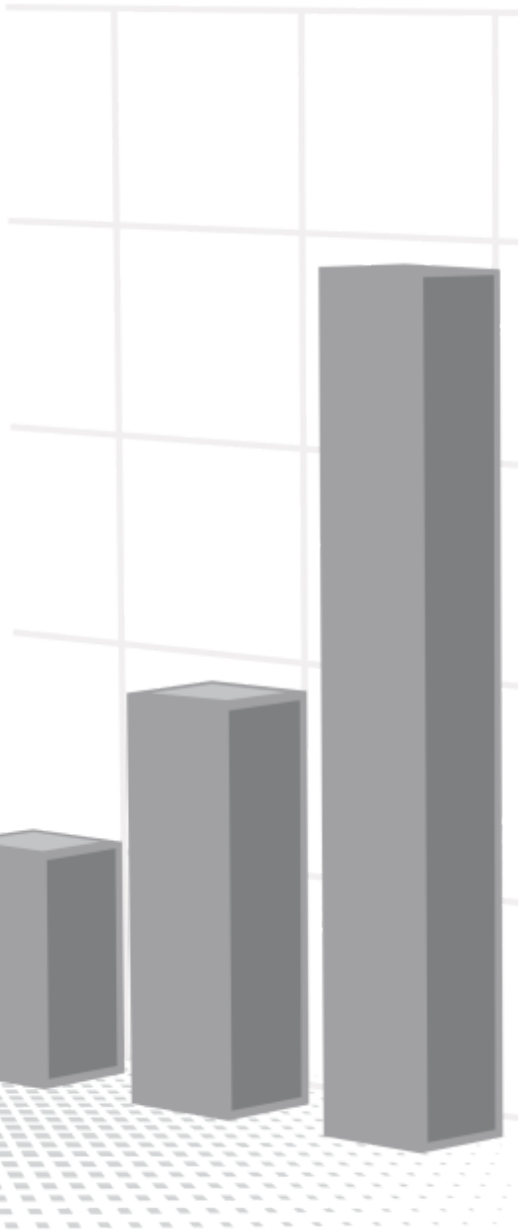
Unified Security Report

Monatlich

Juni 2023

Gesamtstatus

Alles Okay



Ihr Ansprechpartner

Securepoint GmbH IT

Bleckeder Landstr. 28
21337 Lüneburg

E-Mail: info@securepoint.de

Wenn Sie Fragen zu diesem Bericht haben, können Sie sich gerne an unsere Hotline wenden.

Inhaltsverzeichnis

Securepoint NextGen UTM-Firewall

Status
Alles Okay

UTMs	Auslaufende Lizenzen	Viren
1	Alle Lizenzen sind länger als 4 Wochen gültig	118 Viren abgewehrt

Alerts	UTMs mit Risiko	Logins fehl.
Keine Alerts gefunden	Alle UTMs sind ohne Risiko	Keine Logins gefunden

Securepoint Mobile Security

Status
Alles Okay

Devices	VPNs	Traffic total	Viren
4	3	8 Gigabytes	14 Viren abgewehrt

Profile	Lizenz	Blocked URLs	BYOD
2	8 Monate verbleibend	4	1

Securepoint Antivirus Pro

Status
Alles Okay

Devices	Devices muted	Lizenz	Devices frei
15 In Benutzung	8 Devices sind muted	6 Monate verbleibend	Kein Device mehr frei

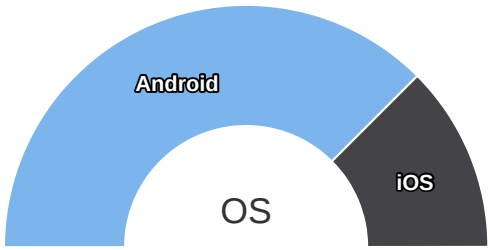
Viren	Viren entfernt	PUA	PUA entfernt
3 Viren gefunden	Alle Viren entfernt	3 PUA gefunden	Alle Viren entfernt

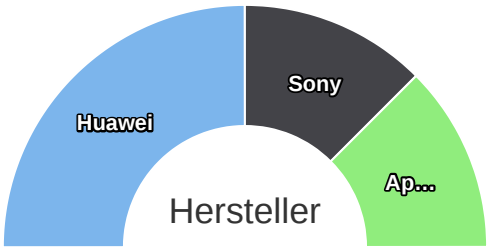
Lizenz	Devices frei	Viren	Privacy
8 Monate verbleibend	7 von 14 Devices frei	14 Viren abgewehrt	Privatsphäre ist geschützt

Blocked URLs	Traffic HTTP	Devices	VPN
4 URLs wurden geblockt	8 Gigabytes	4	3

Device Management

Profile	Apps	Benutzer	Rollen	Zertifikate
2	8	7	3	1





Garantie

Alle Devices haben Garantie

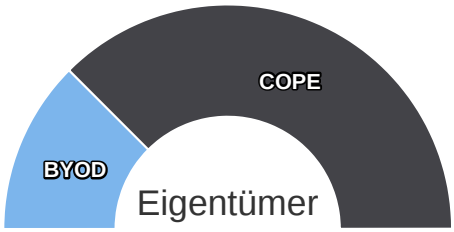
Verträge

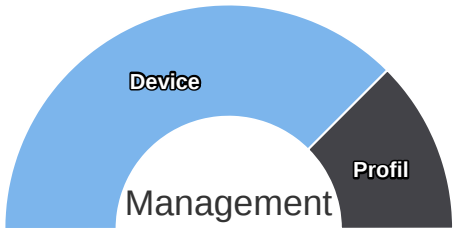
Alle Verträge sind gültig

Anbieter

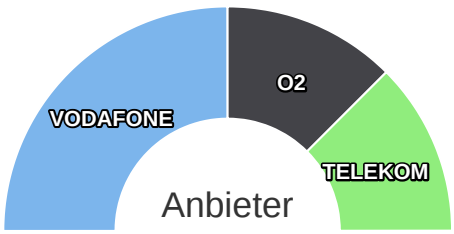
3

Eigentümer





Verteilungen



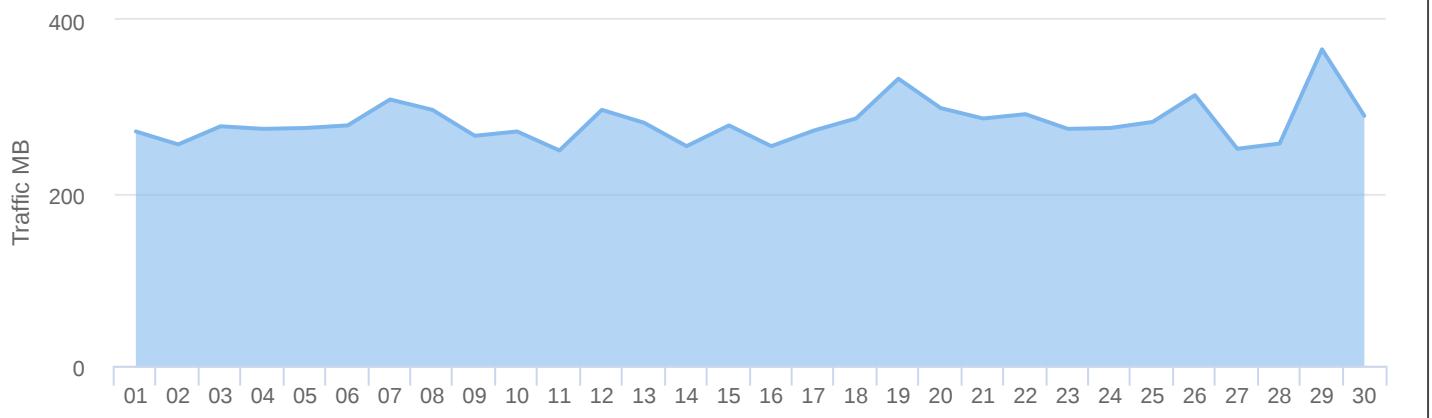
Top Anbieter

Name	Anzahl
VODAFONE	2
O2	1
TELEKOM	1

Top Tarife

Name	Anzahl
RED XS	1
FREE S	1
RED L	1
MAGENTA M	1

Traffic



Top Devices

#	Name	Traffic
1	Anonymisiertes Device	1.22 GB
2	Anonymisiertes Device	1.2 GB
3	Anonymisiertes Device	1.2 GB
4	Anonymisiertes Device	1.2 GB
5	Anonymisiertes Device	1.16 GB

Top abgewehrte Viren

#	Virus	Anzahl
1	Backdoor.Win32.Kirts	3
2	AdWare.MultiPlug	2
3	Trojan-Ransom.Locky	2
4	Trojan.Win32.Crypt	2
5	Trojan.Win32.Injector	2

Top Kategorien

#	Kategorie	Traffic
1	Humor	977 MB
2	Haus und Garten	964 MB
3	Reisen	957 MB
4	Soziale Netzwerke	951 MB
5	News	943 MB
6	Shopping	934 MB
7	Auktionen	929 MB
8	Kinder	902 MB
9	Computer	894 MB

Top geblockte Kategorien

#	Kategorie	Anzahl
1	Werbe Dienste	2
2	Threat Intelligence Feed	1
3	Tracking strict	1

Top Domains

#	Domain/IP	Traffic
1	securepoint.de	894 MB
2	lachschon.de	117 MB
3	spin.de	111 MB
4	ebay-kleinanzeigen.de	110 MB
5	odnoklassniki.ru	109 MB
6	thermomix.com	109 MB
7	handelsblatt.com	108 MB
8	hotels.com	108 MB
9	tchibo.de	107 MB
10	die-kinderwelt.com	106 MB
11	maedchenflohmarkt.de	105 MB
12	hagebau.de	105 MB
13	martin-perscheid.de	104 MB
14	br-online.de	104 MB
15	saturn.de	103 MB
16	ebay.com	103 MB
17	booking.com	103 MB
18	1jux.net	103 MB
19	knuddels.de	102 MB
20	conrad.de	102 MB
21	car24.bg	101 MB

Top geblockte Domains

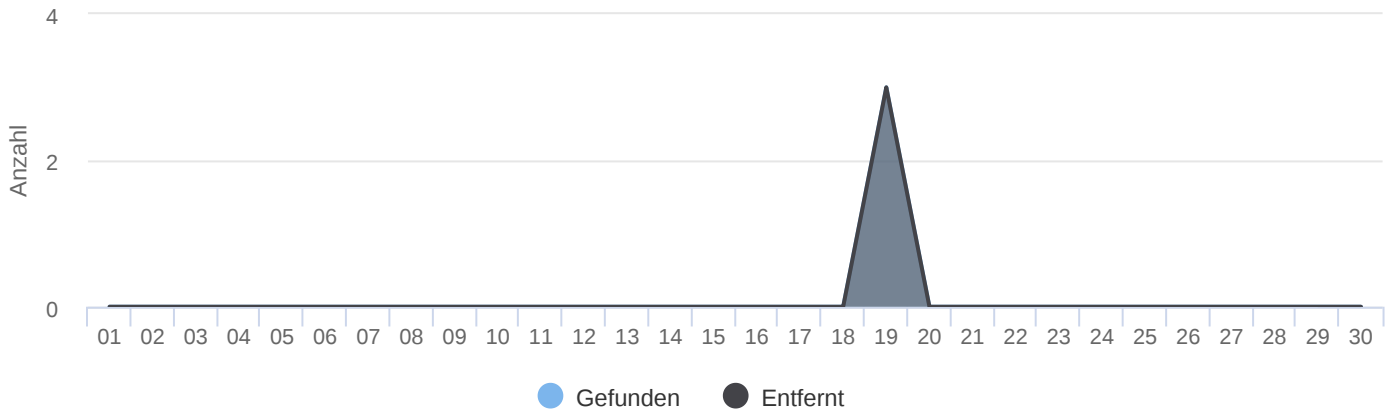
#	Domain/IP	Anzahl
1	ad4mat.net	1
2	doubleclick.net	1
3	siteimproveanalytics.io	1
4	smartpcupdate.com	1

Antivirus Security Übersicht

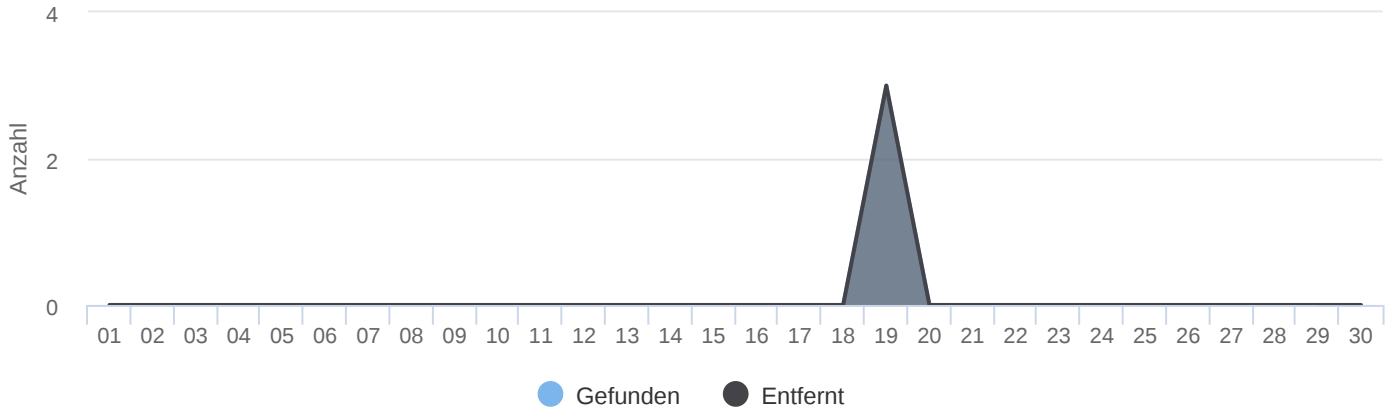
Devices	Devices muted	Lizenz	Devices frei
15			
In Benutzung	8 Devices sind muted	6 Monate verbleibend	Kein Device mehr frei

Viren	Viren entfernt	PUA	PUA entfernt
3 Viren gefunden	Alle Viren entfernt	3 PUA gefunden	Alle Viren entfernt

Virusaktionen



PUA-Aktionen



Top Viren Devices

Name	Infektionen
Anonymisiertes Device	1
Anonymisiertes Device	1
Anonymisiertes Device	1

Top PUA Devices

Name	Infektionen
Anonymisiertes Device	1
Anonymisiertes Device	1
Anonymisiertes Device	1

Top Viren

Name	Infektionen
Trojan.Win32.Filecoder	2
Trojan.Win32.Injector	1

Top PUA

Name	Infektionen
PUA.Amonetize	1
PUA.DownloadSponsor	1
PUA.Somoto	1

UTM Übersicht - Gateway 001

Securepoint RC200

CPU: CPU G620 @2594

Speicher: 3 GB

Appliance läuft seit: 264 Tage, 8 Stunden

Lizenz: Securepoint GmbH
Entwicklung, 20 Benutzer

Lizenz

1 Jahre verbleibend

UTM-Version

11.8.7 ist aktuell

Festplatte

10%
belegt

Noch 168 GB frei

RAM

8%
belegt

Noch 3 GB frei

Antivirus

Pattern ist aktuell

Abgewehrte Bedrohungen

4 HTTP-Viren abgewehrt
114 E-Mail-Viren abgewehrt
19881 C&C-Zugriffe abgewehrt
278 schädliche URLs abgewehrt

Kernel

33433
Drops

73698
Rejects

Alerts

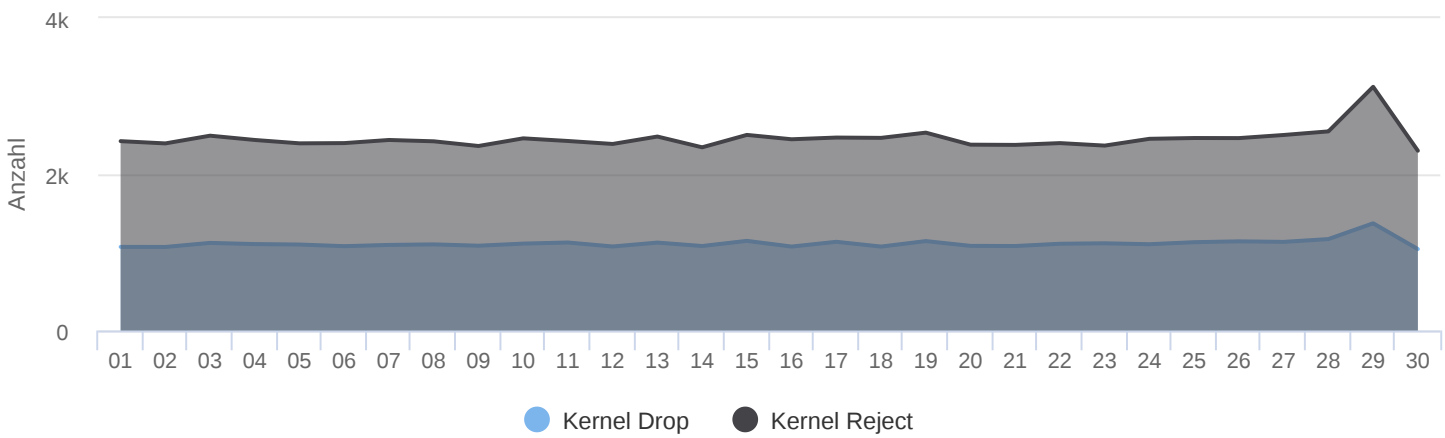
Kein Alert aufgetreten

Traffic HTTP

235
Gigabytes

Login fehlges.

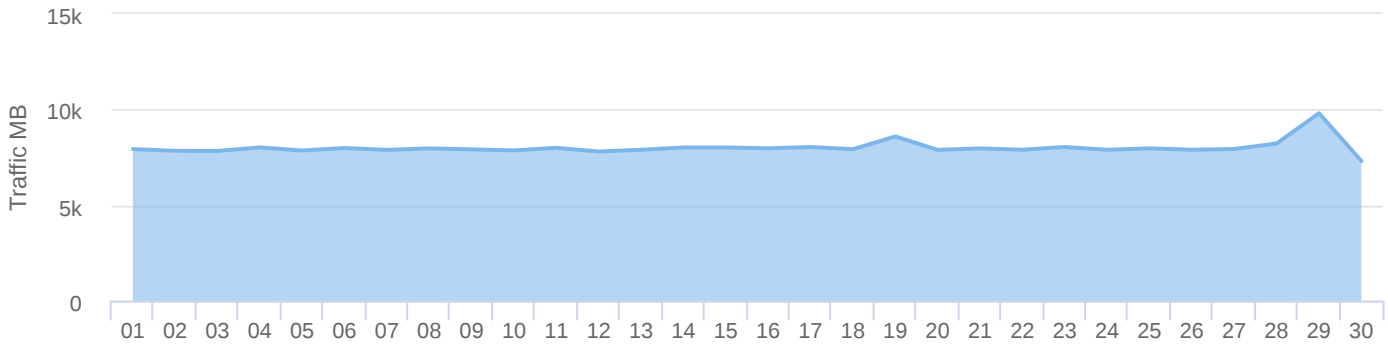
Keine Logins gefunden



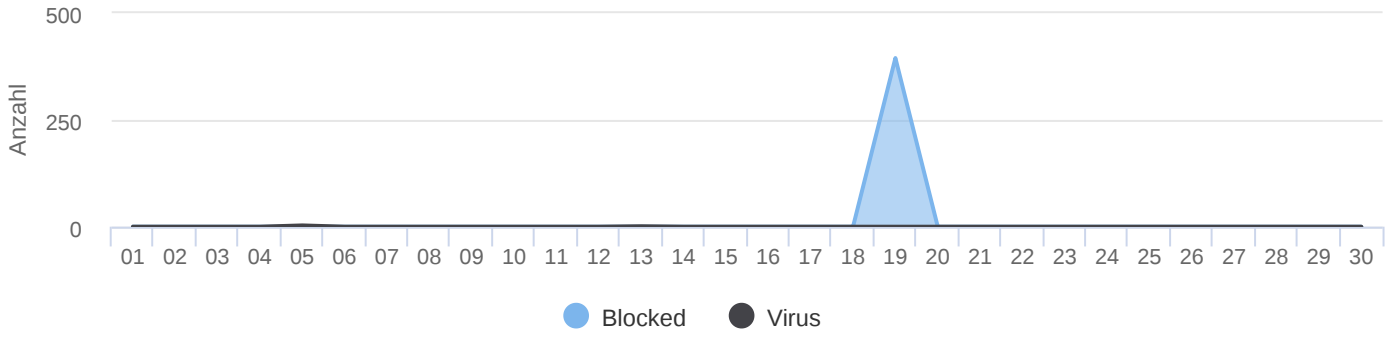
HTTP Übersicht

Traffic HTTP	Viren	Max. Benutzer	Geblockte URLs
235 Gigabytes	4 Viren abgewehrt	9 Benutzer	395 URLs geblockt

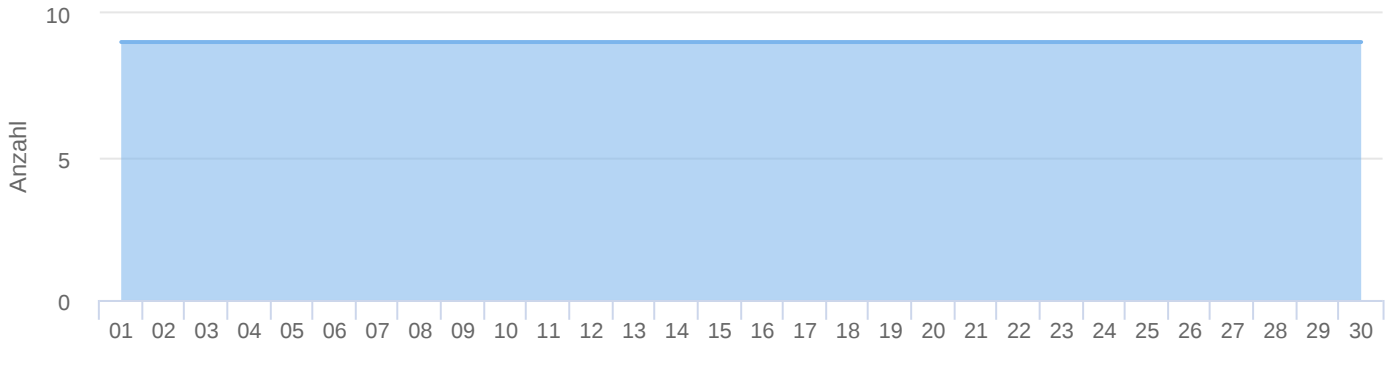
Traffic total



Sicherheitsaktionen



Benutzer



Top Domains

#	Domain/IP	Traffic
1	securepoint.de	17.22 GB
2	mediamarkt.de	3.24 GB
3	real.de	3.15 GB
4	mercedes-benz.com	1.66 GB
5	martin-perscheid.de	1.65 GB
6	sharepoint.de	1.65 GB
7	freenetmobile.de	1.64 GB
8	tchibo.de	1.64 GB
9	fahrrad-tour.de	1.64 GB
10	arcor.de	1.63 GB
11	lgl-bw.de	1.63 GB
12	polskieradio.pl	1.63 GB
13	seat.de	1.63 GB
14	test.de	1.62 GB
15	stayfriends.at	1.62 GB
16	abendblatt.de	1.62 GB
17	mydealz.de	1.62 GB
18	jako-o.de	1.62 GB
19	skoda-auto.com	1.62 GB
20	qvc.com	1.61 GB
21	nichtlustig.de	1.61 GB

Top geblockte Domains

#	Domain/IP	Anzahl
1	certified-toolbar.com	30
2	fromdoctopdf.com	25
3	driverupdate.net	23
4	smartpcupdate.com	23
5	mergedocsnow.com	22
6	brandlock.io	18
7	easyfileconvert.com	17
8	wootric.com	17
9	ad4m.at	15
10	adnxs.com	15
11	leokross.com	15
12	adform.net	14
13	adxcel-ec2.com	14
14	ad4mat.net	13
15	doubleclick.net	13
16	smartadserver.com	13
17	adalliance.io	12
18	nuggad.net	12
19	revjet.com	12
20	seeip.org	12
21	ad-srv.net	11

Top Kategorien

#	Kategorie	Traffic
1	Fahrzeuge	15.84 GB
2	Allow	15.79 GB
3	Kommunikation	15.76 GB
4	Haus und Garten	15.7 GB
5	Tiere	15.67 GB
6	Audio	15.65 GB
7	Computer	15.62 GB
8	Kinder	15.59 GB
9	Auktionen	15.58 GB
10	Shopping	15.57 GB
11	Humor	15.55 GB
12	Consumertechnik	15.53 GB
13	Reisen	15.52 GB
14	News	15.47 GB
15	Soziale Netzwerke	15.46 GB

Top geblockte Kategorien

#	Kategorie	Anzahl
1	Threat Intelligence Feed	140
2	Tracking strict	133
3	Werbe Dienste	122

Top abgewehrte Viren

#	Virus	Anzahl
1	Backdoor.Win32.Kirts	1
2	Trojan-Ransom.GlobeImposter	1
3	Trojan-Ransom.Locky	1
4	Trojan.Crypt	1

Top Benutzer

#	Name	Traffic
1	Anonymisierter Benutzer	26.22 GB
2	Anonymisierter Benutzer	26.21 GB
3	Anonymisierter Benutzer	26.14 GB
4	Anonymisierter Benutzer	26.05 GB
5	Anonymisierter Benutzer	26.03 GB
6	Anonymisierter Benutzer	26 GB
7	Anonymisierter Benutzer	25.99 GB
8	Anonymisierter Benutzer	25.98 GB
9	Anonymisierter Benutzer	25.69 GB

Top Viren-Benutzer

#	Name	Anzahl
1	Anonymisierter Benutzer	1
2	Anonymisierter Benutzer	1
3	Anonymisierter Benutzer	1
4	Anonymisierter Benutzer	1

Top geblockte Benutzer

#	Name	Anzahl
1	Anonymisierter Benutzer	50
2	Anonymisierter Benutzer	49
3	Anonymisierter Benutzer	48
4	Anonymisierter Benutzer	47
5	Anonymisierter Benutzer	45
6	Anonymisierter Benutzer	43
7	Anonymisierter Benutzer	42
8	Anonymisierter Benutzer	36
9	Anonymisierter Benutzer	35

Top Alerts

#	Name	Anzahl
1	IP gesperrt	393
2	Fallback-Aktivierung	376
3	Fallback-Deaktivierung	362
4	(V)DSL-Verbindungsfehler 2	348

Top Schweregrade

#	Name	Anzahl
1	Notice	391
2	Debug	373
3	Info	366
4	Warning	349

Top Logins

#	Name	Anzahl
1	sshd	641
2	user-ui	618
3	sslvpn	603
4	admin-ui	600

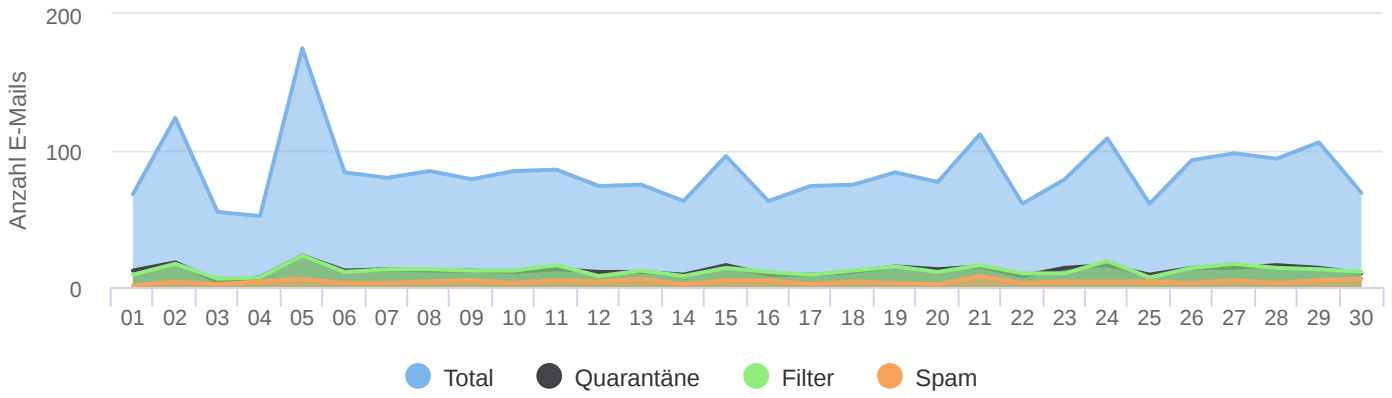
Top fehlgeschlagene Logins

Keine Daten vorhanden.

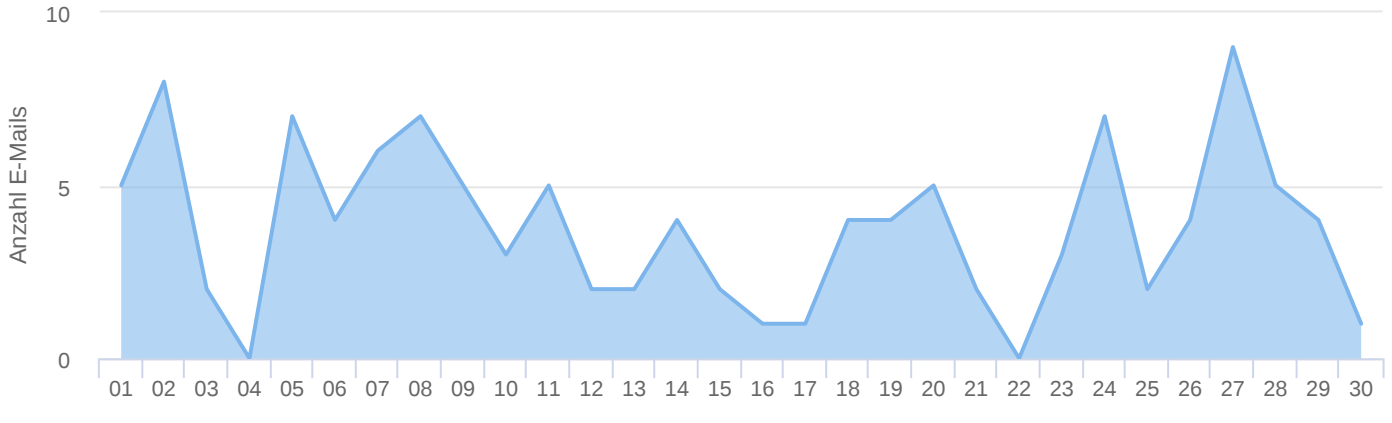
E-Mails total	Accept	Viren	Filter
2536	1056	114 Viren abgewehrt	370 E-Mails gefiltert

Drop	Quarantäne	Reject	Spam
370 E-Mails gedropt	371 E-Mails in Quarantäne	369 E-Mails rejected	118 E-Mails im Spam

E-Mails verarbeitet



Viren E-Mails



Top E-Mail-Empfänger

#	Adresse	Anzahl
1	Anonymisierte Adresse	100
2	Anonymisierte Adresse	100
3	Anonymisierte Adresse	100
4	Anonymisierte Adresse	99
5	Anonymisierte Adresse	98
6	Anonymisierte Adresse	97
7	Anonymisierte Adresse	97
8	Anonymisierte Adresse	97
9	Anonymisierte Adresse	95
10	Anonymisierte Adresse	94
11	Anonymisierte Adresse	93
12	Anonymisierte Adresse	91
13	Anonymisierte Adresse	91
14	Anonymisierte Adresse	91
15	Anonymisierte Adresse	90
16	Anonymisierte Adresse	89
17	Anonymisierte Adresse	88
18	Anonymisierte Adresse	86
19	Anonymisierte Adresse	82
20	Anonymisierte Adresse	81
21	Anonymisierte Adresse	79

Top E-Mail-Sender

#	Adresse	Anzahl
1	Anonymisierte Adresse	74
2	Anonymisierte Adresse	64
3	Anonymisierte Adresse	63
4	Anonymisierte Adresse	63
5	Anonymisierte Adresse	62
6	Anonymisierte Adresse	61
7	Anonymisierte Adresse	60
8	Anonymisierte Adresse	59
9	Anonymisierte Adresse	59
10	Anonymisierte Adresse	59
11	Anonymisierte Adresse	58
12	Anonymisierte Adresse	58
13	Anonymisierte Adresse	56
14	Anonymisierte Adresse	56
15	Anonymisierte Adresse	55
16	Anonymisierte Adresse	55
17	Anonymisierte Adresse	55
18	Anonymisierte Adresse	54
19	Anonymisierte Adresse	54
20	Anonymisierte Adresse	53
21	Anonymisierte Adresse	53

Top Spam-Empfänger

#	Adresse	Anzahl
1	Anonymisierte Adresse	10
2	Anonymisierte Adresse	8
3	Anonymisierte Adresse	7
4	Anonymisierte Adresse	7
5	Anonymisierte Adresse	6
6	Anonymisierte Adresse	6
7	Anonymisierte Adresse	5
8	Anonymisierte Adresse	5
9	Anonymisierte Adresse	5
10	Anonymisierte Adresse	5

Top Spam-Sender

#	Adresse	Anzahl
1	Anonymisierte Adresse	7
2	Anonymisierte Adresse	7
3	Anonymisierte Adresse	6
4	Anonymisierte Adresse	6
5	Anonymisierte Adresse	6
6	Anonymisierte Adresse	5
7	Anonymisierte Adresse	4
8	Anonymisierte Adresse	4
9	Anonymisierte Adresse	4
10	Anonymisierte Adresse	4

Top Quarantäne-Empfänger

#	Adresse	Anzahl
1	Anonymisierte Adresse	20
2	Anonymisierte Adresse	19
3	Anonymisierte Adresse	18
4	Anonymisierte Adresse	17
5	Anonymisierte Adresse	17
6	Anonymisierte Adresse	17
7	Anonymisierte Adresse	17
8	Anonymisierte Adresse	16
9	Anonymisierte Adresse	16
10	Anonymisierte Adresse	15

Top Quarantäne-Sender

#	Adresse	Anzahl
1	Anonymisierte Adresse	15
2	Anonymisierte Adresse	15
3	Anonymisierte Adresse	13
4	Anonymisierte Adresse	12
5	Anonymisierte Adresse	11
6	Anonymisierte Adresse	10
7	Anonymisierte Adresse	10
8	Anonymisierte Adresse	10
9	Anonymisierte Adresse	10
10	Anonymisierte Adresse	9

Top Virus-Empfänger

#	Adresse	Anzahl
1	Anonymisierte Adresse	8
2	Anonymisierte Adresse	7
3	Anonymisierte Adresse	6
4	Anonymisierte Adresse	6
5	Anonymisierte Adresse	6
6	Anonymisierte Adresse	6
7	Anonymisierte Adresse	6
8	Anonymisierte Adresse	5
9	Anonymisierte Adresse	5
10	Anonymisierte Adresse	5

Top Virus-Sender

#	Adresse	Anzahl
1	Anonymisierte Adresse	6
2	Anonymisierte Adresse	5
3	Anonymisierte Adresse	4
4	Anonymisierte Adresse	4
5	Anonymisierte Adresse	4
6	Anonymisierte Adresse	4
7	Anonymisierte Adresse	4
8	Anonymisierte Adresse	4
9	Anonymisierte Adresse	4
10	Anonymisierte Adresse	4

Top Virus

#	Name	Anzahl
1	VIRUS:EICAR_Te...IRUS FILTERED	114

Top Kernel Drops

#	IP	Anzahl
1	192.168.81.88	7
2	192.168.11.26	6
3	192.168.135.119	6
4	192.168.143.97	6
5	192.168.172.88	6
6	192.168.178.21	6
7	192.168.19.54	6
8	192.168.195.42	6
9	192.168.23.90	6
10	192.168.31.85	6
11	192.168.32.79	6
12	192.168.48.63	6
13	192.168.70.151	6
14	192.168.72.128	6
15	192.168.87.88	6
16	192.168.89.135	6
17	192.168.103.94	5
18	192.168.106.16	5
19	192.168.109.186	5
20	192.168.115.119	5
21	192.168.115.65	5

Top Kernel Reject

#	IP	Anzahl
1	192.168.101.125	10
2	192.168.167.117	10
3	192.168.185.40	10
4	192.168.67.32	10
5	192.168.116.153	9
6	192.168.126.151	9
7	192.168.192.46	9
8	192.168.198.44	9
9	192.168.34.156	9
10	192.168.40.112	9
11	192.168.46.95	9
12	192.168.73.106	9
13	192.168.73.136	9
14	192.168.87.10	9
15	192.168.104.196	8
16	192.168.107.114	8
17	192.168.109.152	8
18	192.168.114.11	8
19	192.168.117.103	8
20	192.168.128.35	8
21	192.168.135.65	8

Status

Risiko

Risiko

Rot markierte Werte, Geräte- oder der Unternehmensstatus zeigen eine akute Gefahr, ein Fachmann sollte unverzüglich den Grund überprüfen.

Status

Gefährdet

Gefährdet

Werden Werte, Geräte- oder der Unternehmensstatus orange angezeigt, so sollte der markierte Eintrag von einem Fachmann kontrolliert werden.

Status

Alles Okay

Alles Okay

Einzelne Werte, Geräte- oder der Unternehmensstatus werden grün angezeigt, wenn die ausgewerteten Daten unterhalb der Schwellwerte für „Gefährdungen“ liegen.

Status

Ohne Risikobewertung

Grau angezeigte Werte dienen ausschließlich der Information und fließen nicht in die Risikobewertung ein.

Hinweis

Wir weisen ausdrücklich darauf hin, dass der Unified Security Report unverbindlichen Informationszwecken dient und keine Systemberatung im eigentlichen Sinne darstellt. Der Inhalt des Unified Security Report kann und soll keine eigenverantwortliche Systembetreuung darstellen oder ersetzen. Alle Informationen verstehen sich ohne Gewähr auf Vollständigkeit und Richtigkeit.

Datenschutzerklärung

Datenschutzerklärung Unified Security Report

Tenant: 9993200.sms

Version: 1.1.20 [0af5bb]

Erklärung der Datenschutzeinstellung

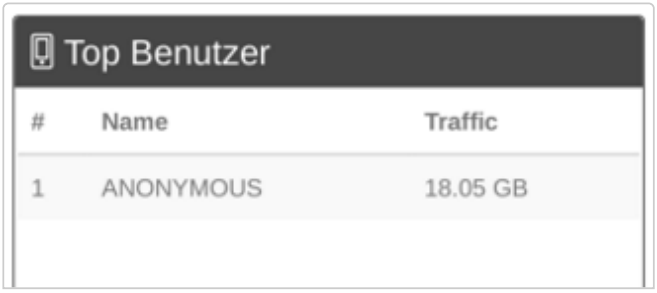
Für diesen Tenant ist die Datenschutzeinstellung aktiv. Wenn Sie Benutzernamen, E-Mail-Adressen, IPs etc. in Klartext sehen möchten, müssen Sie die Datenschutzeinstellung im Unified Security Portal(Wiki) deaktivieren. Dadurch ändern sich folgende Sachverhalte:

- Im Dashboard der Securepoint Mobile Security sind die Geräte in den Statistiken nicht mehr pseudonymisiert.
- Die Benutzernamen, E-Mail-Adressen, IPs etc. sind im Bericht nicht mehr anonymisiert.
- In der Mobile Security ist es möglich Warnungen für bestimmte Devices anzulegen.

Zusätzlich muss auf der UTM die Anonymisierung der Dienste deaktiviert sein, da ansonsten die Daten auf der UTM anonymisiert werden bevor sie an die Unified Security Cloud gesendet werden.

Diese Einstellungen können *nicht automatisch* auf der UTM(Wiki) vorgenommen werden und müssen deshalb vom Administrator durchgeführt werden.

Beispiel: Aktivierte Portal-Datenschutzeinstellung



Beispiel: Aktivierte UTM-Anonymisierung

Risikowerte

Jedes Produkt bzw. Device hat einen Status von 10. Risikoänderungen werden von diesem Status abgezogen. Das bedeutet ein sinkender Status erhöht das Risiko. Ein negativer Wert ist identisch mit dem Wert 0.

Es gibt drei Arten von Risiken, das eine zeigt ein eventuelles Problem bzw. Risiko auf, ändert aber nicht den Status des Produktes bzw. Devices. Das zweite Risiko ändert den Status des Produktes bzw. Devices. Das dritte Risiko ist eine Mischform, dass erst bei einem hohen Risko der Status geändert wird.

Risikobewertung Cover

Der Cover-Wert berechnet sich aus dem Mittelwert aller Risikowerte. Ist der berechnete Risikowert *kleiner 10* ist der Gesamtstatus "Gefährdert". Sobald der Wert *kleiner gleich 4* ist, ändert sich der Gesamtstatus zu "Risiko"!

Risiko = Summe(Produktstatus[Bei UTM wird das höhste Risiko genommen]) / Anzahl der Produkte

Risikobewertung Antivirus Pro

Widget	Erklärung
Lizenz	Das Risiko der Lizenz ändert sich bei einer Gültigkeit von weniger als 30 Tagen auf Medium. Dabei wird der Produktstatus um *-1* verändert. Wenn die Gültigkeit unter 14 Tagen ist, ändert sich das Risiko auf Hoch und der Produktstatus wird um *-2* verändert.
Muted	Das Risiko für Muted-Devices ändert sich auf Medium wenn alle Devices muted sind. Diese Risikoänderung hat keinen Einfluss auf den Produktstatus.
Viren	Wenn mehr Viren gefunden worden sind als Devices vorhanden, ändert sich das Risiko auf Medium. Dabei wird der Produktstatus um *-1* verändert. Wenn mehr Viren gefunden worden sind als *Devices * 2* vorhanden, ändert sich das Risiko auf Hoch. Dabei wird der Produktstatus um *-2* verändert.
Viren enfernt	Wenn weniger Viren entfernt als gefunden worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Produktstatus um *-4* verändert.
PUA	Wenn mehr PUA gefunden worden sind als Devices vorhanden, ändert sich das Risiko auf Medium. Dabei wird der Produktstatus um *-1* verändert. Wenn mehr PUA gefunden worden sind als *Devices * 2* vorhanden, ändert sich das Risiko auf Hoch. Dabei wird der Produktstatus um *-2* verändert.
PUA enfernt	Wenn weniger PUA entfernt als gefunden worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Produktstatus um *-2* verändert.

Risikobewertung Mobile Security

Widget	Erklärung
Lizenz	Das Risiko der Lizenz ändert sich bei einer Gültigkeit von weniger als 30 Tagen auf Medium. Dabei wird der Produktstatus um *-1* verändert. Wenn die Gültigkeit unter 15 Tagen ist, ändert sich das Risiko auf Hoch und der Produktstatus wird um *-5* verändert.
Privacy	Wenn Privacy deaktiviert ist, ändert sich das Risiko auf Medium. Dabei wird der Produktstatus nicht verändert.
Devices frei	Wenn weniger als *20%* der Devices frei sind, ändert sich das Risiko auf Medium. Dabei wird der Produktstatus nicht verändert. Wenn weniger als *5* Devices frei sind, ändert sich das Risiko auf Hoch. Dabei wird der Produktstatus nicht verändert. Wenn Devices ohne Lizenz vorhanden sind, ändert sich das Risiko auf Hoch. Dabei wird der Produktstatus wird um *-5* verändert.

Risikobewertung UTM-Firewall in der Dienste-Übersicht

Widget	Erklärung
Status	Der Status zeigt das höchste Risiko aller UTMs an.
Auslaufende Lizenzen	Das Risiko der auslaufende Lizenzen ändert sich, sobald eine UTM eine Gültigkeit von weniger als 4 Wochen hat auf Medium. Wenn die Gültigkeit einer UTM-Lizenz unter 15 Tagen ist, ändert sich das Risiko auf Hoch.
UTMs mit Risiko	Wenn eine UTM mit hohen Riskio vorhanden ist, ändert sich das Risiko auf Hoch. Wenn keine UTM mit hohem Risiko vorhanden ist, aber eine mit dem Risko "Gefährdet", dann ändert sich das Risiko auf Medium.
Logins fehlgeschlagen	Wenn die *Summe aller fehlgeschlagen Logins größer* ist als die *Anzahl UTM*, ändert sich das Risiko auf Medium. Wenn die *Summe aller fehlgeschlagen Logins größer* ist als die *Anzahl UTM * 5*, ändert sich das Risiko auf Hoch.

Risikobewertung UTM-Firewall

Widget	Erklärung
Auslaufende Lizenzen	Das Risiko der auslaufende Lizenzen ändert sich, sobald die UTM eine Lizenzgültigkeit von weniger als 4 Wochen hat auf Medium. Wenn die Gültigkeit der UTM-Lizenz unter 14 Tagen ist, ändert sich das Risiko auf Hoch.
UTM-Version	Wenn ein *"dryrun"* verfügbar ist, ändert sich das Risiko auf Medium. Dabei wird der Device-Status um *-1* verändert. Wenn ein *"finalize"* verfügbar ist, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-5* verändert.
Festplatte	Wenn vom Storage *mehr als 70% belegt* sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn vom Storage *mehr als 90% belegt* sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-1* verändert.
RAM	Wenn vom RAM *mehr als 70% belegt* sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn vom RAM *mehr als 90% belegt* sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-1* verändert.
Antivirus Clam	Wenn das letzte Pattern-Update *mehr als 24 Stunden* her ist, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn das letzte Pattern-Update *mehr als 48 Stunden* her ist, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-2* verändert. Wenn das Pattern-Update *deaktiviert* ist, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-2* verändert.
Antivirus CT	Wenn das letzte Pattern-Update *mehr als 24 Stunden* her ist, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn das letzte Pattern-Update *mehr als 48 Stunden* her ist, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-2* verändert. Wenn das Pattern-Update *deaktiviert* ist, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-2* verändert.
Alerts	Wenn Alerts mit einem Schweregrad von: EMERGENCY, ALERT, CRITICAL und ERROR auftreten, ändert sich das Risiko auf Medium. Die Zahl in Klammern gibt die gesamte Anzahl (inkl. Schweregrad: WARNING, NOTICE, INFO und DEBUG) der Alerts wieder. Dabei wird der Device-Status nicht verändert.

Risikobewertung UTM-Firewall

Widget	Erklärung
Fehlgeschlagene Logins	Wenn *mehr als 0* fehlgeschlagene Logins gefunden worden sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status um *-1* verändert. Wenn *mehr als 5* fehlgeschlagene Logins gefunden worden sind,, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-2* verändert.
E-Mail-Filter	Wenn *mehr als 10000* E-Mails gefiltert worden sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn *mehr als 50000* E-Mails gefiltert worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status *nicht* verändert.
E-Mail-Drop	Wenn *mehr als 10000* E-Mails gedropt worden sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn *mehr als 50000* E-Mails gedropt worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status *nicht* verändert.
E-Mail-Reject	Wenn *mehr als 10000* E-Mails rejected worden sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn *mehr als 50000* E-Mails rejected worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status *nicht* verändert.
E-Mail-Spam	Wenn *mehr als 10000* E-Mails als Spam erkannt worden sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn *mehr als 50000* E-Mails als Spam erkannt worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status um *-1* verändert.
E-Mail-Quarantäne	Wenn *mehr als 1000* E-Mails in Quarantäne einsortiert worden sind, ändert sich das Risiko auf Medium. Dabei wird der Device-Status *nicht* verändert. Wenn *mehr als 5000* E-Mails in Quarantäne einsortiert worden sind, ändert sich das Risiko auf Hoch. Dabei wird der Device-Status *nicht* verändert.