PROTECTION MADE SIMPLE

NETWORK BOX

Next Generation Managed
IT Security

WIR SCHÜTZEN NETZWERKE WELTWEIT

Sicherer Mittelstand mit Managed Services von Network Box

Als Herz, Motor oder Rückgrat der hiesigen Wirtschaft gilt der deutsche Mittelstand – trotz Widrigkeiten wie teils zu wenig Personal und knappen (Zeit-)Budgets. Damit die IT-Sicherheit dabei nicht zu kurz kommt, bietet das Kölner Unternehmen Network Box Managed Security Services an: buchbare IT-Sicherheitslösungen, die die IT-Profis betreuen. Dieses Konzept ist auch aus finanzieller Perspektive interessant, denn es entfallen u.a. Anschaffungs- und Lizenzkosten sowie Verwaltungsaufwand. Einfach nutzen statt intensiv studieren!

Network Box Deutschland GmbH stellt umfassende und gemanagte IT-Sicherheitslösungen am Gateway bereit, die mit skalierbaren und modularen Systemen ein Höchstmaß an Sicherheit gewährleisten. Zudem verantwortet das Team Konfiguration, Wartung, Patches und Updates.

In unserem weltweiten Netz von Security Operation Centern schützen wir mehr als 1.700 Unternehmen und Organisationen. An 365 Tagen im Jahr und rund um die Uhr verfolgen unsere Mitarbeiter in den USA, Deutschland, Großbritannien, Asien, Australien und im Nahen Osten die Entwicklung neuer Bedrohungen aus dem Internet.

Buchbare Services sind u.a. Firewalls, VPN, Intrusion Detection/Intrusion Prevention, Application Control, Anti-Malware, E-Mail Protection, Data Leakage Prevention, Anti-DDoS, Realtime Monitoring sowie Reporting. Dabei bringt die patentierte PUSH-Technologie alle Sicherheits-Features vollautomatisch auf den neuesten Stand. Speziell für KMU sind Managed Security Services auf Basis der Network Box-eigenen Hard- und Software erhältlich.

Profitieren Sie von unserer langjährigen Erfahrung, und stellen Sie sich ein individuell auf Ihr Unternehmen zugeschnittenes Sicherheitssystem zusammen. Wir beraten Sie gerne bei der Auswahl der Module.

IT LOOKS LIKE A PRODUCT *- IT'S REALLY A SERVICE*

In 16 Security Operation Centern weltweit betreuen hochqualifizierte Experten die Netzwerke unserer Kunden.

IT Security managed in Germany!

Der professionelle und effektive Netzwerkschutz auch für Kleinunternehmen und den deutschen Mittelstand – eine sichere Lösung aus einer Hand.

Entlastung der Finanzen – Fokussierung auf das Kerngeschäft

	Managed Service	Inhouse IT-Security
Dienst	gehostet	lokal
Change Control	durch IT-Security-Experten in einer ISO-zertifizierten Umgebung	limitiert durch fehlendes Fachwissen und Zeit
Service Level	individuell zugeschnitten	limitiert durch fehlendes Fachwissen und Zeit
Security Level	individuell zugeschnitten	abhängig von Produkt und Know-how des Mitarbeiters
Zeit	Wartung und Betrieb durch MSSP	bindet die IT-Abteilung zeitintensiv ein
Updates	automatisierte Updates von einer Instanz	separate Updates der unterschiedlichen Systeme
Management	eine Konsole für alles	mehrere Konsolen
IT-Security Know-How	kontinuierliche und konstante Weiterbildung	reaktiv

Managed IT Security Services sind die ideale Lösung für die individuellen Sicherheitsansprüche kleiner und mittelständischer Unternehmen. Unsere standardisierten, sicheren und skalierbaren Dienste sind technisch immer up-to-date und leicht in Ihre vorhandene IT-Umgebung zu integrieren. Durch den ausgelagerten Verwaltungsaufwand sind sie zudem erheblich günstiger als qualitativ vergleichbare Lösungen im Eigenmanagement.

Unsere datenschutz- und rechtskonformen Dienste wachsen mit Ihrem Unternehmen und sind schnell bereitgestellt. Dadurch wird Ihre IT-Abteilung entlastet und kann wieder produktiv zu Ihrem Unternehmenserfolg beitragen.

Die Vorteile unserer Services:

- **Kontinuierlicher Schutz gegen neueste Angriffsmethoden und -technologien**
- **Überschaubare und vorab kalkulierbare Kosten**
- **Produktivitätssteigerung Ihrer IT-Abteilung durch Fokussierung auf Ihr Kerngeschäft**

Realtime Monitoring · Angriffs-analyse · Bandbreiten Management · Business Continuity · Change Control · Load Balancing · Security Consulting

5 GRÜNDE FÜR MANAGED IT SECURITY VON NETWORK BOX

Sichere Basis für Ihre Unternehmens-abläufe

Ein permanent von Experten gemanagtes System garantiert die Geschäftskontinuität.

01

Integrierte Lösung

Network Box bietet eine gesamtheitliche Lösung für den heutigen Herausforderungen in der IT-Sicherheit.

02

Zugang zu IT-Experten

IT-Sicherheitsexperten sind teuer und schwer zu finden. Network Box bietet das Know-how und permanent erreichbare Ansprechpartner.

03

Langfristiger Lösungsbedarf

Statische Systeme haben ausgedient. Auf dynamische Angriffsformen antwortet Network Box mit dynamischen Sicherheitssystemen.

04

Real-Time Protection

Nahezu in Echtzeit aktualisiert Network Box alle Systeme über die patentierte PUSH-Technologie.

05

DAS ULTIMATIVE SICHERHEITSPAKET

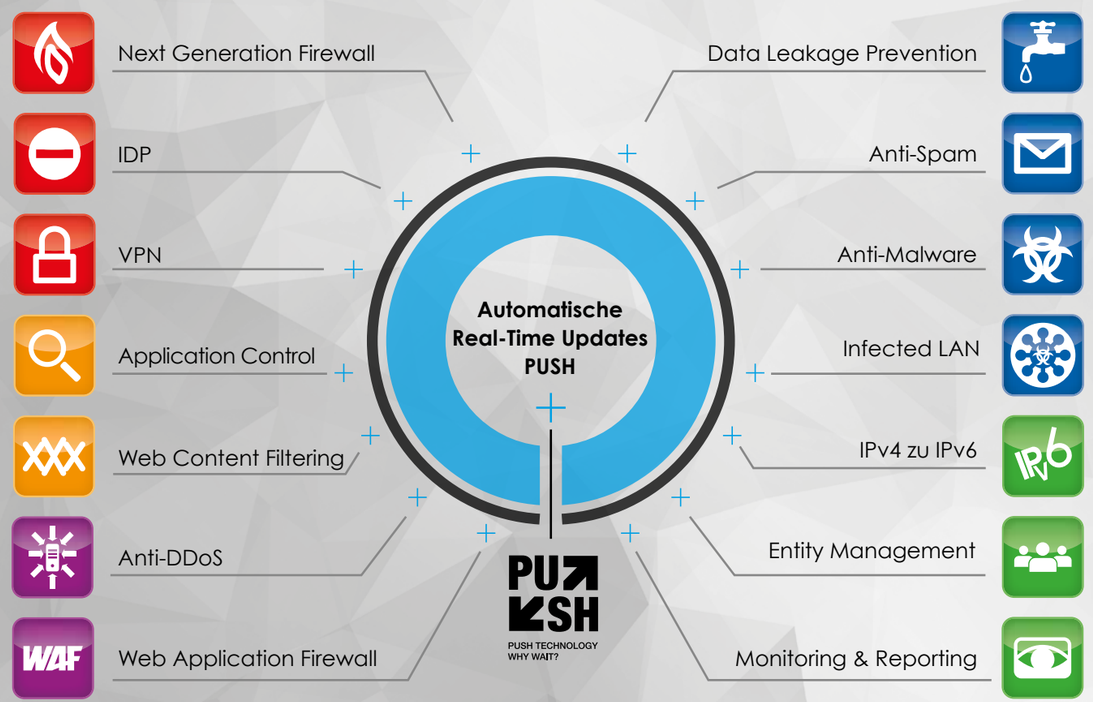
Wirkungsvolle IT-Sicherheit muss von Experten konzipiert, konfiguriert und überwacht werden. Network Box bietet eine breite Palette verschiedener Hardware-Modelle für unterschiedliche Netzwerktypen und -größen. Dabei können alle Sicherheitsfunktionen modular implementiert werden und sorgen so für ein Maximum an maßgeschneiderter IT-Sicherheit.

Schützen Sie Ihre Netzwerke mit unseren umfassenden Sicherheitslösungen und stellen Sie Ihr Level an Security so ein, wie Sie es brauchen.

Wir beraten Sie gerne bei der Auswahl der richtigen Sicherheitsmodule.

Network Box Hardware dient als Plattform für alle Security Appliances.

STATE-OF-THE-ART TECHNOLOGIEN



NETZWERKSICHERHEIT AUF HÖCHSTEM NIVEAU

AUTOMATISCHE ECHTZEIT-UPDATES

PUSH-Technologie

- Updates werden in durchschnittlich 45 Sekunden durchgeführt
- Vollautomatisierter Prozess ohne Aufwand seitens des Users
- Momentan werden täglich 22.481* Updates zur Verfügung gestellt

Topaktueller Schutz in durchschnittlich weniger als 45 Sekunden

Herkömmliche Sicherheitssysteme rufen gewöhnlich einmal am Tag oder bestenfalls einmal pro Stunde Aktualisierungen von einem Server ab. Network Box hingegen stellt durch die PUSH-Technologie alle Aktualisierungen zu, sobald sie verfügbar werden.

Microsoft®

Microsoft Active Protections Program (MAPP)

Als Partner des Microsoft Active Protections Program (MAPP) hat Network Box frühzeitig Zugang zu Informationen über Sicherheitslücken von Microsoft. So ist Ihr Netzwerk proaktiv geschützt.

Patentierte PUSH-Technologie - automatisierte Updates in Echtzeit

	PUSH	Pull
Update Benachrichtigung	Automatisiert und daher nicht notwendig	Zum terminierten Zeitpunkt wird beim Server nach Updates gefragt
Update Access	Vom Network Box SOC gesteuert	Zugang zum Update Dienst muss gewährleistet sein
Downloads	Läuft automatisch im Hintergrund	Müssen manuell oder teilautomatisiert vom User durchgeführt werden
Zeit	Kein Zeitaufwand für den User	Überwachung durch User notwendig
Installation	Automatisiert und bedarf keiner User-Interaktion	Ist manuell für alle Appliances durchzuführen

Network Box ist der einzige Security Service Provider, der Real-Time PUSH-Updates anbietet. Aktuell sind dies durchschnittlich 22.481* Updates am Tag.

* durchschnittlich im November 2014

DIE BASICS DER IT-SECURITY

Firewall

- Packet Filtering
- Stateful Packet Inspection
- Proxy

State-of-the-Art Firewall

Die Hybrid-Firewall schützt Server und Arbeitsplatzrechner auf einer tiefen Netzwerkebene (Layer 3, Network) vor einer Vielfalt an Angriffen, wie Protokollanomalien, Connection-Flooding, SYN-Flooding, Denial-of-Service und Packet-Fragmentation-Techniken.

Intrusion Detection/ Prevention

- 3 Engines
- Heuristische Erkennung
- Mehr als 16.000 Signaturen

IDS und IPS zur Erkennung und Abwehr

Das in die Firewall integrierte IDP System scannt den Datenverkehr auf Anwendungsebene (Layer 7, Application). Dabei erkennt das Detection-Modul anhand der vorhanden Signaturen Angriffsmuster.

Das Prevention-Modul wird „inline" mit der Firewall verwendet und kann so im Erkennungsfall den Netzverkehr ohne Verzögerung blockieren.

VPN

Verschlüsselung

- IPSec
- SSL
- PPTP

Sichere Anbindung von Außenstellen

Mittels geschützter VPN-Tunnel werden Verbindungen von außerhalb des Büros mit speziellen Zugriffsbeschränkungsregeln für Gruppen und für individuelle Benutzer gesichert. Die authentifizierten Verbindungen stellen sicher, dass Daten während der Internetübertragung von außerhalb des Firmennetzwerkes vertraulich bleiben. Die meisten großen VPN-Clients (wie z.B. Microsoft, Cisco, Checkpoint und Symantec) können mit Network Box verbunden werden.

POLICY CONTROL AUF HÖCHSTEM NIVEAU

Content Filter

- S-Scan Engine
- Signatur gestützt
- 56 vorgefertigte Kategorien

Web-Inhalte kontrollieren

Die S-Scan Engine erlaubt es, Internetseiten zu kategorisieren. So können unerwünschte Webinhalte zuverlässig erkannt und blockiert werden. Mit einer Kategoriesierungsrate von 98,7 % der 100.000 weltweit meistbesuchten Webseiten (Alexa100k) bietet das System eine ausgezeichnete Treffsicherheit.

Dabei bedient sich die Engine sowohl einer URL-Datenbank, als auch einer leistungsstarken signaturgestützen Technologie.

Vorgefertigte Kategorien

Anhand vorgefertigter Kategorien besteht die Möglichkeit, zu kontrollieren, auf welche Webinhalte Benutzer Zugriff haben. Diese Kategorien umfassen zum Beispiel: soziale Netzwerke, Online-Spiele, Shopping-Portale, etc.

Datensatz	URLs	S-Scan *Extended*
Alexa100k	100.000	**98,7%**
NBCustDom	270	**93,0%**

Application Control

- 1.200 Anwendungen
- 15 Kategorien
- 20 Tags
- SSL Support

Unternehmens-Policies effektiv durchsetzen

Die Application Control Engine untersucht den Web-Traffic und identifiziert mehr als 1.200 verschiedene Anwendungen. So können Unternehmens-Policies einfach über Regeln umgesetzt werden.

Während eine traditionelle Firewall Protokolle und Ports blocken kann, erkennt die Application Control Engine direkt individuelle Anwendungen und kann entsprechende Policies umsetzen. Dabei kann der Datenverkehr auch zu Reporting-zwecken markiert werden. Die Application Control Engine ist in den SSL-Proxy integriert und kann so auch Traffic verschlüsselter SSL-Sessions identifizieren und kontrollieren.

15 Kategorien		
Dateiübertragung	Messaging	Unbekannt
Datenbanken	Netzwerk Monitoring	Vernetzung
E-Mail	Proxy	VPN
Fernzugriff	Soziale Netzwerke	Web-Dienste
Media Streaming	Spiele	Zusammenarbeit

20 Tags		
Bildschirmfreigabe	Internet-Suche	Proxy
Chat-Programme	Kommunikations-Logs	Stealth (Verdeckung)
Data-Leakage	Malware	Telefonkonferenz
Exzessive Bandbreite	Medienfreigabe	Verschlüsselung
Facebook-Apps	Missbrauch von Apps	Videokonferenz
Fernzugriff	Mobile Applikationen	Werbung
Informations-Logging	Peer-2-Peer	-

MALWARE PROTECTION

Anti-Malware

- 15 + 1 Engines
- 10 Millionen Signaturen
- Zero Day Protection

Z-Scan: Schnellstmöglicher Schutz vor neuen Bedrohungen

Der Zero-Day-Malware-Schutz wurde eigens von Network Box entwickelt und gehört zur neuesten Technologie zum Erkennen bisher unbekannter Internet-Gefahren. 250.000 virtuelle Fallen warten im Internet darauf, von neuer Malware angegriffen zu werden. Erkennt das System einen solchen Angriff, wird dieser sofort analysiert und eine Signatur mit entsprechenden Gegenmaßnahmen in Echtzeit per PUSH-Technologie allen Clients zur Verfügung gestellt. Diese Signaturen bieten eine erste Abwehr, bis verfeinerte Lösungen auf die herkömmliche Art und Weise getestet, geprüft und bereitgestellt werden können.

M-Scan: 15 Engines in Echtzeit auf dem neusten Stand durch PUSH

Die M-Scan-Technologie ist ein mehrschichtiges System. Es greift auf 15 Engines, darunter auch Kaspersky, zurück. Durch die patentierte PUSH-Technologie von Network Box werden alle Updates automatisch und in Echtzeit an die angeschlossenen Clients verteilt.

KASPERSKY lab

Zwei Technologien - ein Ziel: Sicherheit

ZSCAN MSCAN

Gateway-Schutz: umfassende Protokollüberwachung

Die Network Box analysiert fortwährend und transparent ein- und ausgehende Daten auf Anzeichen einer möglichen Infektion. Im Fall der Fälle blockiert sie Malware direkt am Gateway. Zu den überwachten Protokollen gehören HTTP, FTP, SMTP, POP3 und IMAP4. Dabei werden mehr als 670 verschiedene Kompressions- und Encoding-Formate unterstützt. Um neue und unbekannte Bedrohungen bereits im Vorfeld zu erkennen, greift das System darüber hinaus auf Mittel der kryptoanalytischen und statistischen Analyse zurück.

Die Leistungen im Überblick:

› Erkennung von Viren, Würmern, Spyware, Trojanern und anderer Malware
› Gefahrenerkennung über HTTP, FTP, SMTP, POP3 und IMAP4
› Schutz eingehender und ausgehender E-Mails
› Unterstützung komprimierter Datei-Anhänge, um versteckte Gefahren zu erkennen
› Anti-Viren-Engines blocken nicht-kategorisierte Viren, bevor es finale Signaturen gibt

	Z-Scan	M-Scan	Klassische AV
Engines	**1**	**15**	1
Signaturen insgesamt	**250.000+**	**10.000.000+**	3.500 - 5.500.000
Malware-Erfassung	**Real-Time**	**Real-Time**	Batch Processing
Update-Technologie	**PUSH**	**PUSH**	PULL
Signatur-Erstellung	**1 - 30 Sek.**	**10 - 120 Min.**	3 - 12 Std.
Signatur-Freigabe	**2 - 3 Sek.**	**30 - 45 Sek.**	stündl./ tägl.
Reaktionszeit	**3 Sek.**	**10,5 Min.**	3,5 Std.

E-MAIL PROTECTION

Data Leakage Prevention

- Individuelle Regeln und Policies
- Komplexes Pattern Matching
- Inhalts-Analyse
- Heuristiken
- Boolsche und arithmetische Logiken
- Optische Bilderkennung

Interna müssen Interna bleiben

Das DLP-System von Network Box nutzt eine komplexe Regel-Engine, um ausgehenden SMTP-Verkehr zu scannen und zu blocken. Dabei werden sensible Daten, wie etwa Kundeninformationen, Patientenakten, Kreditkartennummern oder Bankinformationen erkannt und davor geschützt, nach außen kommuniziert zu werden.

Die entsprechenden Regeln können individuell aufgestellt werden und führen zu einer optimalen und maßgeschneiderten Umsetzung von Unternehmens-Policies.

Anti-Spam

- 25 Engines
- 30 Millionen Signaturen
- 97,99 % Erkennung

Effektive Spam-Filterung am Gateway

Das Network Box Anti-Spam-System ist eine umfassende und effektive Art, ungewollte Spam-Nachrichten am Gateway zu blockieren. Mit 25 Anti-Spam-Engines kombiniert es unterschiedliche Techniken zur Abwehr und umfasst in Gänze 30 Millionen Signaturen. Dabei liegt die Erkennungsrate bei extrem hohen 97,99 %.

Spam-Erkennung durch:
› Signaturen und Spam Scoring
› individuelles White-Listing und Black-Listing
› Real-Time IP- und URL-Black-Listing
› URL-to-IP-Mapping und Black-Listing
› URL-Kategorisierung / Domain Age
› Challenge / Response Systeme

NETWORK ANALYSIS

Infected LAN

- Erkennung von auffälligem Datenverkehr im Netzwerk
- Eindeutige Identifikation der Quelle (IP)
- Trennung der Quelle vom Internet

Netzwerkeindringlinge in Minuten erkennen

Durchschnittlich 229 Tage bleibt eine Netzwerkkompromittierung unentdeckt – viel Zeit für Cyberkriminelle, um Daten auszuspähen und zu stehlen.
Network Box beschleunigen den Erkennungsprozess deutlich mit der Lösung „Infected LAN". Innerhalb von Minuten kommen unsere Experten auffälligem Traffic auf die Spur, der meist ein Indiz für ein aktives Schadprogramm ist, z.B. einen Trojaner. Nach der Identifizierung wird die Quelle isoliert, was verhindert, dass sich das Schadprogramm weiter ausbreitet bzw. unentdeckt Informationen nach außen kommuniziert.

BUSINESS CONTINUITY

Anti-DDoS

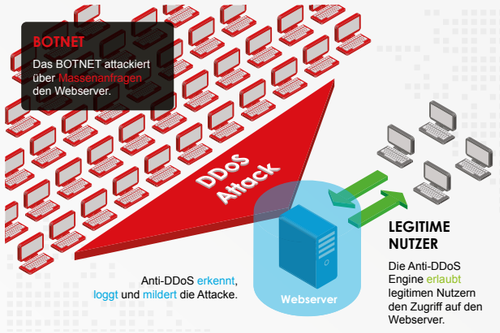
- Wahrung der Geschäftskontinuität
- Vielfältige Möglichkeiten zur Limitierung der Zugriffe

DDoS-Angriffe entschärfen - Geschäftskontinuität sichern

Bösartiger Datenverkehr wird ferngehalten und regulärer Datenverkehr z.B. zum gesicherten Webserver durchgelassen. Auf diese Weise wird die Geschäftskontinuität während laufender Angriffe geschützt und aufrechterhalten.

Die Anti-DDoS-Engines bieten folgende DoS – DDoS-Optionen:

› Begrenzung der Anzahl gleichzeitiger Verbindungen
› Begrenzung der Verbindungsrate (Anzahl an Verbindungen/Sekunde)
› Begrenzung der Anzahl gleichzeitiger Verbindungen pro Quelle
› Begrenzung der Verbindungsrate pro Quelle (Anzahl an Verbindungen/Sekunde)



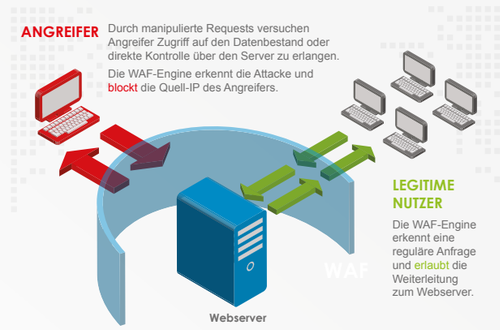
Web Application Firewall

- OWASP TOP 10
- 6.000 Regeln
- Anti-Malware-Engine
- IP-Signaturdatenbank

Schutz für exponierte (Web-)Server

Die Web Application Firewall schützt Webserver gegen eine Vielzahl von Attacken. Durch eine Kombination spezieller Heuristiken mit Anti-Malware- und IP-Signatur-Datenbanken schützt unsere WAF-Engine Ihre Webserver gegen Exploits wie SQL-Injection, Cross-Site-Scripting oder Insufficient-Input-Validation. Mit bis zu 15.000 analysierten Transaktionen pro Sekunde werden mehrere Millionen komplexe Angriffsszenarien erkannt und können neutralisiert werden. Zusätzlich erlaubt die WAF-Engine verschiedene Optionen, um den Datenstrom der Server zu loggen und im Angriffsfall zu blocken.

Die WAF wird mittels unserer PUSH-Technologie permanent auf dem neusten Stand gehalten. Dadurch ist jederzeit die unmittelbare Reaktionsmöglichkeit auf neue Bedrohungen gewährleistet.



FÜR DIE ZUKUNFT GERÜSTET - ÜBERBLICK BEWAHREN

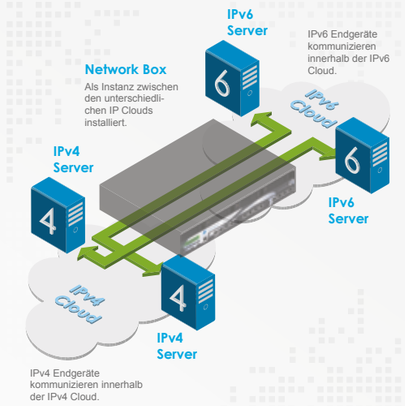
IPv4 zu IPv6

- Zukunftssicher durch Kompatibilität
- Flexibel

Für die Zukunft gerüstet

Network Box kann als Schnittstelle zwischen IPv4 und IPv6 fungieren. Jeder geschützte Webserver, der entweder über eine IPv4- oder IPv6-Verbindung verbunden ist, ist dadurch mit beiden IP-Protokollen kompatibel.

Die Network Box erkennt sowohl das IPv4- als auch das IPv6-Protokoll und agiert als Bridge zwischen den beiden unterschiedlichen IP Clouds. So können Endgeräte aus dem einen Bereich auf Dienste und Ressourcen im anderen Bereich zugreifen.



Monitoring und Reporting

- Real-Time Monitoring
- Dashboard
- Flexible Reports

Echtzeit-Monitoring am PC, auf dem Tablet oder unterwegs vom Smartphone

Das auf HTML 5 basierende Network Box „Dashboard“ ist ein übersichtliches und hoch flexibles Monitoring- und Reporting-Tool. Es bietet Administratoren die Möglichkeit, systemweite Informationen und Benutzern ihre individuellen Statistiken abzufragen. Darüber hinaus ist es möglich, Report-Zeitpläne zu erstellen. Dabei ist nicht nur die Häufigkeit der Reports flexibel gestaltbar, sondern auch der Inhalt jedes einzelnen Reports.

Echtzeit- und mobiles Monitoring

Das Monitoring und Reporting Tool ist mit beinahe allen bekannten mobilen Endgeräten kompatibel. So kann sich der IT-Administrator wieder auf seine Kernaufgaben konzentrieren, ohne den Überblick über die Sicherheitslage zu verlieren - sogar wenn er seinen Arbeitplatz verlässt.

Kompakte Informationen - hochflexibel

Lassen Sie sich sicherheits- und systemrelevante Informationen automatisch als .pdf oder .csv zustellen.

Entity Management

- Endgeräte werden zu einer Entity zusammengefasst
- Zusammengefasstes Monitoring der Netzwerkaktivitäten

Effektives Monitoring aller Endgeräte in zusammengefassten Entities

Das Entity Management System von Network Box hat neu definiert, wie User-Endgeräte verwaltet, überwacht und geschützt werden.

Geräte wie iPads, iPhones, Laptops, Desktop PCs und VOIP-Telefone werden zu einer Entity zusammengeführt. Das System ordnet verschiedene Attribute wie MAC-, IP- und E-Mail-Adressen zu und kann so darstellen, welche Netzwerk-Ressourcen genutzt werden.
Das System pflegt diese Zuordnung automatisch und vereinfacht so den Alltag eines IT-Leiters.

Es präsentiert dem Betrachter eine Gesamtansicht aller Netzwerkaktivitäten jeder einzelnen Entity.

Betrachtet man einen beliebigen User, wird angezeigt, welche Firewall-Blocks, Internet-Aktivitäten, Email-verkehr, etc. dieser User mit all seinen Endgeräten verursacht hat.

Schon gewusst?
In wirtschaftsstarken Ländern besitzt jeder durchschnittlich 2,9 mobile Internetgeräte. Bis 2017 soll sich diese Zahl verdoppeln.*

* Naked Security Survey 2013

VIRTUELLE LÖSUNGEN

Alle Security Module laufen nativ auf unserer Hardware, sind aber auch als virtuelle Appliances für zum Beispiel Cloud-Anwendungen nutzbar. Die virtuelle Variante beinhaltet prinzipiell den gleichen Funktionsumfang wie die Hardware-basierte Variante. Sie wird den Kundenwünschen entsprechend individuell konfiguriert und bereitgestellt.

PRODUKT-MATRIX

Sicherheitslösungen	FW+	AV+	CF+	UTM+	WAF+	EMP+	WBP+	FWAF	UTMW
PUSH-Updates	●	●	●	●	●	●	●	●	●
Network Monitoring und Reporting	●	●	●	●	●	●	●	●	●
Next Generation Firewall	●	●	●	●		●	●	●	●
Intrusion Detection and Prevention (IDP)	●	●	●	●		●	●	●	●
Virtual Private Network (VPN)	●	●	●	●		●	●	●	●
Infected LAN	●	●	●	●		●	●	●	●
Anti-Malware (E-Mail)		●		●		●			●
Anti-Malware (Web)		●		●			●		●
Anti-Spam		●		●		●			●
Content Filtering			●	●			●		●
Application Scanning	●	●	●	●		●	●	●	●
Entity Management	●	●	●	●	●	●	●	●	●
Data Leakage Protection (DLP)				●					●
Anti-DDoS	●	●	●	●	●	●	●	●	●
Web Application Firewall (WAF)					●			●	●
IPv4 zu IPv6 Bridging	●	●	●	●	●	●	●	●	●

Zertifizierung

Weitere Informationen:
www.network-box.eu

Network Box Deutschland GmbH
Ettore-Bugatti-Straße 6-14
51149 Köln
Tel.: +49 (0) 22 03 20 20 78 - 0

NETWORK BOX

NEXT
GENERATION
MANAGED SECURITY