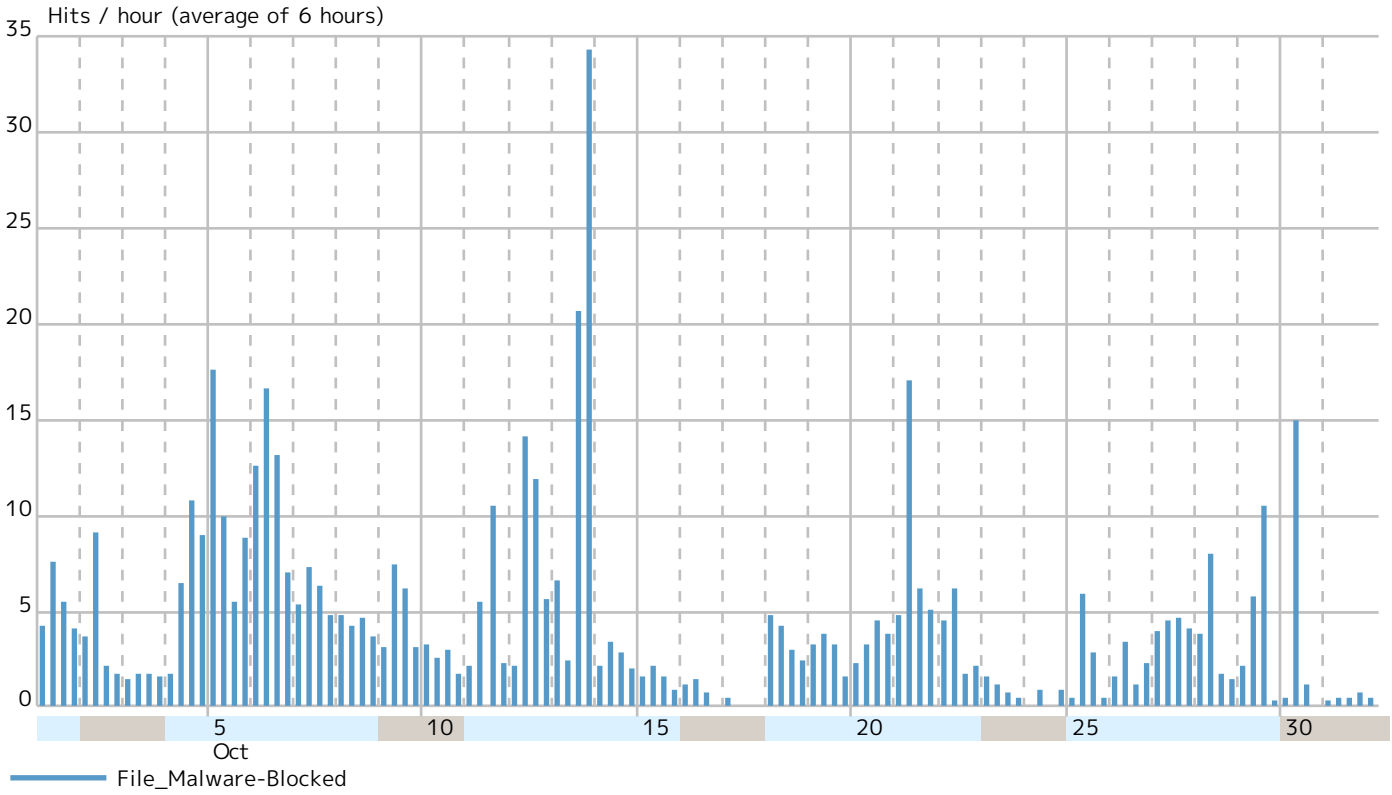
Report

Records by src IP		Hits	%
195.33.210.155	Antakya, Turkey	370	11.4 %
185.46.188.30	Ukraine	350	10.8 %
154.61.75.244	Thane, India	210	6.5 %
134.209.231.21	Frankfurt am Main, Germany	208	6.4 %
101.99.93.50	Malaysia	176	5.4 %
178.128.21.127	Singapore, 62 Singapore	93	2.9 %
45.137.20.129	Bangladesh	92	2.8 %
2.56.59.86	Dulles, Virginia 20103, United States	91	2.8 %
185.222.58.140	Bangladesh	74	2.3 %
86.109.161.43	Spain	74	2.3 %
174.138.22.211	Singapore, 62 Singapore	71	2.2 %
195.162.18.78	Spain	66	2.0 %
212.192.246.150	Germany	64	2.0 %
159.223.72.103	Singapore, 62 Singapore	62	1.9 %
185.74.4.8	Uzbekistan	42	1.3 %
209.59.144.144	United States	37	1.1 %
167.89.100.127	United States	37	1.1 %
91.211.88.206	Kyiv, Ukraine	30	0.9 %
212.193.30.111	Czechia	30	0.9 %
50.31.60.209	United States	27	0.8 %
216.250.251.115	United States	26	0.8 %
104.248.158.86	Singapore, 62 Singapore	26	0.8 %
178.128.17.111	Singapore, 62 Singapore	25	0.8 %
212.193.30.192	Czechia	25	0.8 %
124.29.202.102	Pakistan	24	0.7 %
5.9.49.240	Germany	24	0.7 %
185.222.57.88	Amsterdam, Netherlands	22	0.7 %
45.137.22.143	Bangladesh	22	0.7 %
142.11.211.244	United States	21	0.6 %
212.193.30.127	Czechia	20	0.6 %
Others		809	24.9 %
Total		**3.25k**	**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.