SECUREPOINT
SECURITY SOLUTIONS

Securepoint Operation Center:
Zentrales Management von IT-Security-Systemen

Der Leitstand für Ihre Security- und Netzwerk-Systeme

- Konfiguration und Verwaltung aller Securepoint UTM-/VPN-Gateways, WLAN/Network Access Controller und E-Mail-Archivierungslösungen
- Einfache Integration von Systemen anderer Hersteller in SOC
- Einfaches Passwortmanagement
- Zentrale Remote-Administration und -Konfiguration
- Zentrales Monitoring/Logging/Reporting auch nach dem Vier-Augen-Prinzip
- Automatische, zeitgesteuerte Backups und Tasks
- Echtzeitüberwachung und Risikomanagement mit automatisierter Warnung
- Lizenz- und Inventurverwaltung aller Geräte
- Lauffähig als lokale Desktop- oder zentrale Server-Anwendung
- Integrierbar in Ihre IT-Backup-Struktur

Securepoint Operation Center (SOC)

Der Leitstand für Ihre IT-Security und Netzwerke.

Das Securepoint Operation Center (SOC) ist eine zentrale Management-Lösung für alle Lösungen von Securepoint wie die VPN-/UTM-Systeme, die Network Access Controller und bietet ebenfalls die einfache Integration von Lösungen von Dritt-Anbietern. Der sofort verfügbare Status und die Möglichkeit der Systemüberwachung von jedem Ort aus machen aus Konfiguration, Monitoring, Reporting und Verwaltung aller Systeme einen zeitsparenden und übersichtlichen Prozess.

SOC passt sich Ihren Anforderungen an

Das Securepoint Operation Center (SOC) ist ein Allround-Talent und passt sich Ihren Anforderungen an. SOC vereinfacht:

- die Übersicht zu allen Securepoint Produkten,
- die System-Konfiguration und das -Management von UTM- und VPN-Systemen, Network Access Controllern sowie den E-Mail-Archivierungssystemen von Securepoint.
- über eine Schnittstelle die Integration von Dritt-Systemen, wie z. B. den Intel Server Control etc. Binden Sie einfach jedes andere System an SOC an, das über ein Webinterface verfügt!
- automatisierte System-Backups und -Updates,
- die Überwachung in Echtzeit und das Monitoring,
- das Logging, die Fehlersuche und das Reporting, auch nach dem Vier-Augen-Prinzip,
- Management und Verschlüsselung von Log-Daten,
- das Access-Management von Usern (Authentisierung, Passwort-Verwaltung),
- zentrale Definition von globalen Einstellungen,
- die Lizenz- und Geräteverwaltung,
- und ermöglicht große VPN- oder UTM-Rollouts!

Schnelle Übersicht über alle Systeme

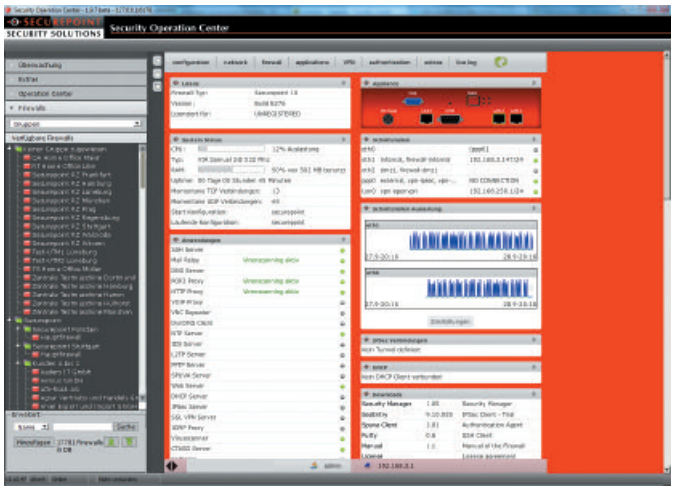
Das Dashboard zeigt eine grafische Übersicht aller UTM- und VPN-Gateways an. Sie haben die Möglichkeit, die wichtigsten Monitoring-Daten im Dashboard von SOC anzuzeigen.

Zentrale Dashboard-Funktionen:

- Das Dashboard verfügt über eine Boxen- und Listenansicht aller UTM- und VPN-Systeme.
- Für jedes UTM- und VPN-Gateway werden die Auslastung der CPU, des Speichers, der Swap Auslagerungspartition und die Gültigkeitsdauer der Lizenz grafisch dargestellt.
- Zusätzlich werden die Anzahl der TCP- und UDP-Verbindungen sowie die verwendete Securepoint Version angezeigt.
- Mit dem Dashboard wird die Suche, das Filtern, die Anzeige und die Sortierung von Systemen durchgeführt, um schnellen Überblick selbst über Tausende von Systemen zu erhalten.
- Das Multi-Tabbing erlaubt die gleichzeitige Remote-Verbindung zu mehreren Systemen.

Haben Sie alles im Blick und im Griff!

Zentrale Administration, Backups und Updates



Mit dem Securepoint Operation Center können alle VPN- und UTM-Systeme verwaltet werden, damit auch sehr weitverzweigte Netzwerke sicher gemanagt werden können. Eine übersichtliche Darstellung aller Systeme stehen Ihnen zur Verfügung. Zahlreiche Sortier- und Filter-Funktionen helfen dem Administrator, den Überblick auch über sehr große UTM- und VPN-Infrastrukturen zu behalten.

Administration und Konfiguration:
Hauptaufgabe des SOC ist die Möglichkeit der zentralen Remote-Konfiguration Ihrer UTM-/VPN-Gateways.

Automatisches Backup:
SOC kann automatisiert alle UTM- und VPN-Systeme ansprechen und zentrale Backups der Systeme zeitgesteuert durchführen. Die Backups werden verschlüsselt in einer Datenbank gespeichert. Bis zu zehn Backups können pro UTM- oder VPN-System zentral gehalten werden. Der Backup-Zeitraum ist frei einstellbar. Die Backups sind über das System ebenfalls wieder sehr einfach auf die UTM- und VPN-Systeme rücksicherbar.

Aufgaben:
Sie können Aufgaben und Befehle für Ihre Gateways und Benutzer erstellen, die zu einem bestimmten Zeitpunkt automatisiert ausgeführt werden sollen. Dies sind z. B. Backups, Updates etc.

Tasklog:
Überprüfen Sie hier, ob die angelegten Aufgaben auch ordnungsgemäß durchgeführt worden oder Fehler aufgetreten sind, die korrigiert werden sollten.

Gruppen:
In diesem Bereich werden Gateway-Gruppen verwaltet. Diese Gruppen helfen bei der Organisation einer großen Anzahl von verwalteten UTM-/VPN-Gateways.

Versionen:
Hier können Sie sich über die verfügbaren Software-Versionen informieren. Liegt eine neuere Version vor, können Sie eine neue Version laden und Software-Updates durchführen.

Protokoll:
Alle Vorgänge, die ein Benutzer am SOC durchführt, werden protokolliert. Zusätzlich werden Aktionen wie das Erstellen von Sicherungen und Monitoring-Läufe des Systems protokolliert. Hier wird nachverfolgt, welche Aktionen von welchem Benutzern oder dem System ausgeführt worden sind.

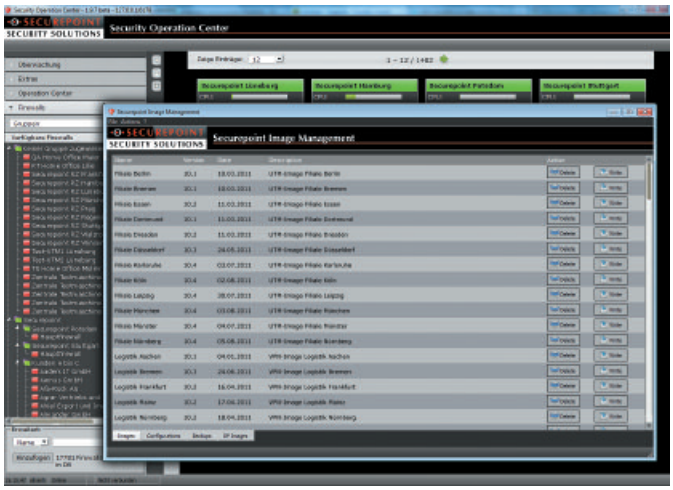
UTM/VPN Gateways:
Hier werden alle verwalteten Gateways aufgelistet. Die Liste enthält den Namen, die IP-Adresse/Hostnamen, Typ, Standort und Besitzer des jeweiligen Systems. Auch Benutzer und deren Rechte werden angezeigt und sind editierbar.

Benutzerverwaltung:
Sie können Benutzer anlegen, die Sie in Benutzergruppen in SOC organisieren können. Für Benutzer können eingeschränkte Benutzerrechte oder Administratorrechte vergeben werden.

Securepoint Operation Center (SOC)

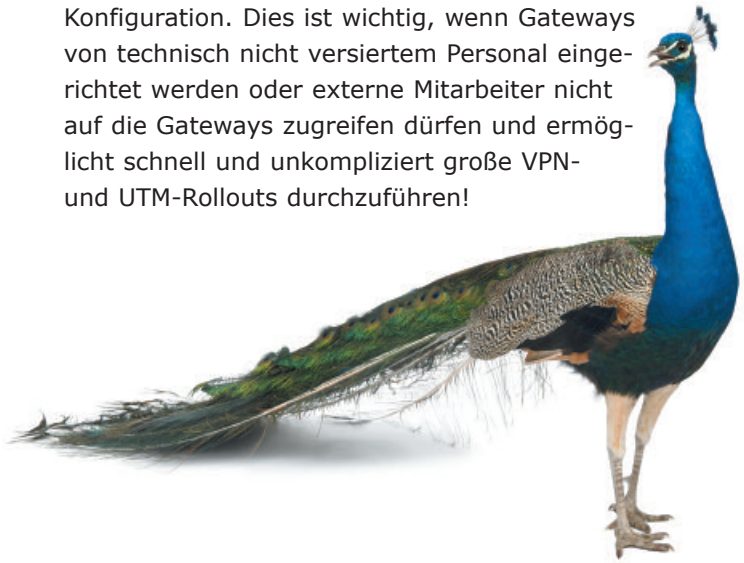
Der Leitstand für Ihre IT-Security und Netzwerke.

Automatisierte Erstellung von Installationsimages

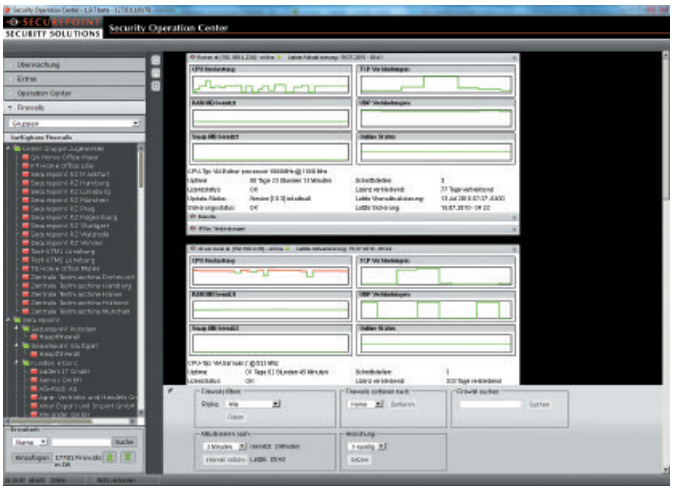


Das Image Management von SOC stellt ein System zur Erstellung/Verwaltung von Installationsimages bereit. Damit ist es möglich, neue Konfigurationen mit Hilfe eines Assistenten automatisiert zu erstellen.

Zentral gesteuerte Rollouts:
Aus neuen Konfigurationen oder aus vorhandenen Backups können Installationsimages erstellt werden. Die Grund- und erstellten Installationsimages werden zentral im SOC verwaltet. Neue Grundimages können aus dem Internet von Securepoint nachgeladen werden. Damit ist es möglich, zentral für beliebig viele Gateways spezielle Installationimages zu erzeugen. Diese können z. B. auf einem USB-Stick gespeichert werden. Von diesem USB-Stick kann jedes Gateway direkt booten und läuft dann mit der gewünschten Konfiguration. Dies ist wichtig, wenn Gateways von technisch nicht versiertem Personal eingerichtet werden oder externe Mitarbeiter nicht auf die Gateways zugreifen dürfen und ermöglicht schnell und unkompliziert große VPN- und UTM-Rollouts durchzuführen!



Zentrales Monitoring, Logging und Reporting



Das SOC bietet eine Vielzahl von zentralen Auditing-, Monitoring-, Logging- und Reporting-Funktionen, damit Sie jederzeit alles im Blick haben.

Vier-Augen-Prinzip:
SOC unterstützt das Vier-Augen-Prinzip für Logs und Reports. Dieses Prinzip besagt, dass wichtige Entscheidungen nicht von einer einzelnen Person getroffen werden oder kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden sollen oder dürfen. Ziel ist es, das Risiko von Fehlern und den Missbrauch zu reduzieren oder erst – bei z. B. arbeitsrechtlich relevanten Vorgängen – nachweisbar zu machen. Die Logdaten können anonymisiert werden und sind verschlüsselt.

Monitoring:
Mittels Monitoring können sich die Administratoren schnell einen Überblick über den Zustand und die Auslastung aller UTM- und VPN-Systeme verschaffen. Verschiedene Eskalationsstufen geben den System-Administratoren die Informationen, die sie in diesem Moment benötigen, um auch bei kritischen Situationen zielgerichtet und schnell handeln zu können.

Auditing:
Sämtliche Vorgänge innerhalb des Securepoint Operation Centers werden geloggt und können nachgewiesen werden. Somit ist die Rückverfolgbarkeit und vollständige Kontrolle jederzeit gegeben.

SOC schärft Ihren Blick:

Logging:
Das SOC LogCenter zeichnet Syslog-Protokolldaten der Gateways auf und archiviert diese in vorgegebenen Intervallen. Der LiveLog ermöglicht es, in Echtzeit Analysen durchzuführen. Archivierte Daten werden für einen wählbaren Zeitraum vorgehalten und danach gelöscht. Das LogCenter versendet auf Wunsch tägliche Berichts-E-Mails, Alarm-E-Mails und Ereignis-E-Mails zu selbstdefinierten Ereignissen.

Reporting:
Der SOC LogClient erstellt aus den Protokolldaten Berichte für jedes eingetragene Gateway. Die Berichte werden tabellarisch, grafisch oder gemischt dargestellt. Es werden Daten für die letzten 24 Stunden, die Woche, den Monat oder ein Jahr angezeigt.

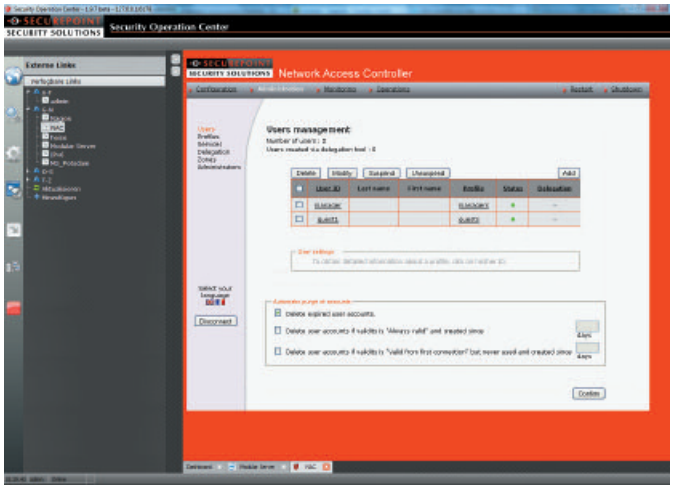
Reports:
Um die Protokolldaten gezielt zu analysieren, sind die in SOC implementierten Filter hilfreiche Werkzeuge, um die unterschiedlichsten Reports zu erstellen. Folgende Reports werden vom SOC LogClient grafisch und in Text-Form generiert:

- Interface-Auslastung: gesendete/empfangene Traffic
- Alerts: ausgelöste Alarme
- IDS IPs: Intrusion Detection System Angriffe
- IDS IP+Attack: IP der Angreiferer und Angriffsarten
- IDS Attack: Tabelle der erkannten Angriffe
- Malware: Namen, Art und Anzahl der Malware
- Top Websites: Traffic der aufgerufenen Webseiten
- Top Surfer: alle User, die Traffic verursachen
- Webreport: Auswertung des Traffics eines Benutzers
- Surfer+Websites: aufgerufenen Websites nach Usern
- Blocked Categories: blockierte Webseiten-Kategorien
- Blocked Websites: blockierte Webseiten
- Top Drop: abgelehnte Pakete
- Top Accept: angenommene Pakete
- Top Reject: zurückgewiesene Pakete
- Top rejected E-Mail: zurückgewiesene E-Mails
- Top recipients E-Mail: angenommene E-Mails
- Top sender E-Mail: angenom./zurückgewies. E-Mails
- Top accepted Mailservers: angenommene Mailserver
- Top rejected Mailservers: zurückgewies. Mailserver
- Top Server in Greylisting whitelisted
- Top Server in Greylisting rejected
- Possible SMTP Attack: Server-IPs bei SMTP-Angriff

Securepoint Operation Center (SOC)

Der Leitstand für Ihre IT-Security und Netzwerke.

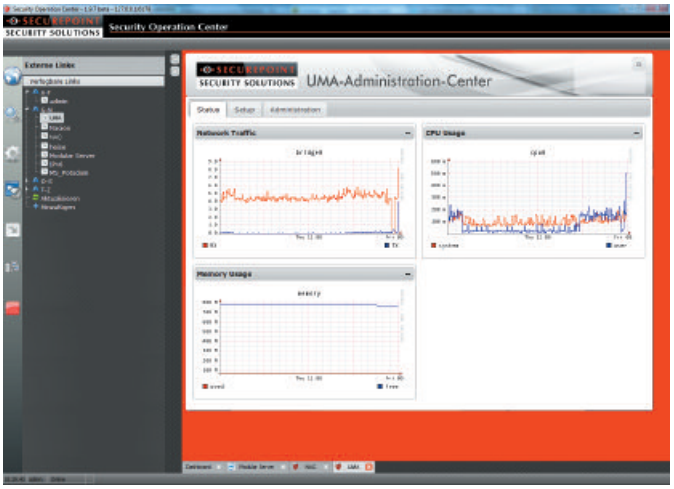
Management von Network Access Controllern



Die neuen Securepoint WLAN und Network Access Controller (NAC) können mit SOC einfach und bequem zentral administriert werden. Die NAC ermöglicht Mitarbeitern/Gästen, sich in Konferenz- und Schulungsräumen, Büros, öffentlichen Bereichen wie in Hotels, Kliniken, Behörden, Internet-Cafes, Restaurants etc. per WLAN oder LAN sehr einfach (da konfigurationsfrei) und sicher einzuwählen, um Zugang zum Internet, zu Daten-, Voice- und Video-Anwendungen zu erhalten. Eine Abrechnung (Billing) von Gast-Accounts ist ebenfalls möglich, die Rückverfolgbarkeit und Kontrolle ist jederzeit gegeben. Beliebige PCs, Notebooks, Handys, iPhones und iPads werden selbstverständlich unterstützt.

Konfigurationsfreier Zugang zum Internet:
Die Zugänge stehen konfigurationsfrei zur Verfügung und Hotel-, Klinik-Personal oder Pförtner sind in der Lage, die Dienste ohne technisches Hintergrundwissen Kunden, Besuchern und Mitarbeitern zur Verfügung zu stellen. Eine einfache Einweisung in das NAC-System reicht aus. Alle gesetzlichen Anforderungen (Provider-Haftung, Schutz bei Urheberrechtsverletzungen etc.) werden erfüllt.

Management des Unified Mail Archives



Über SOC ist es ebenfalls möglich, das Securepoint Unified Mail Archive (UMA) zu administrieren.

Funktionen des Unified Mail Archives:
- Gesetzeskonforme, revisionssichere und automatische Archivierung des gesamten E-Mail-Verkehrs nach dem hohen deutschen Behördenstandard mit Governikus LZA.
- Beweiswerterhaltende Langzeitspeicherung nach technischer Richtlinie 03125 des BSI (TR-ESOR) und DIN – in Evaluierung nach Protection Profile Archi-Safe und Zertifizierung nach TR (Governikus LZA).
- Einsetzbar mit MS Exchange/anderen Mail-Servern.
- Direkter Zugriff aus Microsoft Outlook, andere E-Mail-Clients (z. B. Thunderbird, ApplE-Mail etc.) und über Webinterface.
- Volltextindizierte Suche nach E-Mails.
- Einfache Wiederherstellung versehentlich oder vorsätzlich gelöschter E-Mails.
- „Supervisor Mode" nach Vier-Augen-Prinzip für Auditoren zur Einhaltung des gesetzlich vorgeschriebenen Datenschutzes.
- Anbindung an Active Directory oder LDAP-Verzeichnisdienste.
- Automatische, interne Zeitstempelung.
- Qualifizierte Zeitstempel.
- Ohne Aufwand transparent in das Netzwerk integrierbar.
- Einsetzbar als Hardware-Appliance oder in virtuellen Maschinen bzw. Clouds.

Als Desktop- oder Server-Version!

Einfaches Einbinden von Dritt-Systemen

Das Securepoint Operation Center (SOC) ist ein Multi-Talent und erlaubt es Ihnen, eine Vielzahl von verschiedenen IT-Security-Systemen – auch von anderen Herstellern – einfach einzubinden und zu verwalten. Hierzu gehören:

- Unified Threat Management (UTM)-Lösungen von Securepoint und TERRA,
- VPN-Lösungen von Securepoint und TERRA,
- Network Access Controller (NAC) Lösungen für das WLAN-Management von Securepoint,
- Unified Mail Archive (UMA)-Lösungen zur revisionssicheren E-Mail-Archivierung von Securepoint.

Link Center:
Über das Link Center können Sie folgende Dritt-Anbieter-Produkte einbinden:

- Intel Server Control-Lösungen werden von SOC direkt unterstützt
- sowie jede andere Lösung von Herstellern, die über ein Webinterface verfügen.
- Im Link Center können ebenfalls RDP- und VNC-Verbindungen eingebunden werden.

SOC gibt's als Desktop- und Server-Anwendung

Das Securepoint Operation Center kann als lokale Desktop- oder Client-/Server-Anwendung konfiguriert und betrieben werden. Das SOC kann auf einem Server installiert werden, von wo aus alle Dienste zentral verfügbar sind. Beliebig viele SOC-Clients können auf den zentralen SOC-Server zugreifen, um die UTM- und VPN-Systeme bzw. weitere IT-Security-Systeme remote zu administrieren. Das SOC ist integrierbar in ein zentrales IT-Backup-Konzept. Selbstverständlich ist ein sicherer, verschlüsselter Zugriff und die Verschlüsselung der SOC-Datenbank integriert. SOC ist damit insbesondere für Managed Services, Provider und Rechenzentren geeignet, die ein hohes Maß an Sicherheit voraussetzen.

Securepoint Operation Center (SOC)

Die Vorteile von SOC zusammengefasst:

- Sparen Sie Zeit bei Einrichtung, Wartung und Update durch das zentrale Management.

- Reduzieren Sie Ihre tägliche Arbeitsbelastung, indem Sie einfach im SOC organisieren und Verantwortlichkeiten verteilen.

- Weisen Sie Benutzern und Gruppen einfach Installationen/ Konfigurationen zu, für die sie verantwortlich sein sollen.

- Führen Sie Aufgaben wie Updates zentral durch und richten Sie die Durchführung wiederkehrender Aufgaben zu festen Zeiten ein.

- Vermeiden Sie eine komplexe Passwortverwaltung und haben Sie einen einfachen, schnellen Zugriff auf beliebige Securepoint Gateways und Dritt-Systeme.

- Behalten Sie stets den Überblick, was in Ihrem Netzwerk passiert. Überwachen Sie Daten wie Lizenzen, Bedrohungen, Versionen und Auslastungen in Echtzeit über das intelligente Dashboard.

- Reagieren Sie schneller auf Bedrohungen und bleiben Sie stets auf dem Laufenden.

- Beobachten Sie detaillierte Statistiken über Performance, Netzwerk-aktivitäten, Webnutzung und Traffic für einzelne oder mehrere Standorte.

- Sorgen Sie für Sicherheit mit automatisierten Backups und Tasks.

- Sparen Sie Kosten, die typischerweise für die Verwaltung einer Vielzahl von Systemen anfallen.

- Und: SOC kostet Sie nichts!

Systemhaus/Partner:

SECUREPOINT SECURITY SOLUTIONS

Securepoint GmbH
Salzstraße 1
21335 Lüneburg
Germany

fon: ++49 (0) 41 31 / 24 01-0
fax: ++49 (0) 41 31 / 24 01-50

mail: info@securepoint.de
web: www.securepoint.de