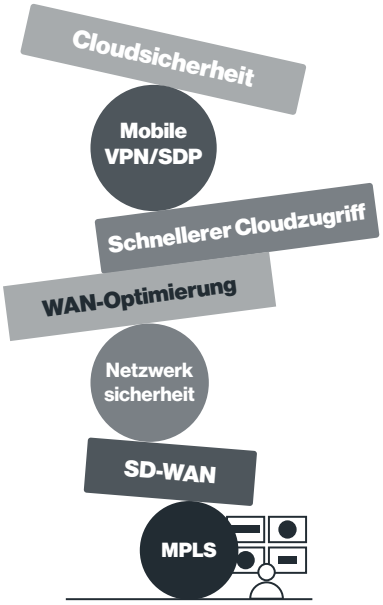
CATO NETWORKS

Cato Cloud: Der globale und sichere Managed SD-WAN-Service

Lösungsübersicht

Die Herausforderungen der digitalen Transformation im Bereich Netzwerk und Sicherheit



Immer mehr Prozesse in Ihrem Unternehmen werden digitalisiert. Daher ist ein reibungsloser Zugriff auf Anwendungen und Daten unverzichtbar. Zudem müssen diese sowohl vor Ort als auch in der Cloud verfügbar sein, da es immer mehr global agierende, mobile Mitarbeiter gibt.

Das veraltete Netzwerk, das auf einer kostspieligen und unflexiblen MPLS-Technologie basiert, ist für die digitale Transformation Ihres Unternehmens weder heute noch in Zukunft geeignet.

Genau genommen wären zu viele Punktlösungen nötig, um Ihre Netzwerk-, Sicherheits-, Clouds-, Mobilitäts- und globalen Anforderungen zu erfüllen. Den Aufbau eines derart komplexen Netzwerks allein zu bewerkstelligen ist schwierig und ressourcenintensiv, und es ist sehr teuer, einen Telekommunikationsanbieter damit zu beauftragen. Aber es gibt einen besseren Weg.

Ein digitales Unternehmen hat eine „Cloud First"-Strategie und zeichnet sich durch Schnelligkeit und Agilität aus – und diese Entwicklung wird durch veraltete Netzwerk- und Telekommunikationslösungen ausgebremst.

Bestehende MPLS-Netzwerke sind nicht mehr geeignet, weil

- die MPLS-Technologie kostspielig, unflexibel und nicht für den Cloudzugriff konzipiert ist.
- ein direkter und sicherer Internetzugang an jedem Standort benötigt wird, während MPLS-Netzwerke den Internetdatenverkehr auf zentralisierte Webportale zurückleiten.
- MPLS auf physische Standorte beschränkt ist, wodurch Cloud- und mobile Ressourcen nur zweitklassig behandelt werden.
- MPLS-Netzwerke spezielle Appliances und Lösungen erfordern, was die Netzwerkverwaltung und Wartungsmaßnahmen über den gesamten Lebenszyklus erschwert.

Herkömmliche Telekommunikationsanbieter sind die falschen Partner, denn sie sind

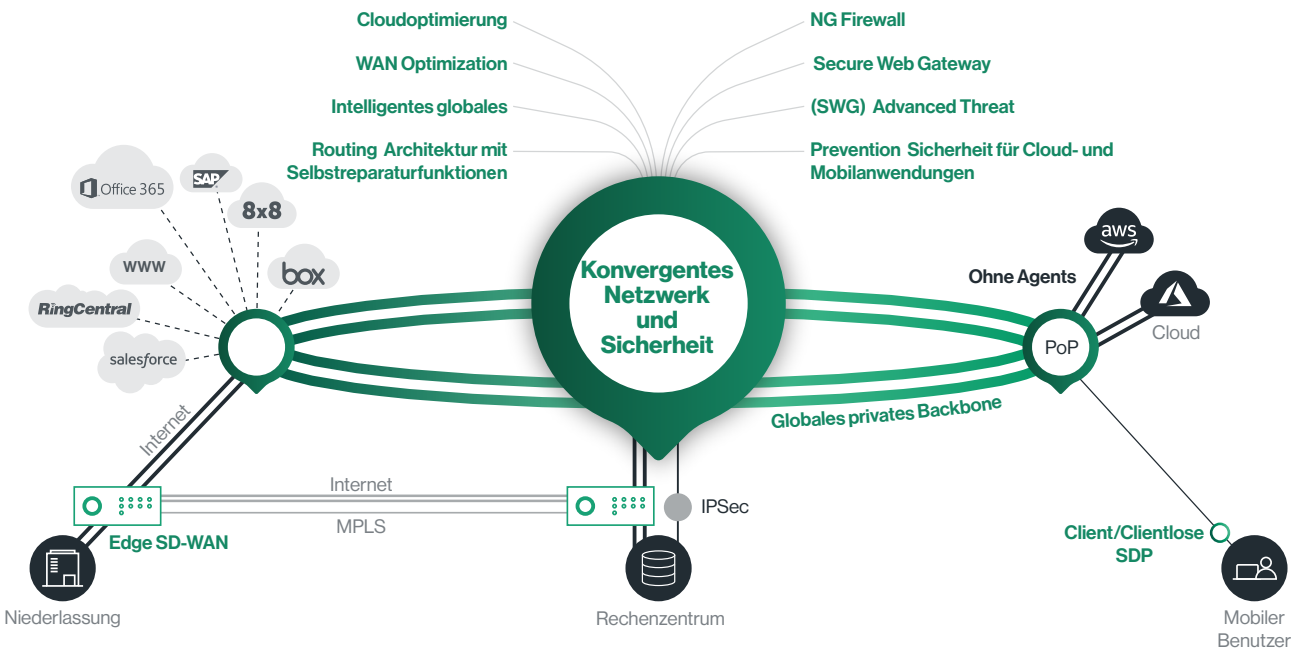
- teuer im Vergleich zu einer Lösung, die Sie selbst implementieren.
- bürokratisch, da Bereitstellungen an neuen Standorten sehr lange dauern.
- langsam, da sie mit einem ticketbasierten Kundendienst arbeiten.
- undurchsichtig und bieten wenig Transparenz und Kontrolle für Kunden

Der cloudnative Carrier

Der EINZIGE Managed SD-WAN-Service, der standardmäßig die globale Reichweite, den Self-Service und die Agilität der Cloud bietet.

Mit Cato können Unternehmen von ihrer kostspieligen, unflexiblen MPLS-Technologie und einer Sammlung von Punktlösungen zu einer einfachen, flexiblen und erschwinglichen Netzwerklösung wechseln.

Cato Cloud verbindet alle Netzwerkressourcen des Unternehmens, wie Niederlassungen, mobile Mitarbeiter sowie physische und cloudbasierte Rechenzentren, in einem globalen, sicheren Managed SD-WAN-Service. Da der gesamte WAN- und Internetdatenverkehr in der Cloud konsolidiert ist, wird jederzeit das gesamte Netzwerk durch die Sicherheitsservices von Cato geschützt.



Globales privates Backbone-Netzwerk

Das private globale Backbone-Netzwerk von Cato besteht aus über 45 PoPs auf der ganzen Welt, die durch mehrere SLA-gestützte Tier-1-Provider miteinander verbunden sind. Alle PoPs werden auf dem cloudnativen Software-Stack von Cato ausgeführt. Er ist vollständig mehrinstanzenfähig, skalierbar, flächendeckend einsetzbar und führt alle benötigten Netzwerkfunktionen aus, wie z. B. intelligentes globales Routing, dynamische Pfadauswahl, Datenverkehrsoptimierung und End-to-End-Verschlüsselung. Darüber hinaus implementiert er die von den Cato-Sicherheitsservices benötigten Kontroll- und Durchsetzungsmechanismen.

WAN-Optimierung

Die WAN-Optimierung ist ein wesentlicher Bestandteil des Netzwerksoftware-Stacks, wobei TCP-Proxys und komplexe Algorithmen für das Überlastungsmanagement eingesetzt werden, um den Throughput bei wichtigen Vorgängen, z. B. Dateiübertragungen, zu maximieren.

Intelligentes globales Routing

Die proprietären Routing-Algorithmen von Cato berücksichtigen Latenz, Paketverlust und Jitter. Anders als beim Internetrouting sind beim Cato-Routing stets die Leistung und nicht die Kosten entscheidend, sodass für jedes Netzwerkpaket die optimale Route ausgewählt wird.

Verschlüsselung

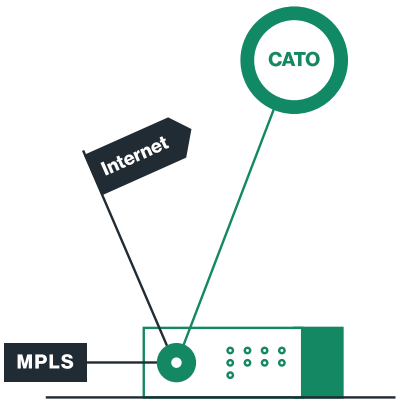
Die End-to-End-Verschlüsselung mit den leistungsstärksten branchenüblichen Verschlüsselungsprogrammen gewährleistet die Vertraulichkeit der Daten, den Schutz der Privatsphäre und eine sichere Nutzung auf mehreren Instanzen.

Architektur mit Selbstreparaturfunktionen

Das Cato-Backbone-Netzwerk wird kontinuierlich überwacht und kontrolliert. Dank der Selbstreparaturfunktionen ist eine Serviceverfügbarkeit von 99,999 % garantiert. Die flexiblen, skalierbaren Entwurfsprinzipien für die Cloudsoftware sorgen für ein ungestörtes Wachstum der Serviceinfrastruktur ohne Ausfallzeiten oder Unterbrechungen.

Die Standorte stellen eine Verbindung zum globalen privaten Cato-Backbone-Netzwerk her, indem sie verschlüsselte Tunnel von einem Cato-Socket, der WAN-Edge-Appliance ohne Benutzereingriff, oder einem beliebigen anderen Gerät, das IPsec-Tunnel unterstützt, einrichten. Cloudrechenzentren verbinden sich über eine agentenlose Konfiguration; mobile Benutzer verbinden sich clientlos oder über einen Cato-Client.

Edge-SD-WAN



Das Edge-SD-WAN von Cato nutzt mehrere Internetanschlüsse für einen zuverlässigen, leistungsstarken Zugang zum globalen privaten Backbone-Netzwerk von Cato. Zudem kann der Datenverkehr über MPLS, direkt zwischen den Standorten (nicht über den Cato-PoP) und über IPsec-Tunnel zu Geräten von Drittanbietern geleitet werden.

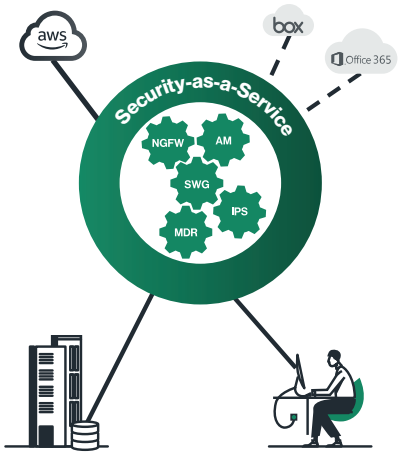
Beim Cato-Socket, der Edge-SD-WAN-Appliance von Cato, handelt es sich um ein Gerät, dass nach Anschluss an die Stromversorgung und das Internet ohne Benutzereingriff innerhalb weniger Minuten einsatzbereit ist. Die Sockets sind in zwei Ausführungen erhältlich: X1500 für Niederlassungen und X1700 für Rechenzentren. Beide werden kontinuierlich vom Cato-Netzwerkbetriebszentrum überwacht und aktualisiert.

Cato-Sockets bieten folgende Funktionen:

- **Link Aggregation,** wodurch der ein- und ausgehende Verkehr über MPLS und verschiedene Internetleitungen (Glasfaser, DSL, Kabel, 4G/LTE oder 5G) ausgeglichen wird, um die Bandbreite (aktiv/aktiv) und die Verfügbarkeit zu maximieren.
- **Dynamische Pfadauswahl**, die den Datenverkehr abhängig von der Anwendungs-, Benutzer- und Echtzeit-Verbindungsqualität (Jitter, Latenz und Paketverlust) optimal weiterleitet.
- **Anwendungsidentifizierung**, die die neueste Deep Packet Inspection-Engine von Cato verwendet, um automatisch Tausende von Anwendungen und Millionen von Domains beim ersten Paket zu identifizieren.
- **Regeln zur Verwaltung der Bandbreite** stellen sicher, dass kritischere Anwendungen stets die erforderliche vor- und nachgelagerte Kapazität erhalten, wohingegen andere Anwendungen zweitrangig versorgt werden.
- **Reduzierung von Paketverlusten** durch dynamische Umschaltung des Datenverkehrs auf alternative, leistungsfähigere Verbindungen und proaktive Duplizierung von Paketen für jede einzelne Anwendung. Die Cato-Architektur eliminiert Paketverluste auf der mittleren Meile.
- **Integration von Routingprotokollen** mit Nutzung des BGP, um fundierte Routingentscheidungen in Echtzeit zu treffen, wobei die bestehende Routinginfrastruktur eines Unternehmens einfach in das Cato-Edge-SD-WAN integriert werden kann.
- **Hochverfügbarkeit,** die keine zusätzlichen, wiederkehrenden Kosten mit sich bringt und sich einfach innerhalb von Minuten bereitstellen lässt. Die Sockets verbinden sich automatisch mit dem besten verfügbaren Cato-PoP. Sollte die Verbindung schlechter werden oder ausfallen, verbindet sich das Cato-Socket automatisch wieder mit dem besten verfügbaren PoP.

Security-as-a-Service

Die Cato-Sicherheits-Engines sind in das private globale Backbone-Netzwerk von Cato integriert und werden als Service bereitgestellt. Der Erwerb oder die Bereitstellung zusätzlicher Appliances ist dazu nicht erforderlich. Zu den Sicherheits-Engines gehören eine anwendungsbezogene Next Generation Firewall (NGFW), ein Secure Web Gateway (SWG) mit URL-Filterung, Standard- und Next-Generation-Antischadsoftware und eine vom Cato-SOC (Security Operation Center) verwaltete IPS-Lösung. Diese Sicherheits-Engines basieren auf einem umfassenden MDR-Service (Managed Threat Detection and Response), der als Teil des Managed Services-Angebots von Cato zur Verfügung gestellt wird. Alle Engines lassen sich nahtlos skalieren, um den gesamten Kundendatenverkehr verschlüsselt und unverschlüsselt zu verarbeiten, ohne dass eine Größenanpassung, ein Patching oder ein Upgrade von Appliances und Punktlösungen erforderlich ist. Cato stellt sowohl den Datenschutz der Benutzer als auch die Einhaltung der DSGVO sicher. Es werden keine geprüfte Daten auf Cato-Servern gespeichert oder an Dritte weitergegeben. Kunden haben die Möglichkeit, vertrauliche Anwendungen, wie z. B. im Bank- und Gesundheitswesen, von der Prüfung auszuschließen.



Next Generation Firewall

Die NGFW von Cato wird auf allen Cato-PoPs eingesetzt und schützt das gesamte Unternehmen mit einer einheitlichen, anwendungs- und anwenderorientierten Sicherheitsrichtlinie – und das alles ohne die Kosten und die Komplexität, die Upgrades und Wartungen einzelner Firewallappliances mit sich bringen.

Die NGFW von Cato bietet einzigartige Vorteile:

- **Vollständige Transparenz** durch Prüfung des gesamten WAN- und Internetdatenverkehrs für alle Benutzer – vor Ort und unterwegs. Es gibt keine „toten Winkel" und somit keine Notwendigkeit, mehrere Sicherheitsappliances oder -tools einzusetzen.
- **Unbegrenzte Skalierbarkeit** durch die Anwendung von Sicherheitsrichtlinien und die Prüfung des gesamten kombinierten Datenverkehrs (verschlüsselt und unverschlüsselt) bei Leitungsgeschwindigkeit. Es wird sichergestellt, dass die Verarbeitungsleistung und die Netzwerkkapazität stets den vereinbarten Service-Levels entsprechen.
- **Einheitliche Sicherheitsrichtlinien**, die die Durchsetzung von genau definierten Richtlinien und Regeln benutzerbezogen aber auch unternehmensweit ermöglichen. Das Regelwerk ist für sämtliche Sicherheitsfunktionen und Datenverkehrstypen gleich. Daher ist es nicht notwendig, die Richtlinien mit verschiedenen Appliances oder Punktlösungen zu verknüpfen.
- **Einfache Lebenszyklusverwaltung** ohne erforderliche Dimensionierungen, Upgrades, Patches oder Aktualisierungen von Firewalls. So werden Kunden von ständigen Routineaufgaben entlastet, bei denen sie ihre Netzwerksicherheit gegen aufkommende Bedrohungen und für neue Geschäftsanforderungen auf dem neuesten Stand halten müssen – ohne dafür einen Telekommunikationsanbieter zu bezahlen.

Secure Web Gateway

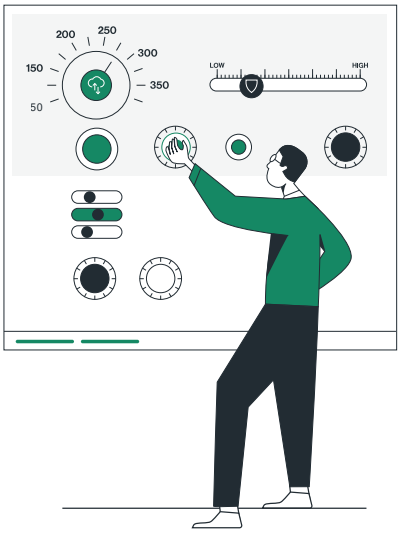
Secure Web Gateways (SWGs) bieten Schutz gegen Phishing, Schadsoftware und andere Bedrohungen aus dem Internet. Cato kombiniert SWG mit NGFW und macht es so überflüssig, Richtlinien für verschiedene Punktlösungen und den Lebenszyklus von Appliances einzurichten. Das integrierte SWG von Cato bietet eine **dynamische Sitekategorisierung** mit einer stets aktuellen URL-Datenbank, die mit Informationen über Phishing-Bedrohungen, Malware, Botnets und andere schadhafte Inhalte angereichert ist. Zudem können Kunden **verschiedene Webzugriffsrichtlinien** für mobile und standortgebundene Benutzer **festlegen und durchsetzen**, die sich auf **Informationen über die Benutzeraktivitäten** stützen, und so das **Unternehmensrisiko verringern**.

Advanced Threat Prevention

Bei Advanced Threat Prevention handelt es sich um eine Sammlung von Netzwerksicherheits- und damit verbundenen Schutzmaßnahmen, die zur Abwehr aktueller und neuer Bedrohungen eingesetzt werden. IT-Abteilungen stehen vor der schwierigen Aufgabe, eine komplexe Infrastruktur so zu verwalten, dass neuartige Bedrohungen identifiziert werden und verhindert wird, dass sie in das Netzwerk eindringen. Die Advanced Threat Prevention-Komponente von Cato löst dieses Problem, indem verschlüsselter und unverschlüsselter Datenverkehr bei Leitungsgeschwindigkeit auf Schadsoftware und Netzwerkbedrohungen überprüft wird.

TLS-Prüfung
Da der meiste Internetdatenverkehr verschlüsselt ist, spielt das Erkennen und Abwehren von Bedrohungen, die im SSL-/TLS-Datenverkehr übertragen werden, eine entscheidende Rolle. Die direkte Überwachung des SSL-/TLS-Datenverkehrs verschlingt jedoch einen beträchtlichen Teil der Rechenressourcen. Für appliancebasierte Sicherheitslösungen sind die Ressourcen aufgrund der oft unzureichenden Hardware begrenzt, sodass Hardwareupgrades außerhalb des vorgegebenen Budgetrahmens erforderlich sind. Wie bereits erwähnt, kommt den Sicherheitsservices von Cato die unendliche Rechenleistung der Cloud zugute. Cato prüft alle TLS-verschlüsselten Datenströme ohne dabei das Benutzererlebnis oder die Anwendungsleistung zu beeinträchtigen.

Schutz vor Schadsoftware Der netzwerkbasierte Schutz vor Schadsoftware nutzt mehrere, mehrschichtige und nahtlos integrierte Antischadsoftware-Engines, die in allen Cato-PoPs ausgeführt werden. Die erste Schicht umfasst eine auf Signaturen und Heuristik basierende Kontroll-Engine, die durch weltweite Bedrohungsdatenbanken stets auf dem neuesten Stand gehalten wird und Dateien während der Übertragung über das Cato-Backbone-Netzwerk zum Schutz vor bekannter Schadsoftware prüft. In der zweiten Schicht werden bewährte Machine Learning-Algorithmen von SentinalOne eingesetzt, um unbekannte Schadsoftware zu identifizieren und zu blockieren. Dazu gehören beispielsweise Zero-Day-Angriffe oder vielschichtige Varianten bekannter Bedrohungen, die darauf ausgelegt sind, signaturbasierte Kontroll-Engines zu umgehen. Dank dieser beiden Schichten sind die verbundenen Endpunkte umfassend vor über das Netzwerk eingeschleuster Schadsoftware geschützt.



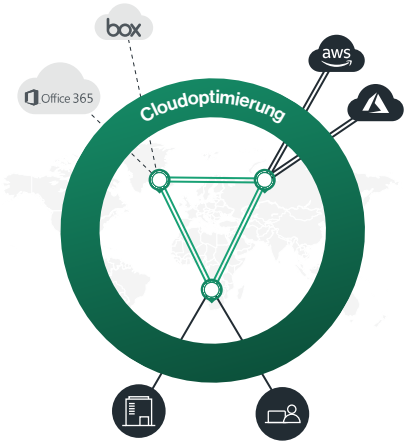
Eindringschutz
Die IPS-Lösung von Cato nutzt mehrere Schichten und Technologien, um Netzwerkangriffe erfolgreich abzuwehren. **Durch die** Validierung von Netzwerkprotokollen werden Protokollmanipulationen und beschädigte Pakete erkannt. **Kontextbezogene Signaturen und Regeln** blockieren Angriffe anhand bekannter CVEs, unbekannte Angriffe anhand des Verhaltens des Netzwerkdatenverkehrs und Netzwerkprüfungen. Interne und externe **Zuverlässigkeits-Feeds** erweitern die Informationen der IPS-Komponente. **Geografische Einschränkungen** grenzen die Bedrohungslandschaft zusätzlich ein.

Die veraltete IPS-Technologie setzt umfassende Fachkenntnisse voraus und bringt einen hohen Verwaltungsaufwand mit sich. IT-Mitarbeiter müssen neue Signaturen bewerten, entscheiden, welche davon aktiviert werden, sicherstellen, dass sie die Geschäftsabläufe nicht unterbrechen, und die Auswirkungen auf die Leistung der IPS-Appliance und des Netzwerks berücksichtigen. All diese Überlegungen müssen bei der IPS-Lösung von Cato nicht mehr angestellt werden. Wie alle anderen Cato-Sicherheitsservices wird auch die Cato-IPS-Lösung durch das Cato Security Research Lab und das SOC für Sie verwaltet und so gewährleistet, dass entsprechende Regeln gegen neu auftretende Bedrohungen mit den richtigen Maßnahmen für die Validierung und Kapazitätsanalyse angewendet werden. Die Aktivierung ist ganz einfach. Cato-Kunden müssen die IPS-Komponente lediglich über ihre Verwaltungskonsole aktivieren und können schon die Vorteile der leistungsstarken Präventionsfunktionen nutzen.

Cloud- und Mobilzugriff und Optimierung

Integration von Cloudrechenzentren

Cloudrechenzentren werden mit Cato mühelos und eng in das SD-WAN eingebunden. Alle Cloudprovider – Amazon AWS, Microsoft Azure, Google Cloud und andere – verbinden sich mit dem globalen Cato-Backbone-Netzwerk über redundante IPsec-Tunnel, die normalerweise nur das mit dem Cato-PoP gemeinsam genutzte physische Rechenzentrum passieren müssen.



Auf diese Weise bietet Cato das bestmögliche Clouderlebnis. Der Datenverkehr von Cloudrechenzentren wird über den optimalen Pfad über das globale private Cato-Backbone-Netzwerk zum Cato-PoP geleitet. Von dort werden die Daten in der Regel über das Rechenzentrumsnetzwerk an das Cloudrechenzentrum gesendet. Diese Architektur macht Premiumdienste für Cloudlösungen wie AWS Direct Connect oder Microsoft Azure ExpressRoute überflüssig.

Die Integration erfolgt **ohne Agents und erfordert keine virtuellen Appliances.** Durch die Nutzung der IPsec-Gatewayverbindung die von allen Cloudprovidern zur Verfügung steht, werden zusätzliche VM-Kosten sowie das Risiko von Änderungen an den Netzwerkkonfigurationen der Produktionsserver vermieden. Wie jeder andere Datenverkehr unterliegt auch der aus Cloudrechenzentren einer vollständigen Sicherheitskontrolle durch die Cato-Sicherheitsservices.

Schnellerer Cloudzugriff

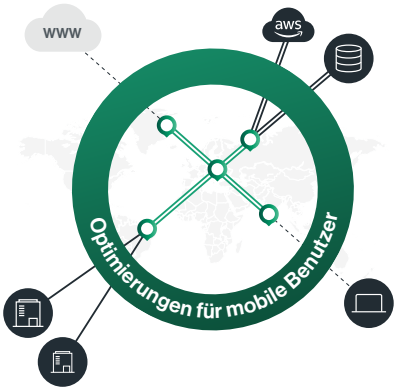
Auch die Leistung von öffentlichen Cloudanwendungen wie Office 365, Cloud ERP, UCaaS und Cloud Storage wird dank der Cato-Lösung verbessert. Zudem werden Latenzen reduziert, indem der Datenverkehr von Cloudanwendungen optimal über das globale private Backbone-Netzwerk von Cato zu dem Cato-PoP geleitet wird, der dem Rechenzentrum des Cloudproviders am nächsten liegt.

Die integrierte WAN-Optimierung von Cato sorgt für maximalen End-to-End-Throughput, um so die Anwendungsleistung, insbesondere bei bandbreitenintensiven Vorgängen wie Dateiübertragungen, zu verbessern.

Der gesamte Datenverkehr und alle Dateien, die mit der Cloudanwendung ausgetauscht werden, unterliegen innerhalb von Cato Cloud einer vollständigen Sicherheitskontrolle.

Optimierungen für mobile Benutzer

Das gesamte Angebot der Netzwerk- und Sicherheitsfunktionen von Cato umfasst einfach alles – selbst mobile Benutzer.

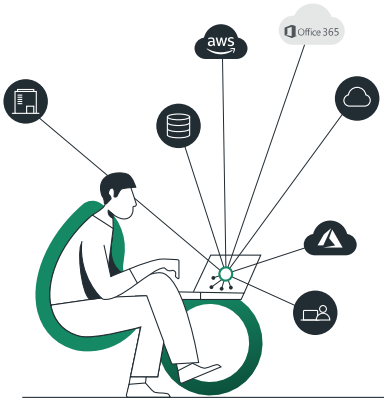


Über einen Cato-Client oder einen clientlosen Browserzugang stellen Benutzer eine Verbindung zum nächstgelegenen Cato-PoP her, sodass ihr Datenverkehr optimal über das globale private Backbone-Netzwerk von Cato zu Anwendungen vor Ort oder in der Cloud geleitet wird.

Das **Zero-Trust-SDP-Modell** (Software Defined Perimeter) von Cato für die mobile Anbindung ermöglicht eine sehr genaue Steuerung des Benutzerzugriffs – sogar für einzelne Anwendungen. Im Gegensatz dazu beschränken bisherige VPN-Lösungen den Zugriff auf ganze Subnetze.

Sämtliche Benutzeraktivitäten sind durch den integrierten Netzwerk-Security-Stack der Cato-Lösung geschützt, wodurch alle Benutzer überall auf der Welt von dem unternehmensweiten Schutz profitieren.

Verwaltungsanwendung von Cato



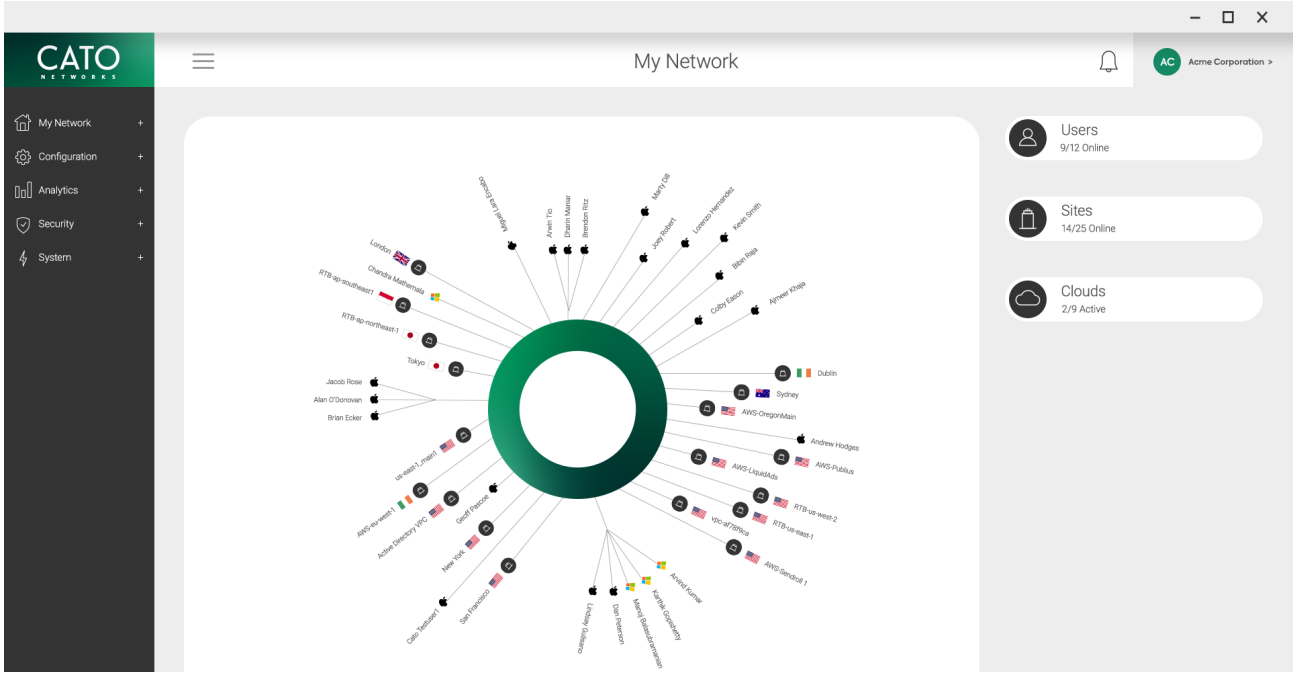
Cato bietet mit seiner cloudbasierten Verwaltungsanwendung eine zentrale Schnittstelle zum gesamten Unternehmensnetzwerk und bietet darüber Netzwerk- und Sicherheitsfunktionen für alle Standorte, Cloudressourcen und mobilen Benutzer. Über die Anwendung können Kunden und Anbieter das gesamte Serviceangebot steuern, einschließlich der Konfiguration von Netzwerk- und Sicherheitsrichtlinien, der detaillierten Netzwerkanalyse und der Berichterstattung über sicherheitsrelevante Ereignisse.

Die Cato-Verwaltungskonsole kombiniert Leistungsstärke und Benutzerfreundlichkeit. Administratoren definieren konkrete Netzwerk- und Sicherheitsrichtlinien ohne lange Lernkurve oder sich wiederholende manuelle Eingriffe, die jetzt durch eine intuitive Benutzeroberfläche vereinfacht werden.

Analysen und Berichte in Echtzeit und im Verlauf bieten umfassende Netzwerktransparenz und helfen, die wichtigsten Herausforderungen in den Bereichen Zugriffssteuerung, Benutzerfreundlichkeit, Problembehebung und Schatten-IT zu lösen.

Die Sammlung und Bereitstellung vollständiger Netzwerk- und Sicherheitsereignisprotokolle für externe Analyselösungen wie SIEM bietet den einzigartigen Vorteil, dass für alle Ereignisse nur eine einzige Schnittstelle verwendet wird, anstatt Daten aus mehreren Appliances und Quellen manuell zusammenführen zu müssen.

Die Verwaltungsanwendung ist webbasiert und online über eine mehrstufige Authentifizierung verfügbar. Alle Zugriffs- und Konfigurationsänderungen werden in einem zentralen Überwachungsprotokoll aufgezeichnet.



Die Cato-Verwaltungskonsole fungiert als zentrale Schnittstelle, in der alle verbundenen Standorte, Cloudressourcen und Benutzer angezeigt werden.

Managed Services

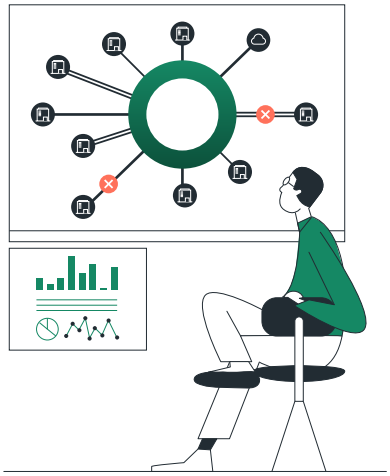
Abhängig vom Verwaltungsmodell, das die Kundenanforderungen am besten erfüllt, bietet Cato ein entsprechendes Managed Services-Paket. In jedem Fall verwaltet Cato die zugrundeliegende Plattform und befreit Kunden von den Kosten und der Komplexität, die mit der Skalierung, den Upgrades und der sonstigen Verwaltung der Netzwerk- und Sicherheitsinfrastruktur verbunden sind.

Beim Self-Service-Management liegt die Kontrolle aller Aspekte ihrer eigenen Netzwerke auf Kundenseite. Im Rahmen des Co-Managements können Kunden Konfigurations- und Fehlerbehebungsaufgaben an das Cato-NOC (Netzwerkbetriebszentrum) oder einen regionalen Partner delegieren. Beim kompletten Managed Service liegt die Überwachung und Verwaltung des Kundennetzwerks im Verantwortungsbereich eines regionalen Partners.

Die verschiedenen Verwaltungsmodelle sind ein einzigartiger Vorteil von Cato gegenüber herkömmlichen Telekommunikationsanbietern und Anbietern von verwalteten Netzwerkdiensten, bei denen die Kunden für jede Änderung am Netzwerk ein Ticket öffnen müssen. Zusätzlich zur Unterstützung bei der Bereitstellung vor Ort bieten Cato und seine Partner die folgenden Managed Services an:

Intelligente Verwaltung der letzten Meile

Cato bietet Kunden einen Premium-Service zur kontinuierlichen Überwachung von ISPs auf der letzten Meile. Im Falle eines Ausfalls (Blackout) oder einer Leistungsbeeinträchtigung (Brownout) arbeitet Cato gemeinsam mit dem ISP an der Lösung des Problems, indem sachdienliche und detaillierte Netzwerkinformationen rund um den Vorfall zur Verfügung gestellt werden. Dank dieses Service können Kunden, die von einem vollständig verwalteten MPLS-Netzwerk migriert sind, Netzwerkprobleme bei ihren verschiedenen, weltweiten ISPs schnell lösen, ohne wertvolle interne IT-Ressourcen zu beanspruchen.



Managed Threat Detection and Response

Wie zuvor erwähnt, bietet Cato Kunden einen Premium-Service zur kontinuierlichen Überwachung ihre Netzwerke für betroffene Endpunkte.

Präventivmaßnahmen reichen nicht mehr aus, um das Unternehmensnetzwerk zu schützen. Für die lückenlose Verteidigung gegen neuartige Angriffe ist deren Erkennung von entscheidender Bedeutung. Solche Managed Threat Detection and Response (MDR)-Services sind jedoch oft mit hohen Kosten und einer sehr komplexen Bereitstellung verbunden.

Der MDR-Service von Cato nutzt die tief gehende Transparenz des Cato-Netzwerks, um eine Zero-Footprint-Erkennung vorhandener Bedrohungen durch eine Kombination aus Machine Learning-Algorithmen, die den Netzwerkverkehr überwachen, und einer menschlichen Überprüfung der erkannten Anomalien zu ermöglichen. Anschließend leiten Cato-Experten Kunden bei der Problembehebung an den kompromittierten Endpunkten an.

Verwaltung ohne Benutzereingriff

Kunden können sich dafür entscheiden, die vollständige Verwaltung ihres Netzwerks Cato oder einem Cato-Partner zu überlassen. Änderungsanforderungen werden über ein Ticketportal eingereicht, nachverfolgt und entsprechend dem Cato-SLA bearbeitet. Daraufhin führen fachkundige Mitarbeiter alle Änderungen an den Netzwerk- und Sicherheitsrichtlinien nach Bedarf durch, um den geschäftlichen und technischen Anforderungen gerecht zu werden.

Anwendungsfälle

MPLS-Migration zur SD-WAN-Lösung

Mit der Cato-Lösung können Kunden von kostspieligen, unflexiblen und kapazitätsbeschränkten MPLS-Netzwerken auf mehrere Hochleistungs-Internetverbindungen und die Cato-Funktionen zur Optimierung für die letzte und mittlere Meile umsteigen. Durch den Einsatz des Edge-SD-WAN von Cato erhöhen Kunden die nutzbare Kapazität und verbessern die Ausfallsicherheit bei geringeren Kosten pro Megabit. Für Kunden mit globaler Präsenz eignet sich das erschwingliche, globale private Backbone-Netzwerk von Cato, um das weltweite MPLS und unzuverlässige Internetverbindungen zu ersetzen, die Leistung zu optimieren und den Throughput von Ressourcen vor Ort und in der Cloud zu maximieren.

Intelligente globale Vernetzung

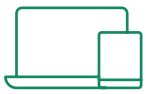
Zur Bereitstellung eines SLA-gestützten, zuverlässigen und leistungsstarken Netzwerks – das standortunabhängig ist – setzt Cato ein globales privates Backbone-Netzwerk mit integrierter WAN- und Cloudoptimierung ein. Kunden, die Probleme mit hohen Latenzen und Netzwerkunregelmäßigkeiten an ihren globalen Standorten haben, nutzen das Cato-System, um das Benutzererlebnis beim Zugriff auf lokale und Cloudanwendungen erheblich zu verbessern.

Sicherer Internetzugang für Niederlassungen

In Cato Cloud ist ein kompletter Netzwerk-Security-Stack integriert. Durch die Verbindung aller Standorte mit dem globalen privaten Backbone-Netzwerk von Cato über das Cato-Edge-SD-WAN ist der gesamte Datenverkehr des Unternehmens im Internet und im WAN durch die Security-as-a-Service-Lösung von Cato vollständig geschützt. Die Einbindung zusätzlicher kostenintensiver und komplexer Punktsicherheitslösungen, Appliances oder Cloudservices ist somit hinfällig.

Schnellerer und sicherer Cloudzugriff

Cato beschleunigt den Cloudzugriff, indem der gesamte Clouddatenverkehr an den Cato-PoP weitergeleitet wird, der dem Cloudziel am nächsten liegt. Da Cato-PoPs die Leistungsstärke der Rechenzentren großer Cloudprovider teilen, ist die Latenz zwischen Cato und diesen Providern im Grunde genommen gleich Null. Für die Optimierung des Cloudzugriffs wird nur eine einzige Regel auf Anwendungsebene benötigt, die festlegt, wo der Datenverkehr von Cloudanwendungen die Cato Cloud-Lösung verlassen soll. Aufwendige und kostspielige Bereitstellungen von Cloudappliances oder Einrichtungen regionaler Kommunikationsknoten, um das SD-WAN auf die Cloud auszuweiten, gehören endlich der Vergangenheit an.



Sicherer und reibungsloser Mobilzugriff

Die globalen Netzwerk- und Sicherheitsfunktionen von Cato erstrecken sich sogar auf den Laptop, das Smartphone oder das Tablet eines einzelnen mobilen Benutzers. In Ihrer Netzwerk- und Sicherheitsinfrastruktur sind mobile Benutzer endlich mit anderen Benutzern gleichgestellt. Über einen Cato-Client oder einen clientlosen Browserzugang stellen die Benutzer eine Verbindung zum nächstgelegenen Cato-PoP her, sodass ihr Datenverkehr optimal über das globale private Backbone-Netzwerk zu Anwendungen vor Ort oder in der Cloud weitergeleitet wird. Die Security-as-a-Service-Komponente der Cato-Lösung schützt mobile Benutzer überall vor Bedrohungen und setzt die Zugriffssteuerung für Anwendungen durch.

Cato Cloud: vollständige WAN-Transformation

Das Ersetzen von MPLS und veralteten WANs ist nicht einfach nur eine Möglichkeit, schnelle und kostengünstige Verbindungen zwischen Niederlassungen zu nutzen. Es ist die Gelegenheit, das gesamte Unternehmen zu revolutionieren, indem jeder Benutzer mit jeder Ressource auf der ganzen Welt verbunden wird. Einige Unternehmen sind diesen Schritt bereits gegangen und haben nicht nur Upgrades, sondern eine völlige Umstrukturierung Ihrer Netzwerke durchgeführt. Das Ergebnis kann sich sehen lassen: erheblich geringere WAN-Kosten bei gleichzeitiger **Verdopplung des Throughputs und immer mehr Standorten**, eine bemerkenswerte **Verkürzung der Bereitstellungszeiten von Monaten auf nur 30 Minuten und die Identifizierung von Bedrohungen in ihren Niederlassungen, die von den bestehenden Sicherheitsanwendungen übersehen wurden.**

Zugegeben, dies ist eine drastische Maßnahme – aber die Zukunft beginnt jetzt. Hunderte unserer Kunden nutzen bereits die Vorteile der Cato Cloud-Lösung. **Überzeugen Sie sich selbst, und vereinbaren Sie noch heute einen Gesprächstermin.**

Weitere Informationen:

www.catonetworks.com

@catonetworks

Womit möchten Sie beginnen?

MPLS-Migration zur SD-WAN-Lösung

Sicherer Internetzugang für Niederlassungen

Optimierter und sicherer Zugriff für mobile Benutzer

Intelligente globale Vernetzung

Optimierter und sicherer Cloudzugriff