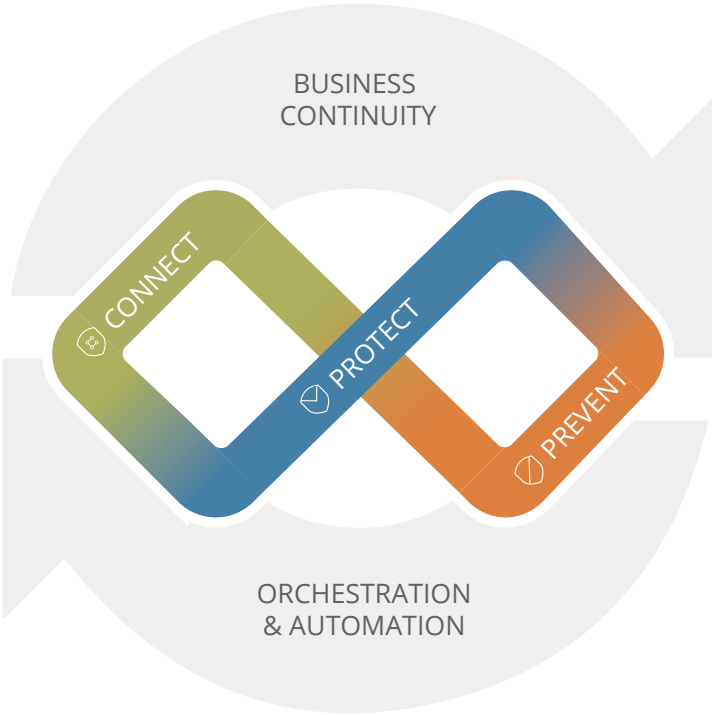
The Clavister Aurora Security Framework

clavister®

CONNECT. PROTECT

Die neue Art des Sicherheitsmanagements beginnt mit einem ganzheitlichen Ansatz



Clavister Aurora Sicherheits-Rahmenwerk

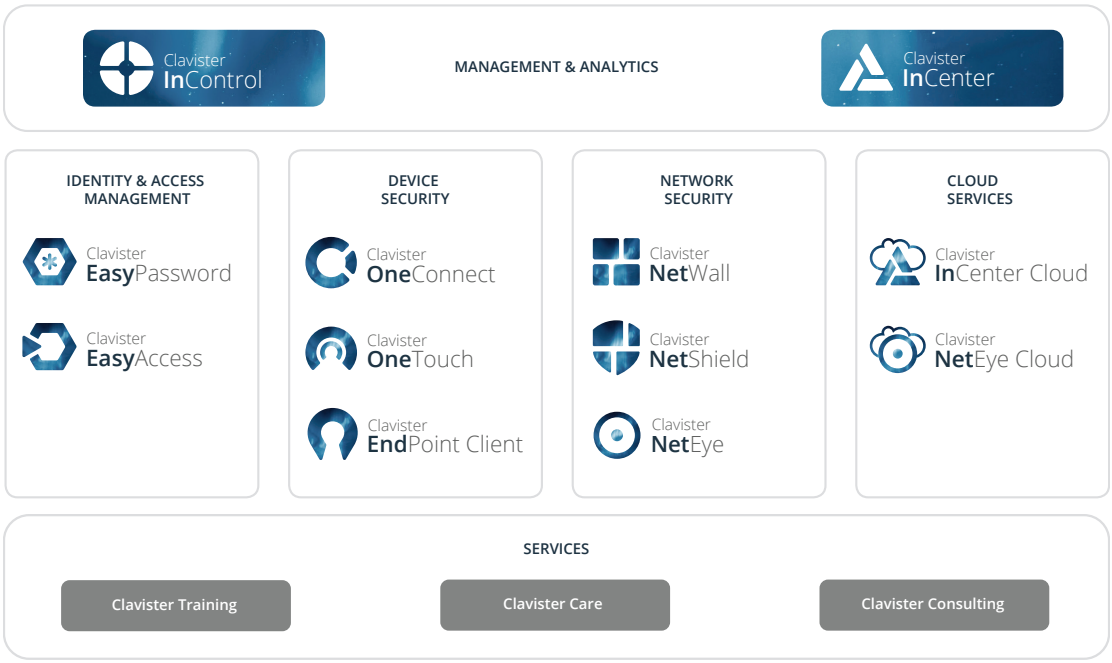
Sicherheit war in der Vergangenheit eine einfache Angelegenheit: Eine UTM-Appliance kaufen, Netzwerk segmentieren und Protokolldaten verwalten. So war das früher. Aber das war damals. Heute müssen Sie für eine robuste Cybersicherheit des 21. Jahrhunderts nicht nur Ihr Netzwerk schützen, sondern auch Endpunkte verwalten, den Zugriff auf die Cloud sichern und die Identität der Benutzer überprüfen, die auf das Netzwerk, die Anwendung und die Informationssysteme zugreifen. Und dabei benötigen Sie die besten Management- und Analysetools, um über die Bedrohungen auf dem Laufenden zu bleiben und die operative Leistungsfähigkeit Ihres Unternehmens zu schützen.

Wie machen Sie das? Durch den Einsatz eines Portfolio-Ansatzes, durch die Anwendung eines intelligenten Ökosystems von Produkten und Lösungen zur Bewältigung der Herausforderungen. Sie tun dies, indem Sie innovative Lösungen von Clavister's Aurora Security Framework einsetzen, die Hand in Hand miteinander arbeiten.

Mit den Produkten und Lösungen von Clavister setzen Sie einige oder viele Use Cases in den Bereichen Connect, Protect und Prevent ein. Vernetzung von Unternehmensstandorten untereinander und mit dem Internet, mit Fokus auf Sicherheit und Zuverlässigkeit. Überprüfen Sie den Traffic und das Verhalten des Traffics auf Bedrohungen, um Ihre digitalen Assets zu schützen. Und die Aktivierung präventiver Sicherheitsmaßnahmen und -regeln, die das Risiko von Fehlern der Benutzer bei der Bedrohung oder Gefährdung des digitalen Perimeters Ihres Unternehmens verringern können.

Orchestriert und automatisiert arbeiten die Use Cases mit dem Fokus zusammen, um Ihnen Business Continuity zu bieten.

Product Portfolio



Sicherheits-Use-Cases

Unsere robusten Produkte sind die perfekten Plattformen für das, was unsere wahre Leidenschaft ist: Innovative Software, die unseren Kunden die besten Anwendungslösungen liefert. Ob es sich nun um unsere exzellenten VPNs oder um Anwendungsfälle zur Verkehrsoptimierung handelt, Sie können sicher sein, dass Ihre Clavister Sie in Verbindung hält, schützt und Schäden verhindert, die in Ihr Unternehmen eindringen.

CONNECT

Zuverlässiges & sicheres VPN
Anbindung von Niederlassungen und entfernten Standorten sicher und kostengünstig umsetzen

Routing & Load Balancing
Vermeiden Sie Ausfallzeiten und sichern Sie Ihre Geschäftskontinuität durch Redundanz

Sichere Netzwerkzonen
Netzwerksegmentierung zum Schutz der digitalen Unternehmensressourcen

Server Load Balancing
Vereinfachung der Skalierung und Ermöglichen einer präventiven Wartung

Sicherer Fernzugriff
Ermöglicht Remote-Mitarbeitern und -Geräten einen flexiblen und sicheren Zugriff

Single Sign-On
Schnelle, sichere Anmeldung an Ihren Apps, VPNs und Cloud Services

Stabile Verbindungskonnektivität
Vernetzung mit dem Border Gateway Routing (BGP) für Carrier-Unabhängigkeit

Carrier Grade NAT
Leistungsstarke IPv4 - IPv6 Netzwerk-Adressübersetzung

PROTECT

Firewalling
Netzwerk-Firewall zur Absicherung der IT-Ressourcen und Benutzer

Schutz vor Netzwerkangriffen
Einbruchserkennungs- und -vermeidungs-System (IDS/IPS) und Denial of Service-Schutz (DoS)

Antiviren-Überprüfung
Kontinuierlicher Scan von Anhängen in E-Mails, Web- und Datei-Downloads nach bösartigen Inhalten

Endbenutzer-Gerätesicherheit
Blockieren von Bedrohungen und Erkennen von Datenverlusten an Endgeräten

Control Signalling Validation
Gateway-Funktion für spezifische Signalisierungs-Validierung einschließlich DNS, SIP, GTP und SCTP

Sicherer Server-Schutz
Entschlüsselung des Server-Traffics für die vollständige Inspektion des eingehenden Verkehrs

PREVENT

Anwendungssichtbarkeit & Kontrolle
Kontrolle von Anwendungen und Benutzerverhalten zur Optimierung der Nutzung von Netzwerkressourcen

Web Content Filtering
Beschränken Sie den Zugriff auf unangemessene Inhalte und gefährliche Webseiten

Aktive Traffic-Optimierung
Traffic-Priorisierung sichert die gewünschte Verteilung von Ressourcen

Multi-Faktor-Authentifizierung
Eine Plattform, welche die Authentizität von Endanwendern für Cloud-/ Webanwendungen, VPN's etc. sichert

Password Self Service
Ermöglicht Endbenutzern die Verwaltung von Firmenpasswörtern

Captive Portal-Authentifizierung
Integration ins Active Directory- sowie 2FA-Verfahren für den offenen Netzzugang

Botnetz-Blockierung
Blockieren von ausgehendem und eingehendem Datenverkehr durch IP-Reputation

Benutzerverifizierung
Einfache On-Demand-Validierung der Identität des Endbenutzers

Clavister InCenter

Aber die meisten Unternehmen befassen sich erst mit den Fakten, wenn es bereits zu spät ist... der Ansatz ist reaktiv. Was also fehlt, ist eine klare Sicht auf das, was vor sich geht ... in Echtzeit, um die notwendigen Maßnahmen ergreifen zu können.

In dem Moment macht sich Clavister InCenter an die Arbeit. Mit unserer webbasierten Echtzeit-GUI, die auf maschinellem Lernen basiert, bietet dieses Tool IT-Managern eine ganzheitliche Sicht auf Bedrohungen und Datenverkehr mit Drill-Down-Funktionen zur Erkennung von Anomalien und einfach zu verstehenden Dashboards, die die Gesamtbetriebskosten im Vergleich zu Log-Management-Systemen von Drittanbietern senken. Mit Clavister InCenter werden MSSPs und IT-Administratoren besser informiert, um ihre Sicherheit zu verbessern.

Clavister InCenter Cloud

Clavister InCenter Cloud ist mit jeder Clavister Security Subscription erhältlich. Es ermöglicht IT-Administratoren, mit sehr wenig Aufwand und ohne Hardwareinvestitionen Einblicke in Ihre Netzwerke zu erhalten. Clavister InCenter Cloud bietet alle Anwenderberichte einschließlich Forensik mit vollständiger Protokollsuche, Dashboarding, Alarmierung und Berichterstellung sowie Zustandsüberwachung.

Clavister InControl

Clavister InControl ist unser erstklassiges zentralisiertes Managementsystem, das für die Verwaltung von Tausenden von Clavister Next-Generation-Firewalls in großen Netzwerken entwickelt wurde. Die Zero-Touch Provisionierung ermöglicht es neu installierten Firewalls, automatisch den Weg zum richtigen Clavister InControl Server zu finden. Von dort aus werden direkte Managementfunktionen ein sicheres Onboarding und die Bereitstellung von Richtlinien ermöglichen. Mit integrierter Unterstützung für Reporting, Konfigurationsmanagement und Versionskontrolle ist Clavister InControl die ideale zentralisierte Managementlösung für große Unternehmen und Managed Security Service Provider.

Clavister EasyAccess

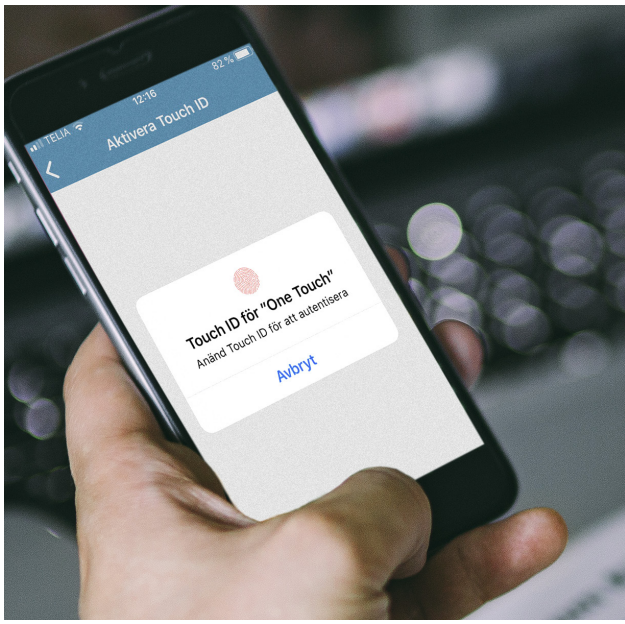
Einfache Kombinationen von Benutzernamen und Passwörtern sind einer der Hauptgründe für größere Sicherheitsvorfälle. Dieser Vorgehensweise kann man heute beim Schutz von Geschäftsanwendungen und sensiblen Daten nicht mehr trauen.

Claviser EasyAccess mit Multifaktor-Authentifizierung (MFA) bietet die nötige Sicherheit, um Ihre Umgebung vor diesen Problemen zu schützen. Durch die Nutzung von etwas, das der Benutzer bereits hat, weiß und beantworten kann, ermöglicht unsere MFA-Lösung eine nahtlose und kostengünstige Lösung zur Authentifizierung von Benutzern.

Clavister OneTouch

Clavister OneTouch ist die mobile Anwendung zur biometrischen Autorisierung jeder mehrstufigen Login-Anfrage. Dutzende von Passwörtern auf einer gleichen Anzahl von Plattformen; wie kann man sich an sie alle erinnern, ohne in die Falle zu tappen, ein gemeinsames, hackbares Passwort zu verwenden? Mit Clavister OneTouch müssen sich keine Gedanken mehr machen: Verwenden Sie einfach Ihren Daumenabdruck oder Ihre Gesichtserkennung, um alle Anwendungen und Dienste, mit denen Sie arbeiten und spielen, sicher freizuschalten.

Download on the App Store | GET IT ON Google Play



Clavister EasyPassword

Und dann ist da noch die Situation, in der wir alle schon mal waren: Unsere IT-Administratoren anrufen, damit diese uns ein neues Passwort geben, weil wir unseres nicht abrufen können oder vergessen haben. Mit Clavister's EasyPassword ist es ein Kinderspiel und das Beste daran, Sie erledigen es selbst in wenigen Minuten. Keine Scham und im Handumdrehen wieder einsatzbereit.

Clavister NetShield

SERVICE-BASED FIREWALLS

Die Service-Based Firewall (SBFW) ist ein revolutionäres Produkt, das den Bedürfnissen moderner Netzwerkbenutzer und Administratoren gerecht wird. Ideal für den Schutz von Rechenzentren und Netzwerkinfrastrukturen, die Geschwindigkeiten und Funktionen in Carrier-Qualität erfordern. Neben dem flexiblen Perimeterschutz kann das Produkt den sicheren Datenverkehr zu einer Webserver-Farm beenden und die Inspektion mit einem eingebauten Intrusion Detection System durchführen, das sowohl die Serverinfrastruktur sichert als auch entlastet. Es beinhaltet Funktionen zum Screening auf spezifische kritische Signale wie DNS, GTP und SIP und bietet Carrier-Dienste einschließlich Carrier-Grade-Netzwerkadressübersetzung und BGP-Routing-Funktionalität, die dieses Produkt ideal für den Schutz großer Netzwerke wie Campus-Netzwerke, öffentliche Wi-Fi oder mobile und feste Kommunikationsdiensteanbieter-Netzwerke machen. Clavister NetShield kann in einer Hochdurchsatz-Appliance oder virtuell optimiert für die Leistung in KVM- und VMWare-Umgebungen eingesetzt werden.

KVM vmware vSphere

CLAVISTER SECURITY SUBSCRIPTION

Den Clavister-Kunden werden zwei Arten von Dienstleistungen angeboten: Die umfassende, all-inclusive Clavister Security Subscription (CSS) oder die kostengünstige Clavister Product Subscription (CPS), die jederzeit auf das CSS aufgerüstet werden kann. Die Clavister Product Subscription (CPS) umfasst sowohl Software-Services wie Upgrades und Wartung als auch den direkten 24/7-Lieferantensupport (online, per Telefon) sowie das zentrale Managementsystem Clavister InControl. Alternativ beinhaltet die Clavister Security Subscription (CSS) alle in der Clavister Product Subscription enthaltenen Dienste mit den vollständigen Firewall- und Unified Threat Management (UTM)-Funktionen der nächsten Generation, mit Diensten wie Anti-Virus, Web Content Filtering, Intrusion Detection and Prevention (IDP), IP-Reputation-Intelligenz und echter Anwendungskontrolle. Jedes Modell der Clavister NetWall-Reihe, ob Appliance oder Virtuell, unterstützt die gleichen Anwendungsfälle und erweiterten Funktionen.

Clavister NetWall

NEXT GENERATION FIREWALLS

Hacker, Viren, Ransomware, Datendiebstahl, Industriespionage und sogar von der Regierung gesponserte Angriffe. Die Liste der Cyber-Bedrohungen, die Ihr Unternehmen gefährden könnten, wird immer länger. Hinzu kommen all die neuen Arten von Technologien wie Cloud, BYOD, WiFi und andere, die Ihr Unternehmen produktiver machen sollen.

Unsere kompakten, schnellen und leistungsstarken Desktop-Appliances liefern komplette Sicherheitsanwendungen für Remote Offices oder als CPEs. Für größere Unternehmen oder den Einsatz in der Zentrale bieten unsere rackmontierbaren Appliances selbst für die größten Unternehmen erstklassigen Schutz.

Last but not least ist Clavister seit 2008 ein Pionier bei virtuellen Produkten und benötigt nur sehr geringe Ressourcen, was es ideal für sichere Verkäufe in Cloud-Umgebungen macht.

Clavister OneConnect

Clavister OneConnect ist unser SSL VPN Client, der eine einfache und leicht zu bedienende Lösung für den Fernzugriff auf die NetWall Next Generation Firewalls von Clavister bietet.

Eine sichere Verbindung ist so einfach wie die Nutzung unseres integrierten Portals in Clavister NetWall: Herunterladen und Installieren des Clients und Sie sind bereit für die Verbindung.

Mit der Unterstützung für Microsoft Windows und Apple macOS gibt es Unterstützung für eine Vielzahl von Geräten. Zusammen mit Clavister EasyAccess bietet Clavister OneConnect ein einzigartiges One-Click-Zugriffserlebnis für den Benutzer, der mit der VPN-Konnektivität beginnt und sich bei seiner Lieblingsanwendung - SaaS oder vor Ort - einloggt.

Clavister NetEye

ADVANCED THREAT PROTECTION

Clavister NetEye ist der führende Weg, um Advanced Threat Protection zu bieten, um eingebettete SSL-Bedrohungen zu inspizieren und zu neutralisieren, indem es sie identifiziert und den Administrator über das InCenter Management Tool von Clavister alarmiert, damit er Maßnahmen ergreifen kann. Außerdem ermöglichen die Detonationsfunktionen von Clavister Sandbox Cloud, dass verdächtige Dateien und Pakete an eine sichere Cloud-Umgebung gesendet, unter Quarantäne gestellt und auf schädliches Verhalten untersucht werden, das versucht, die Sicherheit des Perimeters zu umgehen. Nach erfolgter Installation benachrichtigt die Sandbox-Cloud Clavister InCenter über die Aktivität und warnt die Netzwerkadministratoren über die Malware, um Maßnahmen im Netzwerk zu ergreifen.

Clavister NetEye ist einfach zu implementieren für jede Firewall, Clavister oder Drittanbieter und benötigt nur minimale Zeit für den Start. Es hat keinen wesentlichen Einfluss auf die Leistung der Firewall und bietet eine einfache Möglichkeit, die Skalierung über mehrere Standorte mit einem zentralen Angebot vorzunehmen. Der IT-Manager kann nun die Kosten einfach verwalten und gleichzeitig sicherstellen, dass der gesamte Datenverkehr auf Bedrohungen überprüft wird.

Clavister NetEye Cloud

Clavisters NetEye Cloud bietet eine vollständige Dekodierung und Filterung des verschlüsselten Webverkehrs. Es schützt, loggt und informiert über SSL-Webaktivitäten. Keine Client-Software erforderlich. Darüber hinaus ist Clavister NetEye Sandbox Cloud ein hervorragendes Werkzeug, um exe-Dateien in einen Inspektions- und Detonationsbereich zu bringen und dem Clavister InCenter für weitere Maßnahmen Bericht zu erstatten.

SECURITY BY SWEDEN

clavister®
CONNECT • PROTECT

Clavister GmbH • Kirchstr.23a • 31595 Steyerberg • Germany
Phone: +49 (0)89 21 09-3400 • Mail: info@clavister.de • Web: www.clavister.com