Com² Med
PARTNER FÜR MEDIZIN + TECHNIK

Securepoint NextGen UTM-Firewalls

Zum kompletten Schutz Ihrer Netzwerk-Infrastruktur

Sicheres Netzwerk.

Bester Hersteller. Beste Produkte.

ChannelPartner 2021 CONTEXT
CHANNEL EXCELLENCE AWARD
Security

techconsult PUR 2021
CHAMPION
VIRTUAL PRIVATE NETWORK
SECURITY SOLUTIONS

SecurITy made in Germany

Sicheres Surfen

Durch den High-End Content-Filter mit Zero-Hour-Protection werden Zugriffsbeschränkungen durchgesetzt. Die Analyse verschlüsselten Traffics (SSL) erfolgt mit nur einem Klick.

Sicheres Netzwerk

Mit dem Threat Intelligence Feed und weiteren effizienten Angriffserkennungen schützt die UTM-Firewall Netzwerke von Unternehmen vor Spionage, Ransomware und Cyber-Angriffen.

Sichere Konnektivität

Über verschlüsselte VPN-Verbindungen lassen sich beliebig viele Standorte vernetzen. Mobile Arbeitsplätze werden so hochsicher in das Unternehmensnetzwerk eingebunden.

Sichere Kommunikation

Kommunikationskanäle wie E-Mail, werden durch Analyse, Überwachung und Bereinigung vor Viren, Phishing, Spy- und Malware geschützt.

Securepoint NextGen UTM-Firewall

Securepoint Cyber Defence Cloud

Über das Internet verbreiten sich digitale Bedrohungen durch Schadsoftware oder Malware rasend schnell. Die Zeit zwischen dem Auftreten neuer Gefahren und ihres Eintreffens beim einzelnen Benutzer wird immer kleiner. Klassische Verfahren bieten dafür oft keine Lösungen.

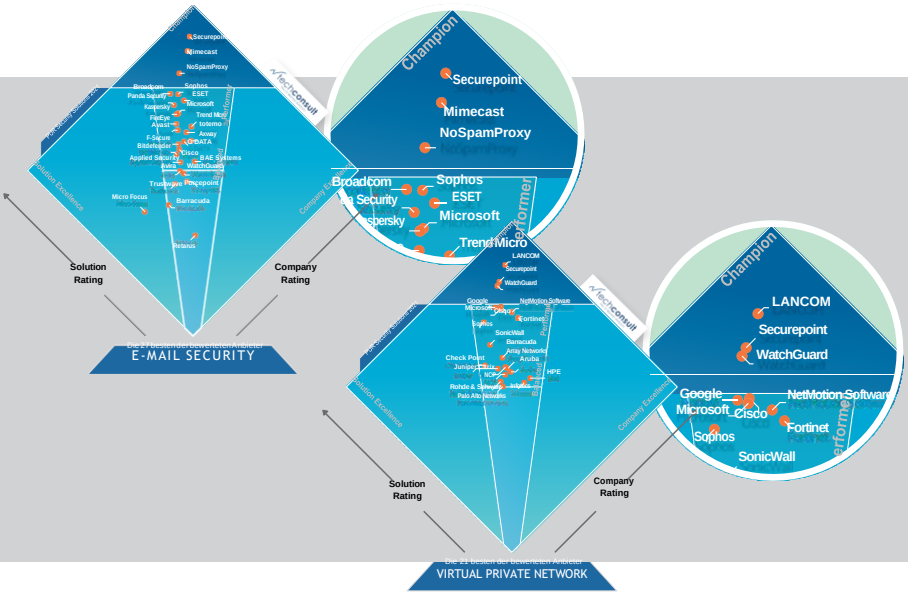
Als Antwort auf diese Herausforderungen verfügt die Securepoint NextGen UTM-Firewall über eine zentrale Technologie: die Cyber Defence Cloud. Statt mit herkömmlichen Update-Zyklen zu arbeiten, liefert sie Daten in Echtzeit. Durch Machine Learning, Schwarm-intelligenz, Data-Mining, leistungsstarke Protokolle und das Know-how unseres Analyseteams verbinden wir die Erkenntnisse aus technischen Innovationen sowie von Menschen.

Sicheres Surfen

Der Content-Filter ist als wichtiges Sicherheitsfeature Teil der Cyber Defence Cloud. Er überzeugt mit hoher Genauigkeit, Schnelligkeit und geringem Ressourcen-verbrauch. Der Threat Intelligence Feed ist die wichtigste Kategorie der Cyber Defence Cloud. IPs und URLs werden auf Spare-/Phishing, Ransomware, Malware- bzw. Makro-Download und andere Gefahren geprüft. Unser Content-Filter macht die Analyse von SSL-verschlüsseltem Traffic einfach – mit nur einem Klick. Die hohe Qualität und die komplexen Analysemöglichkeiten machen den Content-Filter im deutschsprachigen Raum unschlagbar.

„techconsult PUR 2021“

Im Rahmen der unabhängigen Studie „Professional User Rating Security Solutions 2021“ (PUR-S) wurde Securepoint als Champion in den Kategorien „E-Mail Security“ und „Virtual Private Network“ ausge-zeichnet. Für die Studie des Analystenhauses techconsult wurden zum fünften Mal mehr als 2.000 Anwender zu IT-Sicherheitsherstellern und ihren Lösungen befragt.



UTM-Firewall Funktionsumfang

Sichere E-Mails

Wir heben die Mail-Security auf ein neues Level: mit Quarantäne gefährlicher E-Mails direkt auf der NextGen UTM-Firewall und einem selbstentwickelten Zeitschloss für verdächtige Nachrichten. Nach definierter Zeit werden die E-Mails erneut geprüft und erst zugestellt, wenn kein Sicherheitsrisiko besteht. Moderne Verfahren wie DKIM und SPF sorgen für zusätzliche Sicherheit. Das Scannen von 25 Milliarden E-Mails in der Cyber Defence Cloud pro Tag macht das möglich.

Das Ergebnis: 99,9% weniger Spam/Viren und eine maximal reduzierte Fehlerquote bei der Erkennung.

Sichere Verbindungen

Durch VPN-fähige UTM-Gateways lassen sich beliebig viele Standorte sicher vernetzen. Der kostenlos beiliegende Securepoint SSL VPN Client ermöglicht mobilen Mitarbeitern einen verschlüsselten VPN-Zugang zum Unternehmensnetzwerk sowie sichere Internetnutzung. Dem einzelnen Benutzer lassen sich dynamisch anpassbare Regelwerke zuweisen. Für die Anzahl von Verbindungen gibt es keine Beschränkung oder Lizenzierung.

VPN-Clients für iOS und Android stehen ebenfalls kostenlos zur Verfügung.

Sicheres Netzwerk.

- Eingebettet in das Securepoint Unified Security-Konzept
- EU DS-GVO ready: Garantiert ohne Backdoors
- Vollständiger Support von IPv6
- Automatische Optimierung der Bandbreite
- Echtzeitschutz durch Cyber Defence Cloud
- Threat Intelligence Feed
- Sofortige und einfache Absicherung verschlüsselter Verbindungen (TLS)
- Zeitschloss für verdächtige E-Mails
- Sichere Voreinstellungen
- Zentrale Verwaltung (SOC) aller Firewalls bei Kunden oder über Standorte hinweg (inkl. Cloud)
- Alerting-Center übersetzt Log-Informationen in einfach verständliche Meldungen und informiert aktiv per E-Mail
- Optimal für Managed-Service-Anbieter
- Überwachung mit SNMP: Volle Integration in MSP-Umgebungen dank umfassender Schnittstellen
- Integriertes Einmalpasswortsystem für VPN, Benutzerinterface und Administration (Mehrfaktor-Authentifizierung – OTP)
- Inkl. Mail-Connector zur Abholung von E-Mails beim Provider
- Einfach zu bedienende, App-orientierte Adminoberfläche
- Mit nur ca. 70 MB ein sehr kompaktes Firewall-Image
- Unterstützt die virtuellen Umgebungen VMWare®, Microsoft Hyper-V® und KVM
- Regelmäßige Penetrationtests

Den gesamten Funktionsumfang finden Sie hier:
www.securepoint.de/utm-funktionen

Leistungen rund um die NextGen UTM-Firewalls

Hardwarevergleich – NextGen UTM-Firewalls

	Black Dwarf	RC100	RC200	RC300	RC400	RC1000
Maximale Benutzer	10	25	50	150	250	1.000
LAN-Ports (1 Gbit/s)*	3	4	4	6 (max. 22)	14 (max. 22)	14 (max. 22)
GBIC-Ports (10 Gbit/s)*	-	-	-	Optional (max. 8)	Optional (max. 8)	Optional (max. 8)
Formfaktor	Micro-Desktop (Optional Rackmount-Kit)	Micro-Desktop (Optional Rackmount-Kit)	Micro-Desktop (Optional Rackmount-Kit)	19"/1 HE	19"/1 HE	19"/1 HE
WiFi/WLAN	Optional	a/b/g/an/gn	a/b/g/an/gn	-	-	-
LTE/UMTS	Optional	Optional	Optional	-	-	-
Firewall-Durchsatz	900 MBit/s	1.400 MBit/s	1.900 MBit/s	9 GBit/s	18 GBit/s	24 GBit/s
VPN-Durchsatz	300 MBit/s	400 MBit/s	500 MBit/s	1,2 GBit/s	2,1 GBit/s	3,5 GBit/s
HTTP-Proxy mit AV	80 MBit/s	150 MBit/s	200 MBit/s	0,8 GBit/s	1,1 GBit/s	1,4 GBit/s
AES-Hardwarebeschl.	Ja	Ja	Ja	Ja	Ja	Ja
Leistungsaufnahme (Watt)	~13	~15	~15	~60	~80	~100

* = Kombinationsmöglichkeiten beachten, max. zwei Erweiterungskarten

VAT, VOS und Garantie

Firewalls gehören heute zu den wichtigsten Komponenten im Netzwerk. Fallen sie aus, sind viele Prozesse im Unternehmen gestört. Erweiterte Services sorgen für schnelle Reaktion, wenn trotz hoher Qualität einmal etwas defekt ist.

VAT – Unsere Empfehlung zu jedem Gerät: aus „Bring-in“ wird Vorabaustausch. Fehlerhafte Komponenten werden nach Absprache mit dem Support vorab zugesendet.

VOS – Für optimale Verfügbarkeit erfolgt der Tausch der Komponenten direkt vor Ort beim Kunden durch Servicetechniker – und je nach Gerät sogar mit einer Reaktionszeit von 4 Stunden.

Support, Service und Schulung

Wir stehen uneingeschränkt hinter unseren Produkten. Als Partner erhalten Sie bei Securepoint von der ersten Minute an umfassenden Service und Support. Bei Personalengpässen oder bei Planung und Begleitung von Projekten stehen wir Ihnen ebenfalls zur Seite, optional auch vor Ort.

Mit den Wartungsverträgen TA und TA+ ermöglicht Securepoint auch Endkunden den direkten Austausch mit dem firmeneigenen Support-Team.

Unsere Trainingskurse bieten sowohl einen grundlegenden Einstieg in Securepoint-Produkte, als auch kontinuierliche Weiterbildung und Expertenthemen.

UTM-Security bis zu 50 Benutzern (Black Dwarf/RC100/200)

WLAN

LTE/UMTS
Optional

Optimal für KMU

Spezielle Hardware, geringe Stromaufnahme, passive Kühlung und lange Haltbarkeit sorgen für die bestmögliche Leistung der Securepoint NextGen UTM-Firewall in kleinen Netzwerken bis 50 Benutzern. Die Integrierte Hardwarebeschleunigung ermöglicht hohe VPN-Datendurchsätze.

Für diese Appliances sind ein optionales Rackmount-Kit und ein DIN Rail Mount-Adapter verfügbar. Mit diesen Erweiterungen lassen sich die NextGen UTM-Firewalls perfekt in jedem 19" Schrank und auf jeder Hutschiene in Verteiler- sowie Schaltschränken montieren.

WLAN

Die Appliances RC100 und RC200 verfügen über ein integriertes WLAN-Modul mit zwei Antennen. Das 300 MBit/s WLAN inkl. WPA2-Verschlüsselung ist optimal zur Anbindung mobiler Geräte geeignet.
Bei dem Black Dwarf kann das extra erhältliche WLAN-Modul inkl. Antennen einfach nachgerüstet werden.

LTE/UMTS optional

Für eine dauerhafte Internetverbindung oder als Fallback-Lösung lässt sich jederzeit ein optionales LTE/UMTS-Modul nachrüsten.

Black Dwarf/RC100/RC200

Maximale Benutzer:	10/25/50
LAN-Ports:	3/4/4 x 1 GBit/s
Anschlüsse:	VGA, 1 x USB 3.0
WiFi/WLAN:	optional/ja/ja
LTE/UMTS (optional):	Internet oder Fallback
SIM-Kartenslot:	extern zugänglich
Festplatte:	8GB/32GB/32GB
Stromanschluss:	12V; geschraubt
Netzteil (extern):	110-240V; 50-60Hz; 1,5A
Leistungsaufnahme:	~13/~15/~15 Watt
Formfaktor:	Micro-Desktop (B 21 x H 3,5 x T 10,5 cm)
Rackmount-Kit:	optional
DIN Rail Mount:	optional (Hutschienen-Adapter) DIN EN 60715 (35 x 7,5 mm)
Firewall-Durchsatz:	900/1.400/1.900 MBit/s
VPN-Durchsatz:	300/400/500 MBit/s
HTTP-Proxy mit AV:	80/150/200 MBit/s
AES-Hardwarebeschl.:	Ja (Intel)
Lizenzierung:	Single License Modell
Subscription:	1 und 3 Jahre
Softwarebeschränkung:	Black Dwarf nur ein Virus-Scanner
Gewährleistung:	36 Monate Garantie (Bring-in)
RC200/RC300:	*Optional 60 Monate Garantie sowie Vor-Ort-Service buchbar*

UTM-Security bis zu 1.000 Benutzern (RC300/400/1000)

Optimal für Mittelstand bis Rechenzentren

In mittleren und großen Netzwerken ist 19"-Technik der Standard. Die Hardware der RC300 bis RC1000 bietet mit einem modularen Aufbau viel Flexibilität. Die Luftführung sorgt für optimale Leistung in typischen 19"-Umgebungen.

Mit bis zu 22 GBit-Ethernet Anschlüssen und 4 x 10 GBit Fibre-Optik-Anschlüssen (bei gleichzeitig max. 14 GBit Ethernet Anschlüssen) bieten sie für alle Umgebungen ausreichend Konnektivität.

19 Zoll Ready

Module Verfügbar

Erweiterungsmöglichkeiten bis 10 GBit

Die NextGen UTM-Firewalls der Enterprise-Klasse verfügen auf der Vorderseite über zwei Einschübe, um Erweiterungskarten aufzunehmen (bei der RC400 und RC1000 ist bereits einer belegt). Zur Auswahl stehen Karten mit 8-Port GBit Ethernet (RJ45) und 4-Port GBIC für SFP+ 10 GBit Module (SR oder LR).

RC300/RC400/RC1000

Maximale Benutzer:	150/250/1.000
LAN-Ports:	6/14/14 x 1 GBit/s
Anschlüsse:	VGA (hinten), 2 x USB 3.0
Festplatte:	128/150/150 GB
Hardware-RAID 1:	nein/ja/ja
Netzteil (intern):	110-240V; 50-60Hz
Leistungsaufnahme:	~60 Watt
Formfaktor:	19", 1 HE, kurzes Rack-Gehäuse (B 43 x H 4,4 x T 47,5 cm)

Betriebsumgebung

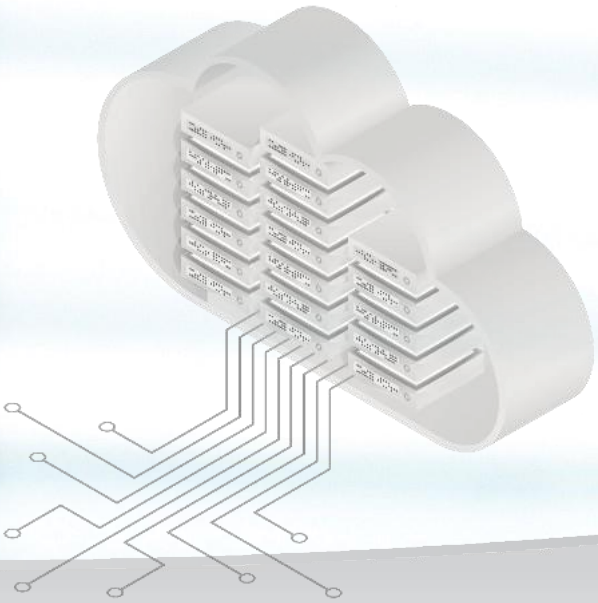
Temperatur:	0°C ~ 40°C
Luftfeuchtigkeit:	10 % ~ 80 %

Firewall-Durchsatz:	9/18/24 GBit/s
VPN-Durchsatz:	1,2/2,1/3,5 GBit/s
HTTP-Proxy mit AV:	0,8/1,1/1,4 GBit/s
AES-Hardwarebeschl.:	Ja (Intel)

Lizenzierung:	Single License Modell
Subscription:	1 und 3 Jahre

Gewährleistung:	36 Monate Garantie (Bring-in) *Optional 60 Monate Garantie sowie Vor-Ort-Service buchbar*

Erweiterte IT-Security



Sichere Cloud mit virtuellen UTM-Gateways

Die virtuellen Securepoint UTM-Gateways sind auf VMware®, Microsoft Hyper-V® sowie KVM lauffähig. Dedizierte Hardware lässt sich ebenfalls nutzen, um die IT-Security-Lösung zum Schutz von Unternehmensnetzwerken, Rechenzentren und Cloud-Systemen zu betreiben.

Soll die IT-Infrastruktur ganz oder teilweise in die Cloud ausgelagert werden, bieten sich die virtuellen Securepoint UTM-Gateways geradezu an. Ein virtuelles Gateway innerhalb der Cloud schützt das Netzwerk, die Daten und Dienste, die an dieser Stelle genutzt werden sollen.

Virtuelle UTM-Gateways

Maximale Benutzer:	10 bis 1.000 (Lizenzabhängig)
Virtuelle Umgebungen:	VMware®, Microsoft Hyper-V® und KVM
LAN-Ports Mbit/s:	bis zu 16 Lan-Ports, mit VLAN erweiterbar
Hardware:	abhängig von der virtuellen Umgebung
Lizenzierung:	Single License Modell
Subscription:	1 und 3 Jahre

Ganzheitlicher IT-Security-Schutzschirm

Securepoint Antivirus Pro und die NextGen UTM-Firewall bilden zusammen die optimale IT-Security-Lösung für Unternehmen. Gemeinschaftlich entsteht ein übergreifender Schutzschirm vor allen mobilen, lokalen und cloudbasierten Risiken. Das erreicht Securepoint vor allem dadurch, dass unterschiedliche führende Scan-Engines in den IT-Security-Produkten eingesetzt werden.

Weitere Informationen:
www.securepoint.de/antivirus

Absicherung von Smartphones und Tablets

Mobile Geräte sind zunehmend Phishing-Versuchen, externen Jailbreaks und anderen Cyberattacken ausgesetzt. Sie benötigen deshalb ein besonders hohes Schutzniveau.

Securepoint schließt mit Mobile Security die Lücke in der mobilen Datensicherheit. Mobile Security bietet vollständigen Schutz für alle mobilen Endpoints in Unternehmen – auch für iOS-Geräte.

Weitere Informationen:
www.securepoint.de/mobilesecurity

Umfassender Schutz für Ihre Praxis

Securepoint Unified Security

Unsere ganzheitlichen Sicherheitslösungen legen sich wie die Schichten einer Zwiebel schützend um Ihre IT. Das nennen wir Securepoint Unified Security: Sicherheit vom ersten Gedanken bis zum letzten Bit.

Sie bildet eine komplexe Sicherheitsstruktur zum Schutz von Unternehmen. Die NextGen UTM-Firewall nimmt einen großen Stellenwert innerhalb der Unified Security ein.

Komplette Netzwerke werden vor Cyberangriffen und Schadsoftware, wie z. B. Spam oder Spyware, abgesichert. Dafür schaltet sich die NextGen UTM-Firewall schützend zwischen Netzwerk und Internet und setzt Zugriffsbeschränkungen durch. Die Sicherheitsanforderungen werden je nach Gerätestandort angepasst – egal ob mobil unterwegs, im Praxis-Netzwerk oder im Home-Office.

Die optimal aufeinander abgestimmten Lösungen wie NextGen UTM-Firewall, Mobile Security, Antivirus Pro und E-Mail-Archivierung garantieren Ihnen jederzeit höchste Sicherheit. Damit ermöglicht Securepoint kleinen und mittleren Unternehmen (KMU) IT-Sicherheit auf Enterprise-Niveau zu attraktiven Konditionen.

Threat Report über alle Systeme

Mit dem Threat Report der Securepoint Unified Security visualisieren wir produktübergreifend den Sicherheitsstatus aller Geräte und Dienste.

Regelmäßige Pentests

Unsere eigenen Betriebssysteme, Software und Dienste werden laufend überprüft. Die Sicherheitsstruktur der Securepoint Unified Security wird durch regelmäßige Penetrationtests zusätzlich von unabhängigen Dritten auf Herz und Nieren getestet.

Änderungen und Irrtümer vorbehalten. Stand: 21.01.2021

SECUREPOINT
SECURITY SOLUTIONS

Securepoint GmbH
Bleckeder Landstraße 28
21337 Lüneburg
Deutschland

IT-Security made in Germany

EU DS-GVO ready

SecurITy made in Germany

Com²Med
PARTNER FÜR MEDIZIN + TECHNIK

Systemhaus/Partner:

Com²Med Medizintechnologien
GmbH&Co.KG
Frankfurter Str. 3a
38122 Braunschweig
FREECALL 0800-5003001
Mail: info@com2med.de
Web: www.com2med.de