Kaspersky Network Security Data Feeds

Erweitern Sie Ihre Next-Generation-Firewall (NGFW) um aktuelle Bedrohungsdaten

80,5%
der Befragten nannten Bedrohungsdaten als ihre am häufigsten genutzte Datenquelle.

SANS CTI Survey
2024

Erweitern Sie die Funktionen Ihrer Next-Generation-Firewall um Echtzeit-Bedrohungsdaten von Kaspersky. Unsere Threat Data Feeds helfen Unternehmen, bösartige Aktivitäten noch effizienter zu erkennen und zu blockieren – ganz ohne komplexe Integrationen oder kostspielige Upgrades.

Starke Bedrohungsabwehr

Ermöglicht Sicherheitsteams, die Erkennungsrate mithilfe geprüfter Bedrohungsdaten zu erhöhen.

Echtzeit-Updates und nahtlose Integration

Über einen Link im Einstellungsbereich der Firewall können ganz einfach regelmäßig neue IoC-Listen hochgeladen werden.

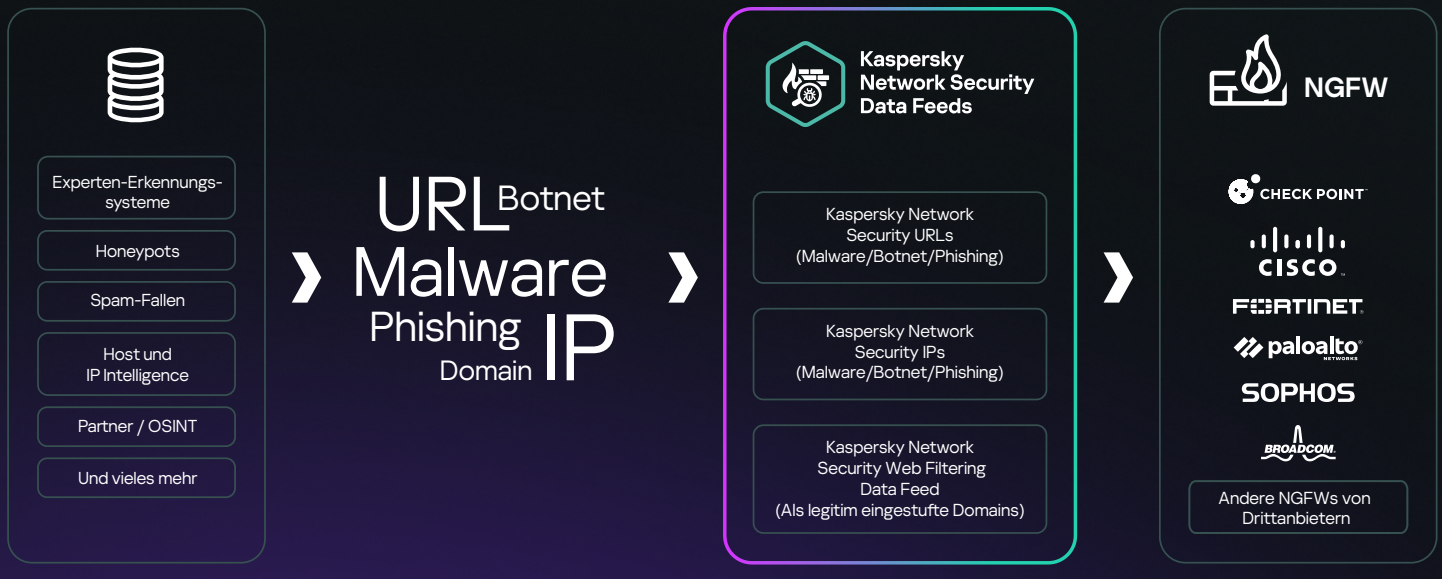
Kaspersky Threat Data Feeds für NGFWs: Erkenntnisse aus der Praxis

Pro Monat werden ein bis drei bösartige Verbindungen erkannt. In Umgebungen mit hohem Risiko können die Werte noch höher ausfallen. Durch die Feed-Anreicherung werden zudem wöchentlich bis zu 30 unerkannte Bedrohungen blockiert.

Die Bereitstellung dauert weniger als 30 Minuten und es ist keine laufende Wartung erforderlich.

Die meisten unserer IoCs sind einzigartig und werden vom NGFW-Anbieter nicht erkannt. Dadurch werden blinde Flecken sichtbar.

Kaspersky Network Security Data Feeds: Integrationsmöglichkeiten



Kaspersky Threat Intelligence entdecken

Kaspersky bietet ein fortschrittliches Threat Intelligence-Portfolio, das taktische, operative und strategische Erkenntnisse umfasst. So bleiben Unternehmen Cyberbedrohungen immer einen Schritt voraus. Integrieren Sie Kaspersky Threat Intelligence und profitieren Sie von proaktivem Schutz.

Mehr erfahren

Kaspersky Network Security Data Feeds können nahtlos in eine Vielzahl von NGFWs integriert werden:

Hersteller	Unterstützte NGFWs
CISCO	Alle NFGWs, die auf dem Cisco Firepower Management Center 6.2.3 und höher laufen und über das Threat Intelligence Director-Modul verfügen
FORTINET	Alle FortiGate NGFWs mit FortiOS 6.0 und höher: • FG-30G, FG-40F, FG-50G, FG-60F, FG-70F, FG-70G, FG-80F, FG-90G • FG-100F, FG-120G, FG-200F, FG-200G, FG-400F, FG-600F, FG-900G • FG-1000F, FG-1800F, FG-2600F, FG-3000F, FG-3200F, FG-3500F, FG-3700F, FG-4200F, FG-4400F, FG-4800F, FG-6300F, FG-6001F, FG-6500F, FG-7081F, FG-7121F
paloalto NETWORKS	• PA-220, VM-50, VM-50 (Lite), VM 100, VM-1000-HV • Serie PA-850, PA-820, PA-3200 • Serie PA-5200, PA-7000
CHECK POINT	Alle Check Point Firewalls mit Gaia OS Version R81. 20 Titan und höher
SOPHOS	Alle Sophos-Firewalls mit SFOS v21 und höher
BROADCOM	Edge SWG (ProxySG) SG-Enterprise c SGOS 7.4 SWG Edition und höher

Mehr erfahren

Warum Kaspersky Threat Data Feeds?

Weltweite Abdeckung

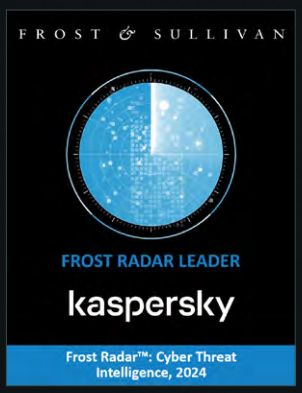
Unsere Infrastruktur umfasst mehr als 100 Millionen Sensoren in 200 Ländern und Regionen. Wir verfügen über die größten Datenbestände, die von unserer KI und unseren Experten analysiert werden, um rundum zuverlässige Threat Intelligence zu liefern.

Einzigartige Einblicke und globale Reichweite

Unsere Abdeckung umfasst Regionen mit hohem Risiko, einschließlich wichtiger staatlicher Einrichtungen und kritischer Infrastrukturen. So ermöglichen wir einen tieferen Kontext sowie noch umfassenderen Schutz.

Bewährt und vertrauenswürdig

Kaspersky Threat Intelligence wird regelmäßig von führenden Branchenanalysten ausgezeichnet.



Von Kunden geschätzt

Organisationen aller Größen und Branchen weltweit vertrauen auf unsere Threat Intelligence.

Die Lösungen von Kaspersky haben unser Netzwerk- und Cybersicherheitsprofil signifikant verbessert. Den Schutz unserer komplexen Abläufe legen wir guten Gewissens in die Hände von Kaspersky.

Patrick de Haan
IT Manager, Condor Carpets

Kaspersky Network Security Data Feeds

Jetzt testen