# NGFW Bewertungsbericht

**Vorbereitet für**
Informata College

**Vorbereitet von**
John Smith
Fortinet

**Berichtsdatum**
Jun 28, 2019

# Executive Summary

Wir haben die wichtigsten Ergebnisse unserer NGFW-Bewertung in der folgenden Executive Summary zusammengefasst. Die Highlights sind unten aufgeführt und es folgt eine detailliertere Ansicht der einzelnen Abschnitte. Lesen Sie auch die Seite „Empfohlene Maßnahmen“ am Ende dieses Berichts, um herauszufinden, welche Maßnahmen Ihr Unternehmen ergreifen kann, um eingehende Bedrohungen zu minimieren, unternehmensinterne Nutzungsrichtlinien umzusetzen und Probleme bei der Kapazitätsplanung zu vermeiden.

## Sicherheit

**11,126**
Angriffe auf Anwendungsschwachstellen erkannt

**13**
Malware und/oder Botnetze erkannt


**17**
Stark risikobehaftete Anwendungen erkannt

Beachten Sie, dass alle in diesem Bericht aufgezeichneten Bedrohungen Ihr bestehendes Netzwerk Security Gateway effektiv umgangen haben, so dass sie als aktiv angesehen werden sollten und zu einem erhöhten Risiko führen können (z. B. zu einer Datenpanne).

---

## Produktivität

**330**
Anwendungen insgesamt erkannt

**5**
Proxy-Anwendungen insgesamt erkannt

**5**
Peer-to-Peer-Anwendungen insgesamt

Die Anwendungsnutzung hat üblicherweise einen starken Einfluss auf Ihre Netzwerkarchitektur. Das Verständnis, welche Arten von Anwendungen verwendet werden, kann sich auf die unternehmensinternen Nutzungsrichtlinien, die Kontrolle über segmentierte Netzwerke und die Nutzung von Cloud-basierten Service-Plattformen auswirken.

---

## Nutzung

**40.5**GB
Genutzte Gesamtbandbreite

**12.5**
Durchschnittliche Protokollrate pro Sekunde


**58.0**%
Prozentsatz des SSL-verschlüsselten Datenverkehrs

Zusätzlich zu den einzelnen Anwendungen kann ein Verständnis der Gesamtauslastung bei der Kapazitätsplanung und der Optimierung des Netzwerkverkehrs im Verlauf der Zeit helfen.

# Sicherheit

**Schnellstatistiken**

- **50** erkannte Angriffe auf Anwendungsschwachstellen
- **1** erkanntes bekanntes Botnet
- **125** erkannte bösartige Websites
- **17** erkannte stark risikobehaftete Anwendungen
- **1** erkannte Phishing-Websites
- **13** erkannte bekannte Malware
- **8,190** von Sandbox analysierte Dateien
- **36** von Sandbox gefundene verdächtige Dateien

## Die wichtigsten erkannten Anwendungsschwachstellen-Exploits

Anwendungsschwachstellen können ausgenutzt werden und die Sicherheit Ihres Netzwerks gefährden. Das FortiGuard-Forschungsteam analysiert diese Schwachstellen und entwickelt anschließend Signaturen zu deren Erkennung. Aktuell bedient sich FortiGuard einer Datenbank mit über 5800 bekannten Anwendungsbedrohungen, um Angriffe auf herkömmliche Firewall-Systeme abzuwehren. Weitere Informationen zu Anwendungsschwachstellen erhalten Sie auf der Website von FortiGuard unter http://www.fortiguard.com/intrusion.

| # | Risiko | Bedrohungsname | Typ | Opfer | Quellen | Anzahl |
|---|---|---|---|---|---|---|
| 1 | 5 | Adobe.Flash.Player.Authplay.DLL.SWF.Handling.Code.Execution | | 1 | 1 | 2,035 |
| 2 | 5 | IBM.Rational.ClearQuest.Username.Parameter.SQL.Injection | SQL Injection | 30 | 1 | 195 |
| 3 | 5 | Bash.Function.Definitions.Remote.Code.Execution | OS Command Injection | 8 | 3 | 15 |
| 4 | 5 | MS.GDIPlus.JPEG.Buffer.Overflow | Buffer Errors | 3 | 2 | 10 |
| 5 | 5 | MS.IE.MSXML.Object.Handling.Code.Execution | Buffer Errors | 1 | 1 | 2 |
| 6 | 5 | McAfee.Web.Reporter.EJBInvokerServlet.Object.Code.Execution | Code Injection | 1 | 1 | 1 |
| 7 | 4 | LaVague.PrintBar.PHP.File.Inclusion | Code Injection | 30 | 1 | 183 |
| 8 | 4 | IISadmin.ISM.DLL.Access | Information Disclosure | 29 | 1 | 169 |
| 9 | 4 | GameSiteScript.Index.PHP.SQL.Injection | SQL Injection | 30 | 1 | 169 |
| 10 | 4 | OTE.Header.PHP.File.Inclusion | Code Injection | 30 | 1 | 163 |

## Die wichtigsten erkannten Fälle von Malware, Botnets und Spyware/Adware

Für die Malware-Verbreitung stehen Cyberkriminellen zahlreiche Kanäle zur Verfügung. Bei den gängigsten Methoden werden Benutzer motiviert, einen infizierten E-Mail-Anhang zu öffnen, eine infizierte Datei herunterzuladen oder auf einen Link zu einer infizierten Website zu klicken. Fortinet hat im Rahmen der Sicherheitsbewertung eine Reihe von Malware- und Botnet-Ereignisse identifiziert. Diese deuten darauf hin, dass schädliche Dateien heruntergeladen oder Websites mit Botnet-Befehlen und -Kontrollfunktionen aufgerufen wurden.

| # | Malware-Name | Typ | Anwendung | Opfer | Quellen | Anzahl |
|---|---|---|---|---|---|---|
| 1 | EICAR_TEST_FILE | Virus | FTP | 1 | 1 | 824 |
| 2 | EICAR_TEST_FILE | Virus | HTTP | 1 | 1 | 792 |
| 3 | Asprox.Botnet | Botnet C&C | Asprox.Botnet | 55 | 1 | 600 |
| 4 | Adware/TEST_FILE | Adware | HTTP | 1 | 1 | 411 |
| 5 | ETDB_TEST_FILE | Virus | FTP | 1 | 1 | 406 |
| 6 | W32/NGVCK | Virus | HTTP | 1 | 1 | 405 |
| 7 | W32/ForeignRansom.583D!tr | Virus | HTTP | 1 | 1 | 400 |
| 8 | W32/ForeignRansom.583D!tr | Virus | FTP | 1 | 1 | 395 |
| 9 | W32/NGVCK | Virus | FTP | 1 | 1 | 384 |
| 10 | Adware/TEST_FILE | Adware | FTP | 1 | 1 | 379 |

# Sicherheit

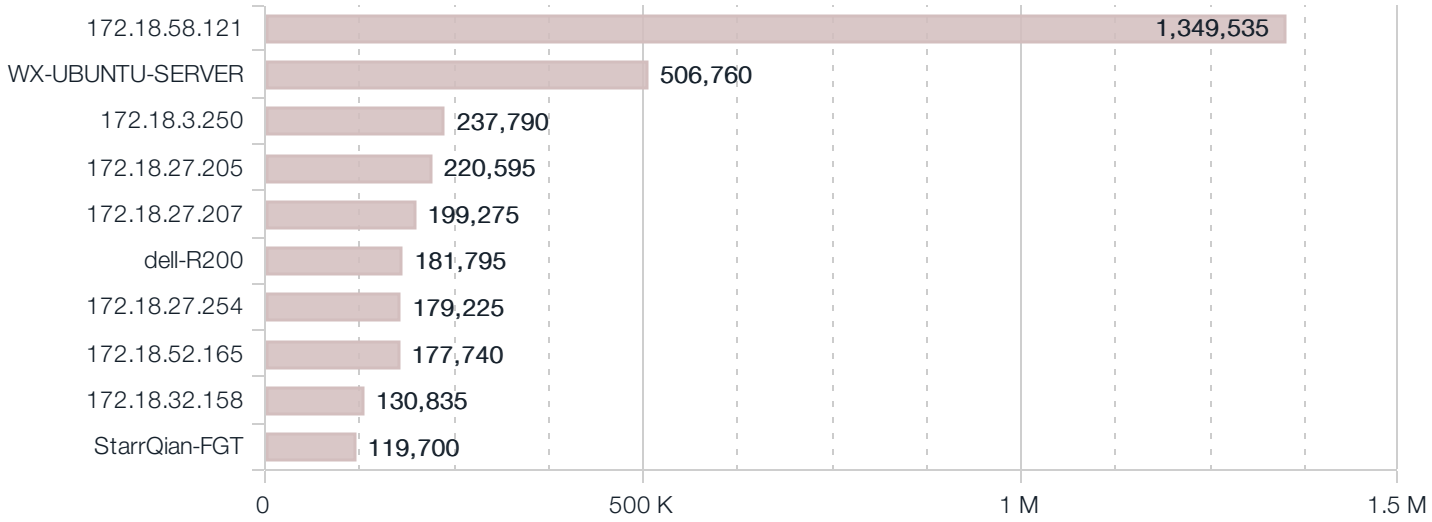
## Stark risikobehaftete Anwendungen

Das FortiGuard-Forschungsteam weist Anwendungen basierend auf ihren Verhaltensmerkmalen eine Risikobewertung zwischen 1 und 5 zu. Administratoren können dadurch stark risikobehaftete Anwendungen schnell identifizieren und bessere Entscheidungen bezüglich der Applikationskontrollrichtlinie treffen. Die folgenden Anwendungen wurden mit einer Risikobewertung von 4 oder höher eingestuft.

| # | Risiko | Anwendung | Kategorie | Technologie | Benutzer | Bandbreite | Sitzungen |
|---|---|---|---|---|---|---|---|
| 1 | 5 | Asprox.Botnet | Botnet | Client-Server | 1 | 1.74 MB | 587 |
| 2 | 5 | Proxy.HTTP | Proxy | Network-Protocol | 11 | 7.10 MB | 457 |
| 3 | 5 | Onavo.Protect | Proxy | Client-Server | 1 | 1.78 KB | 9 |
| 4 | 5 | Hotspot.Shield | Proxy | Client-Server | 2 | 203.99 KB | 8 |
| 5 | 5 | Skyfire | Proxy | Client-Server | 3 | 27.20 KB | 3 |
| 6 | 4 | Rsh | Remote.Access | Client-Server | 67 | 9.82 GB | 302,237 |
| 7 | 4 | BitTorrent | P2P | Peer-to-Peer | 8 | 1.79 MB | 5,096 |
| 8 | 4 | Telnet | Remote.Access | Client-Server | 9 | 37.81 MB | 681 |
| 9 | 4 | RDP | Remote.Access | Client-Server | 14 | 9.89 MB | 48 |
| 10 | 4 | TeamViewer | Remote.Access | Client-Server | 22 | 1.13 MB | 38 |

## Gefährdete Geräte und Hosts

Basierend auf den unterschiedlichen Arten von Aktivitäten eines individuellen Hosts können wir die Vertrauenswürdigkeit jedes einzelnen Clients bewerten. Diese Client-Reputation basiert auf Schlüsselfaktoren wie aufgerufene Websites sowie genutzten Anwendungen und eingehenden/ausgehenden Zielen. Schließlich können wir eine Gesamtbedrohungswertung erstellen, indem wir uns die gesamten Aktivitäten jedes Hosts ansehen.



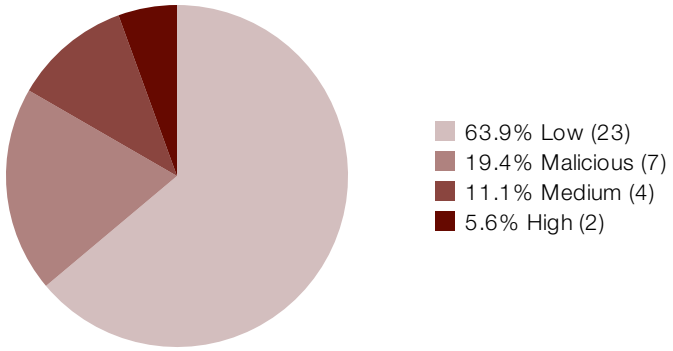
## Unbekannte Malware

Der Umstand, dass heutige Bedrohungen immer ausgefeilter werden, kann deren Bösartigkeit verschleiern und die traditionelle Sicherheit durch Anti-Malware umgehen. Im verfügbaren Zeitrahmen sind herkömmliche Anti-Malware-Engines oft nicht in der Lagen, mit der erforderlichen Sicherheit bestimmte Nutzlasten als gut oder schlecht einzustufen. In der Tat ist es sogar so, dass deren Zweck unbekannt ist. Sandbox-Technologie hilft, dieses Problem zu lösen – unbekannte Dateien werden in eine geschützte Umgebung gelockt, das daraus resultierende Verhalten wird beobachtet und das Risiko basierend auf diesem Verhalten klassifiziert. Da diese Funktionalität für Sie zwecks Bewertung aktiviert ist, haben wir uns die Dateien, die Ihr Netzwerk durchlaufen, genauer angesehen.

| # | Dateiname | Service | Risiko | Verdächtige Verhaltensweisen | Anzahl |
|---|---|---|---|---|---|
| 1 | 1D26B266.vXE | HTTP | Malicious | Threat_Intelligence<br>The executable tries to inject a PE image to other processess<br>Executable deleted itself after execution<br>Executable dropped a copy of itself<br>This file checked registry for anti-virtualization or anti-debug<br>This file checked devices for anti-virtualization or anti-debug | 1 |
| 2 | 1D28E4E7.vsc | HTTP | Malicious | Threat_Intelligence<br>The executable tries to inject a PE image to other processess | 1 |
| 3 | 1D43634F.vsc | HTTP | Malicious | Threat_Intelligence<br>The executable tries to inject a PE image to other processess<br>Executable deleted itself after execution<br>Executable dropped a copy of itself<br>This file checked registry for anti-virtualization or anti-debug<br>This file checked devices for anti-virtualization or anti-debug | 1 |
| 4 | 1D45FCB7.vsc | HTTP | Malicious | Threat_Intelligence<br>The executable tries to inject a PE image to other processess<br>Executable deleted itself after execution | 1 |
| 5 | 1D46A1FA.vsc | HTTP | Malicious | Threat_Intelligence<br>The executable tries to inject a PE image to other processess<br>Executable deleted itself after execution | 1 |
| 6 | 1D46A601.vXE | HTTP | Malicious | Threat_Intelligence<br>The executable tries to inject a PE image to other processess<br>Executable deleted itself after execution<br>Executable dropped a copy of itself<br>This file checked registry for anti-virtualization or anti-debug<br>This file checked devices for anti-virtualization or anti-debug | 1 |

## Bösartige und verdächtige Dateien

Im Allgemeinen werden die Ergebnisse der Verhaltensanalyse auf eine der drei folgenden Arten kategorisiert: sauber, verdächtig oder bösartig. Die Kennzeichnung „sauber“ bedeutet, dass kein anormales Verhalten beobachtet wurde und die Datei als sicher angesehen werden kann. Verdächtige Aktivitäten sind potenziell gefährlich und können weitere Aufmerksamkeit erfordern – zum Beispiel kann eine als hoch verdächtige eingestufte Datei versuchen, sich selbst zu replizieren, während eine als gering verdächtig eingestufte Datei nur abnorme Registrierungseinstellungen erzeugt. Die Kennzeichnung „bösartig“ sollte als legitime Bedrohung für Ihr Netzwerk betrachtet werden und erfordert sofortige Aufmerksamkeit. Das hier dargestellte Diagramm zeigt bösartige und verdächtige Dateien (z. B. enthält es keine als sauber gekennzeichneten Dateien).



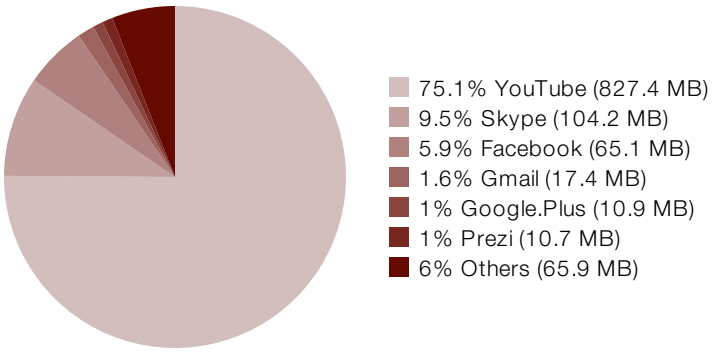
# Produktivität

**Schnellstatistiken**

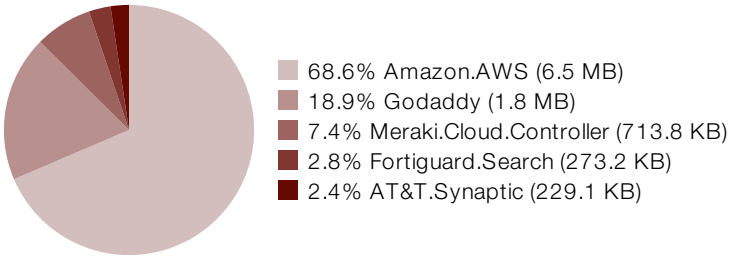
- **330** erkannte Anwendungen insgesamt
- **5** erkannte Proxy-Anwendungen insgesamt
- **5** Gefundene Peer-to-Peer-Anwendungen
- **5** Gefundene Fernzugriffsanwendungen
- **SSL** ist die am häufigsten verwendete Anwendung
- **Network.Service** ist die am häufigsten verwendete Anwendungskategorie
- **567** besuchte Websites insgesamt
- **ca.archive.ubuntu.com** ist die am häufigsten besuchte Website

## Cloud-Nutzung (SaaS)

IT-Manager sind sich häufig der Menge der innerhalb ihrer Organisation verwendeten Cloud-Services gar nicht bewusst. Diese Anwendungen sollten eigentlich die Benutzerfreundlichkeit erhöhen, werden jedoch mitunter genutzt, um die vorhandene Unternehmensinfrastruktur zu umgehen oder sogar zu ersetzen. Ein möglicher Nebeneffekt ist, dass Ihre sensiblen Unternehmensinformationen in die Cloud gelangen. Bei einem Angriff auf die Sicherheitsinfrastruktur des Cloud-Anbieters könnten Ihre Daten folglich offengelegt werden.



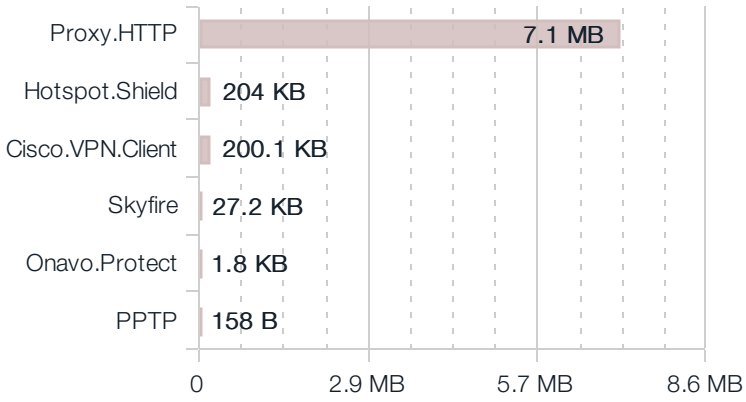

## Cloud-Nutzung (IaaS)



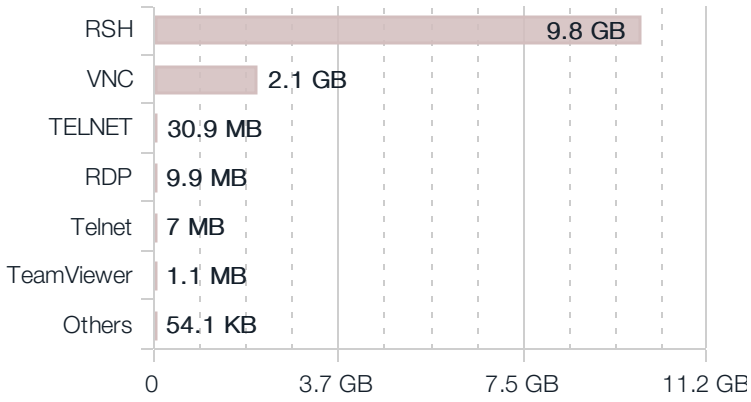

Es werden häufig IaaS-Plattformen (Infrastructure-as-a-Service) genutzt. Dies kann hilfreich sein, wenn Computing-Ressourcen begrenzt sind oder speziellen Anforderungen unterliegen. Das effektive Outsourcing Ihrer Infrastruktur muss dabei gründlich reguliert werden, um einen Missbrauch zu vermeiden. Die gelegentliche Prüfung von IaaS-Anwendungen ist nicht nur aus Sicherheitsgründen von Vorteil, sondern kann auch die Betriebskosten für Pay-per-Use-Modelle oder wiederkehrende Abonnementgebühren minimieren.

# Produktivität

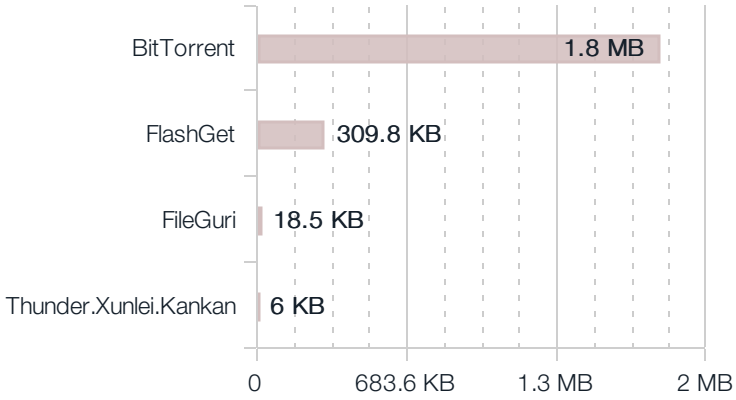
## Proxy-Anwendungen



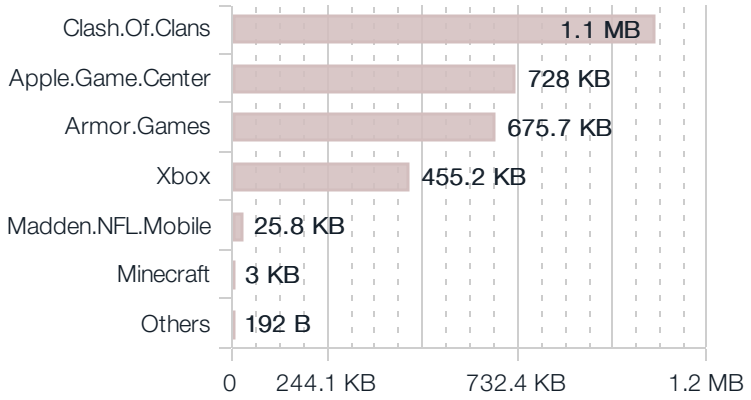

## Fernzugriffsanwendungen



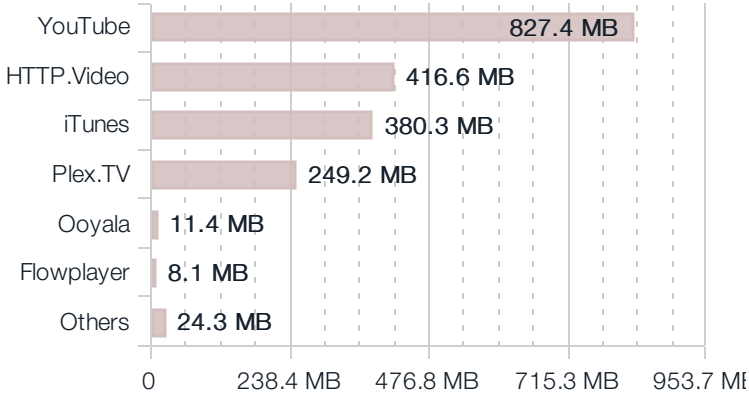

## Top-Peer-to-Peer-Anwendungen



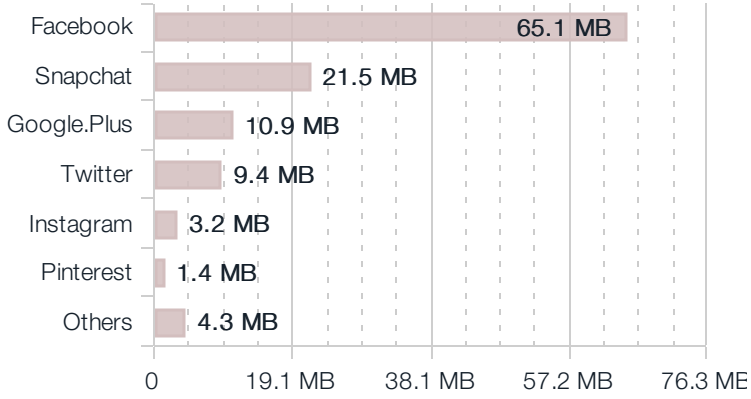

## Top-Spieleanwendungen




## Top-Video-/Audio-Streaming-Anwendungen




## Top-Social-Media-Anwendungen



# Produktivität

## Top-Webanwendungen

In den heutigen Netzwerkumgebungen kommunizieren viele Anwendungen über HTTP – darunter auch einige, von denen man dies eigentlich nicht erwarten würde. Der Hauptvorteil von HTTP besteht darin, dass dieser Kommunikationskanal überall verbreitet, akzeptiert und in den meisten Firewalls (in der Regel) geöffnet ist. Bei den meisten geschäftlichen Anwendungen, die einer Whitelist hinzugefügt wurden, fördert dies im Allgemeinen die Kommunikation. Einige nichtgeschäftliche Anwendungen nutzen HTTP jedoch in unproduktiver oder möglicherweise schädigender Art.

| # | Anwendung | Sitzungen | Bandbreite |
|---|---|---|---|
| 1 | SSL | 129,754 | 6.28 GB |
| 2 | HTTP.BROWSER | 223,132 | 4.41 GB |
| 3 | HTTPS | 110,074 | 2.99 GB |
| 4 | HTTP | 48,555 | 853.75 MB |
| 5 | YouTube | 4,139 | 806.89 MB |
| 6 | HTTP.Audio | 532 | 507.46 MB |
| 7 | HTTP.Video | 298 | 415.62 MB |
| 8 | iTunes | 180 | 380.32 MB |
| 9 | HTTPS.BROWSER | 7,338 | 372.21 MB |
| 10 | Apple.Services | 25 | 241.61 MB |

## Top-Websites nach Surfzeit

Schätzungen der Surfzeiten auf individuellen Websites können nützlich sein, um sich einen Einblick in beliebte Websites zu verschaffen. Die Ergebnisse beziehen sich in der Regel auf interne Webressourcen wie Intranets, können jedoch mitunter auch auf eine übermäßige Nutzung hindeuten. Lange Surfzeiten können die Implementierung von Web-Caching-Technologien rechtfertigen oder Anlass zum Erstellen von unternehmensinternen Nutzungsrichtlinien geben.

| # | Domäne | Kategorie | Surfzeit (hh:mm:ss) |
|---|---|---|---|
| 1 | ssw.live.com | Search Engines and Portals | 00:26:46 |
| 2 | blu407-m.hotmail.com | Web-based Email | 00:17:32 |
| 3 | crl.microsoft.com | Information Technology, Web Hosting | 00:16:22 |
| 4 | www.microsoft.com | Information Technology | 00:12:13 |
| 5 | 173.194.33.86 | Search Engines and Portals | 00:11:15 |
| 6 | 23.209.27.138 | Unrated | 00:10:35 |
| 7 | 64.37.102.54 | Business | 00:10:25 |
| 8 | ca.archive.ubuntu.com | Reference | 00:10:24 |
| 9 | 17.154.66.47 | Unrated | 00:09:53 |
| 10 | 109.200.4.26 | Unrated | 00:09:48 |

# Produktivität

## Top-Webkategorien

Das Surfverhalten weist eventuell nicht nur auf eine ineffiziente Verwendung von Unternehmensressourcen hin, sondern ist ggf. auch ein Zeichen für eine suboptimale Webfilter-Richtlinie. Außerdem kann es Einblicke in das allgemeine Surfverhalten der Mitarbeiter gewähren und bei der Festlegung von unternehmensinternen Compliance-Richtlinien helfen.

| # | URL-Kategorie | Benutzer | Anzahl | Bandbreite |
|---|---|---|---|---|
| 1 | Unrated | 3 | 1,359 | 2.06 MB |
| 2 | Information Technology | 5 | 1,106 | 56.71 MB |
| 3 | Search Engines and Portals | 5 | 757 | 40.05 MB |
| 4 | Advertising | 4 | 558 | 4.82 MB |
| 5 | Web Hosting | 3 | 447 | 2.68 MB |
| 6 | Instant Messaging | 3 | 285 | 1.75 MB |
| 7 | File Sharing and Storage | 3 | 257 | 1,018.61 KB |
| 8 | Business | 4 | 245 | 3.97 MB |
| 9 | News and Media | 3 | 212 | 7.78 MB |
| 10 | Content Servers | 4 | 205 | 7.94 MB |

## Meist besuchte Webdomänen

Besuchte Webseiten geben eindeutige Hinweise auf die Nutzung von Unternehmensressourcen durch Mitarbeiter und darauf, wie Anwendungen mit bestimmten Webseiten kommunizieren. Die Analyse der besuchten Domänen kann zu Änderungen in der Unternehmensinfrastruktur führen. Möglich sind unter anderem das Sperren von Webseiten, die umfassende Untersuchung Cloud-basierter Anwendungen und die Implementierung von Beschleunigungstechnologien für den Webdatenverkehr.

| # | Domäne | Kategorie | Besuche |
|---|---|---|---|
| 1 | ca.archive.ubuntu.com | Reference | 1,256 |
| 2 | ads2.westca.com | Advertising | 462 |
| 3 | security.ubuntu.com | Information Technology | 387 |
| 4 | cdn.speedshiftmedia.com | Advertising | 335 |
| 5 | gs-loc.apple.com | Information Technology | 194 |
| 6 | caextshort.weixin.qq.com | Instant Messaging | 157 |
| 7 | mmsns.qpic.cn | Content Servers | 156 |
| 8 | 173.194.33.86 | Search Engines and Portals | 133 |
| 9 | 23.209.27.138 | Unrated | 123 |
| 10 | 23.3.105.162 | Unrated | 122 |

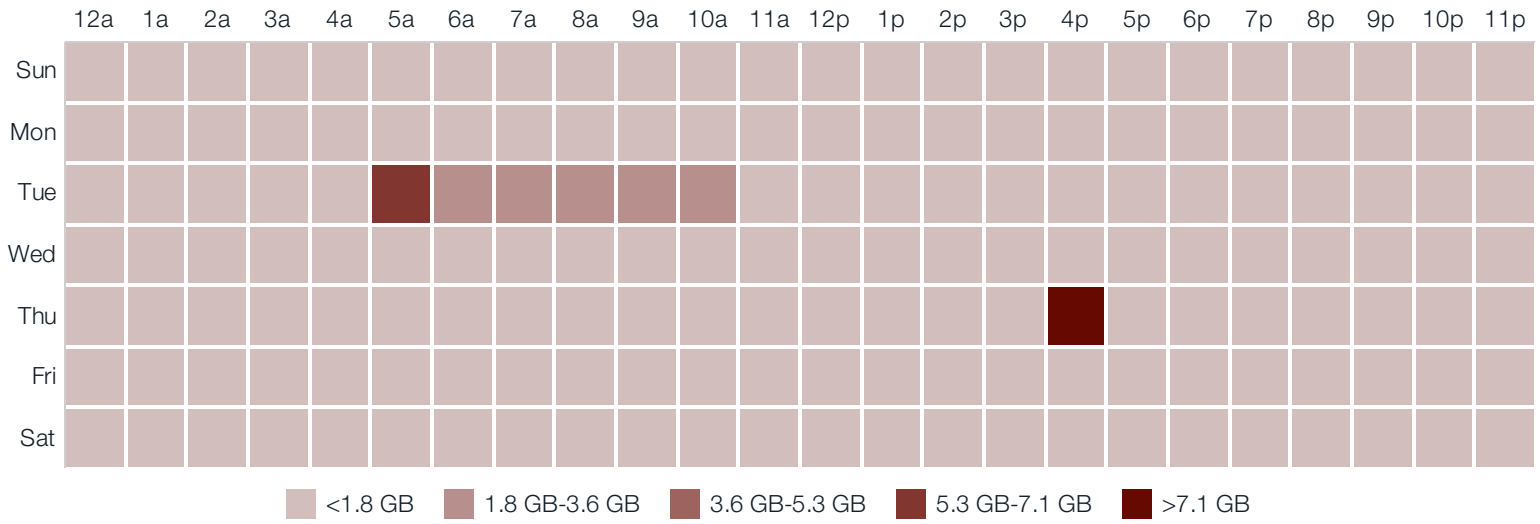
# Nutzung

Schnellstatistiken

- **40.5 GB** genutzte Gesamtbandbreite
- **58.0%** Prozentsatz des SSL-verschlüsselten Datenverkehrs
- **4pm - 5pm** ist die höchste tägliche Spitzenauslastung
- **192.168.1.119** ist die Quelle mit der höchsten Sitzungs-Bandbreite
- **10.2.60.117** ist die Quelle mit der höchsten Anzahl von Sitzungen
- **12.5** durchschnittliche Protokollrate pro Sekunde
- **2.8%** durchschnittliche CPU-Nutzung durch FortiGate
- **61.7%** durchschnittliche Speicherauslastung durch FortiGate

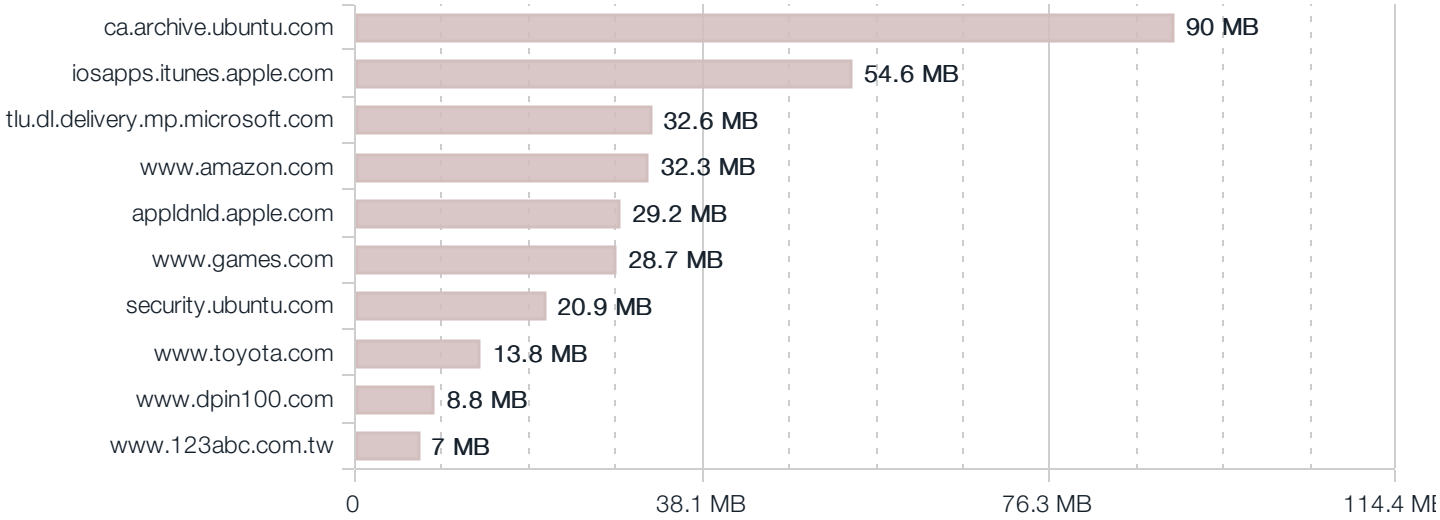
## Durchschnittliche Bandbreitennutzung pro Stunde

Durch die Analyse der Bandbreitennutzung an einem durchschnittlichen Tag erhalten Administratoren einen verbesserten Einblick in die betrieblichen Anforderungen bezüglich ISP-Verbindungen und Schnittstellengeschwindigkeit. Die Bandbreitennutzung kann auch mittels Drosselung für bestimmte Anwendungen optimiert und während Spitzenverkehrszeiten für bestimmte Benutzer priorisiert werden. Updates lassen sich außerhalb der Arbeitszeiten planen.




## Bandbreitenerschöpfende Top-Quellen/-Ziele

Zu den aussagekräftigsten Bandbreitenanalysen zählt die Prüfung der Ziele und Quellen, die den meisten Datenverkehr generieren. Gängige Ziel-Websites (z. B. externe Websites), etwa für Betriebssystem-/Firmware-Updates, können zur Priorisierung von unternehmenskritischem Datenverkehr gedrosselt werden. Interne Hosts mit hohem Datenverkehrsaufkommen lassen sich durch die Kategorisierung des Datenverkehrs (Traffic Shaping) oder unternehmensinterne Nutzungsrichtlinien optimieren.


ca.archive.ubuntu.com
90 MB
iosapps.itunes.apple.com
54.6 MB
tlu.dl.delivery.mp.microsoft.com
32.6 MB
www.amazon.com
32.3 MB
appldnld.apple.com
29.2 MB
www.games.com
28.7 MB
security.ubuntu.com
20.9 MB
www.toyota.com
13.8 MB
www.dpin100.com
8.8 MB
www.123abc.com.tw
7 MB
0
38.1 MB
76.3 MB
114.4 MB

# Nutzung

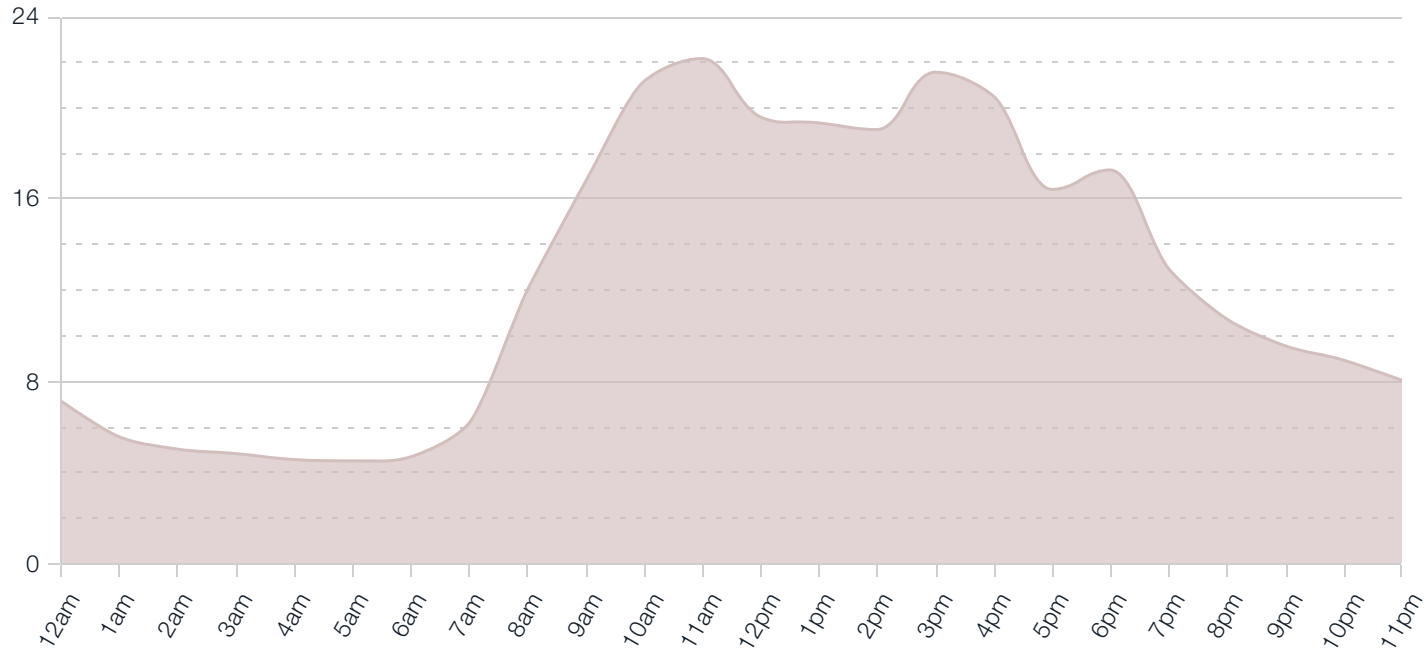
## Top-Ursprungsländer

Anhand des Datenverkehrs von der IP-Quelle können wir das Ursprungsland einer jeweiligen Anforderung ermitteln. Bestimmte Botnets, Befehls- und Kontrollfunktionen und sogar der Fernzugriff können sitzungslastig sein und auf gezielte Angriffe oder dauerhafte Bedrohungen durch Nationalstaaten hindeuten. Dieses Diagramm zeigt den landesspezifischen Datenverkehr. Die Aktivitäten von bestimmten Herkunftsländer können anormal sein und eine eingehendere Untersuchung rechtfertigen.

| # | Land | Bandbreite |
|---|---|---|
| 1 | United States | 213.31 MB |
| 2 | Anonymous Proxy | 7.73 MB |
| 3 | United Kingdom | 4.13 MB |
| 4 | Belgium | 1.51 MB |
| 5 | Netherlands | 603.07 KB |
| 6 | Ireland | 389.32 KB |
| 7 | Romania | 47.75 KB |
| 8 | Russian Federation | 37.82 KB |
| 9 | France | 26.88 KB |
| 10 | China | 4.12 KB |

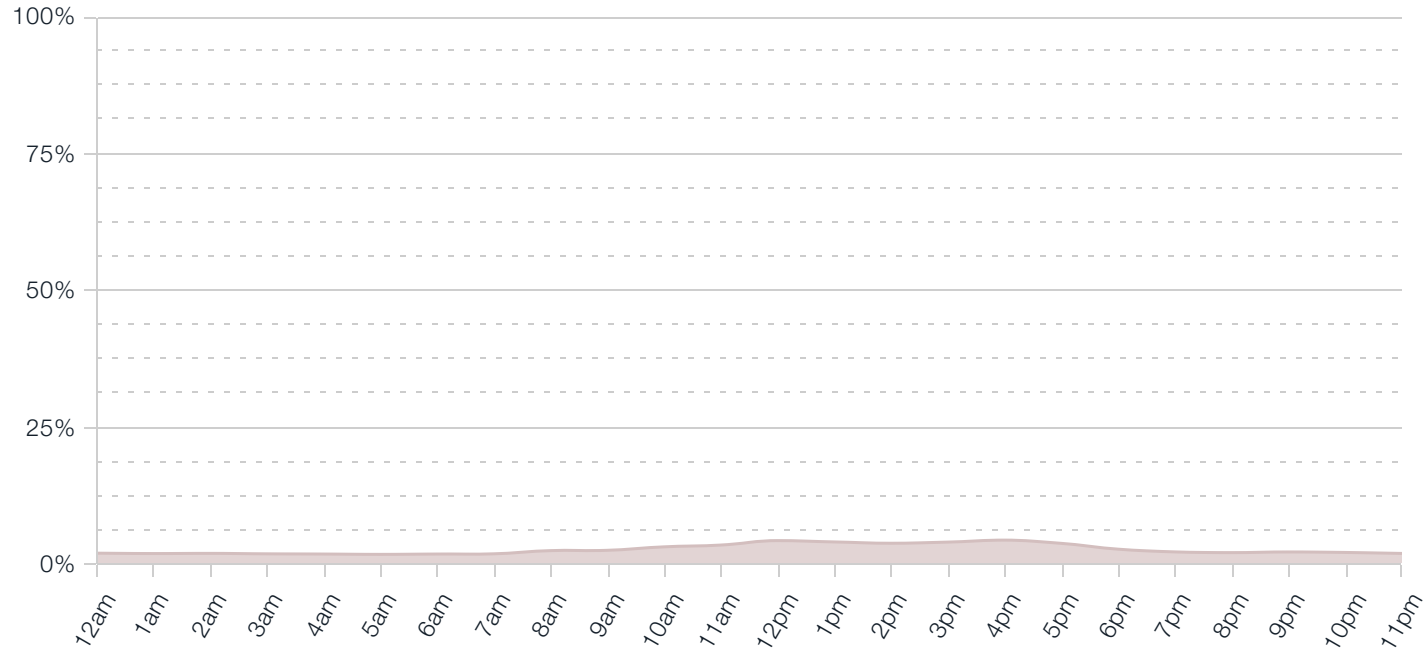
## Durchschnittliche Protokollrate pro Stunde

Bei der leistungsbedingten Größenanpassung einer Sicherheitsumgebung ist es von enormem Vorteil, die durchschnittlichen Protokollraten zu kennen. Erhöhte durchschnittliche Protokollraten zu bestimmten Uhrzeiten weisen in der Regel auf Spitzenzeiten bezüglich der Bandbreitennutzung und des Datendurchsatzes hin. Die unternehmensweiten Protokollraten zu berechnen, kann auch bei der Größenanpassung von Upstream-Protokollierungs- und -Analyseanwendungen wie FortiAnalyzer nützlich sein. Beachten Sie, dass bei den hier angegebenen Protokollraten die vollständigen Protokollierungsfunktionen von FortiGate aktiviert waren und diese daher alle Protokolltypen enthalten (Datenverkehr, Antivirus, Anwendung, IPS, Web- und Systemereignisse).



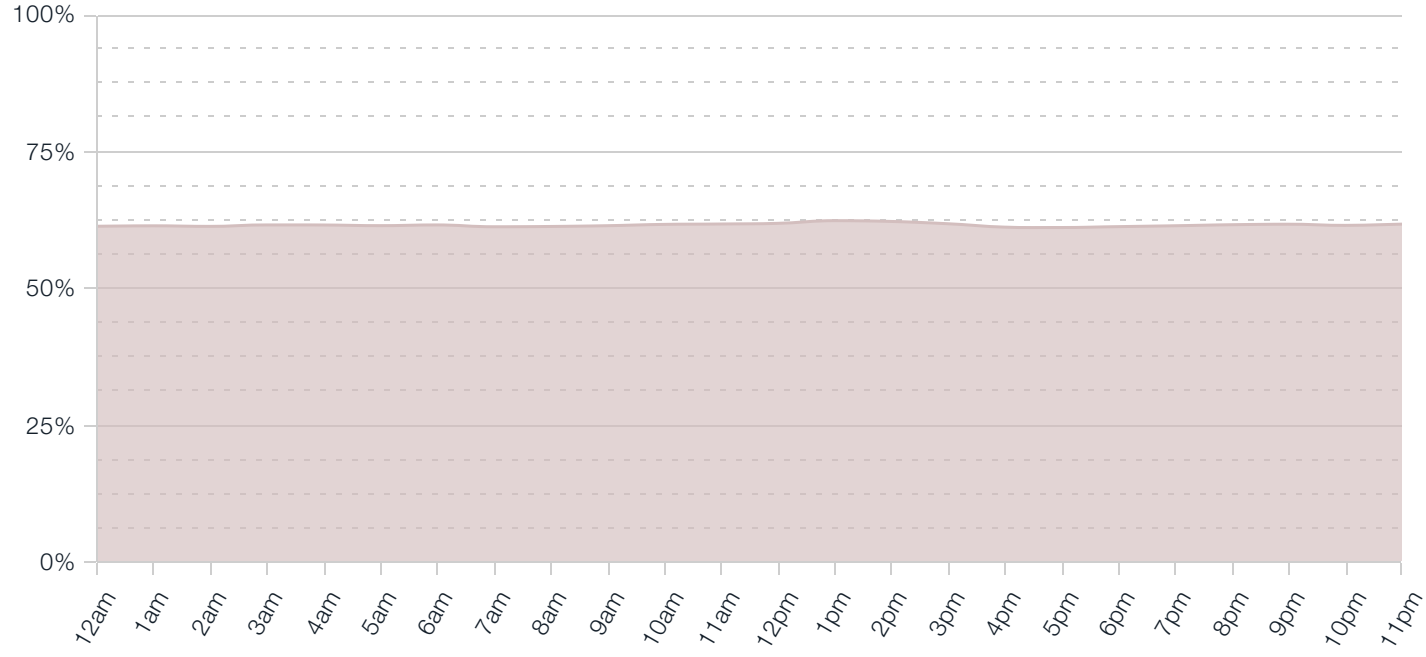
## Durchschnittliche stündliche CPU-Nutzung durch FortiGate

Die Skalierung einer finalen Lösung erfolgt oft anhand der CPU-Nutzung einer FortiGate. Durch die Analyse der stündlich aufgeschlüsselten CPU-Nutzung lässt sich die Leistung von FortiGate-Plattformen im Zielnetzwerk leicht abschätzen. Bei einem höheren Durchsatz werden meist auch mehr Protokolle generiert. Wird eine Auslastung von 75 % oder mehr über einen längeren Zeitraum verzeichnet, sind für die endgültige Implementierung möglicherweise ein neues Modell oder eine überarbeitete Architektur erforderlich.




## Durchschnittliche stündliche Speicherauslastung durch FortiGate

Gleichermaßen bietet die Ermittlung der Speicherauslastung innerhalb eines bestimmten Zeitraum einen Hinweis auf die Nachhaltigkeit eines FortiGate in der Zielnetzwerkumgebung. Die Speicherauslastung kann aufgrund von aktuellen oder ausstehenden Protokollierungsaktivitäten auch bei geringem Durchsatz hoch bleiben.



# Empfehlungen

## 1. Quarantäne von Botnet-Hosts

Aktivität eines Botnet wurde auf mindestens einem Host in Ihrem Netzwerk gefunden. Sie sollten alle Botnet-Hosts sofort unter Quarantäne stellen (z. B. aus dem Netzwerk entfernen) und alle damit verbundenen sicherheitsrelevanten Aktivitäten bzw. Verstöße untersuchen.

## 2. Erweiterung der E-Mail-Sicherheit zum Schutz vor bekannter Malware

Bekannte Malware umgeht derzeit Ihr bestehendes E-Mail-Gateway. Wir empfehlen Ihnen, zu prüfen, ob die Malware-Signaturen auf Ihrem bestehenden E-Mail-Gateway auf dem neuesten Stand sind. Sind die Signaturen aktuell, sollten Sie überlegen, Ihre Sicherheit durch eine sekundäre Firewall zu erhöhen oder Ihre bestehende Gateway-Lösung zu ersetzen.

## 3. Hinzufügen von Sandbox-Technologie zur Erkennung unbekannter Malware

Es wurden Dateien mit verdächtigem Verhalten (potenziell unbekannte Malware) gefunden. Erwägen Sie die Implementierung von Sandbox-Technologie als Ergänzung zu Ihrer Gateway-Sicherheitslösung.

## 4. Verbesserung der Erkennung bösartiger URLs und Schulung

Von Ihrem Unternehmen aus wird auf Websites zugegriffen, die bekannte bösartige URLs enthalten. Es ist möglich, dass diese die Kontrolle über Webfilter umgehen. Wir empfehlen zwei Vorgehensweisen: 1) Stellen Sie sicher, dass Ihre bestehenden Webfilter-Kontrollen aktuelle Blacklists verwenden. 2) Schulen Sie Ihre E-Mail-Benutzer, auf keinen Fall auf unbekannte URLs zu klicken.

## 5. Aufklärung und Schutz von Benutzer in Bezug auf Pishing-Versuchen

Wir haben besuchte URLs gefunden, die versucht haben, sensible Informationen von Ihren internen Benutzern zu extrahieren.Vergewissern Sie sich, dass Sie: 1) Ihre E-Mail-Benutzer darin geschult haben, wie man legitime Absender bestimmt, 2) ein E-Mail-Gateway implementiert haben, das moderne Phishing-Angriffe erkennen und entschärfen kann.

## 6. Auditierung von Hosts mit hohem Angriffsanfälligkeits-Risiko

Einige Hosts in Ihrem Netzwerk weisen ein hohes Maß an verdächtigem Verhalten auf (z. B. durch entstehende Lateral Movement-Angriffe, potenzielle Installation von Malware oder erkannte Botnet-Aktivität). Überprüfen Sie die am stärksten gefährdeten Hosts und isolieren Sie diese Geräte, bis Sie die Ursache für das verdächtige Verhalten ermitteln können.

## 7. Durchsetzung unternehmensinterner Nutzungsrichtlinien für Peer-to-Peer-Anwendungen

Es wurden Peer-to-Peer-Anwendungen in Ihrem Netzwerk erkannt. Einige Unternehmen erlauben P2P-Anwendungen, aber viele sind überrascht zu erfahren, dass ihr Netzwerk an unbefugtem File-Sharing beteiligt ist. Angenommen, Ihr Unternehmen verbietet die P2P-Nutzung. Identifizieren Sie in diesem Fall die ursprünglichen Hosts und nutzen Sie diese Möglichkeit, Ihre Benutzer im Hinblick auf eine ordnungsgemäße Nutzung der Unternehmensressourcen zu schulen.