



| Success Story

Sesotec stellt seine globale Sicherheits- & Netzwerkarchitektur mit der IF-Tech auf SASE um

Wachstum und Security im Einklang

Sesotec führt gemeinsam mit der IF-Tech die SASE Cloud-Plattform von Cato ein und ersetzt so verteilte Firewall-, VPN- und Endpoint Protection-Lösungen durch eine integrierte, Cloud-native Architektur. Dadurch profitiert das Unternehmen von KI-basierter Bedrohungserkennung, automatisierten Prozessen und einheitlichen Richtlinien – über alle weltweiten Standorte und Endpoints hinweg.

Das Ziel: Schneller wachsen, ohne Kompromisse bei der Sicherheit.

Die Sesotec GmbH mit Hauptsitz im niederbayerischen Schönberg zählt zu den weltweit führenden Spezialisten für Fremdkörperdetektion, Materialsortierung und -analyse. Das Unternehmen entwickelt und produziert seit 1976 Hightech-Systeme, die in sensiblen Branchen wie der Lebensmittel-, Kunststoff- und Recyclingindustrie zum Einsatz kommen – überall dort, wo Qualität, Produktsicherheit und Effizienz entscheidend sind. Sesotec ist international aufgestellt und mit 17 Auslandsgesellschaften und über 60 Partnern weltweit präsent.

Technologisch bewegt sich Sesotec in einem hochinnovativen Umfeld. Neben klassischer Industrie- und Messtechnik spielen datengetriebene Verfahren und KI-gestützte Auswertungen eine immer größere Rolle. Entsprechend hoch sind die Anforderungen an den Schutz von Know-how, Entwicklungsdaten und sensiblen Kundeninformationen.

Die Kombination von hohen Sicherheitsstandards und dynamischem Geschäftswachstum stellte die IT-Organisation von Sesotec zunehmend vor Herausforderungen. Wenn das Unternehmen einen neuen Standort eröffnete, benötigten die Anwender möglichst kurzfristig sicheren Zugriff auf alle zentralen Anwendungen und Daten.

„Wir als IT-Abteilung waren dabei oft der limitierende Faktor. Für jede neue Niederlassung mussten wir erst Firewalls beschaffen, VPNs einrichten und Sicherheitsregeln definieren. Das war zeitaufwändig und passte nicht mehr zu der Geschwindigkeit, mit der sich unser Unternehmen entwickelt.“

~ Alexander Graßl,
Head of IT, Sesotec



Der Weg zu einer modernen SASE-Architektur

Auf der Suche nach einer zukunftsfähigen Strategie wandte sich Sesotec an seinen langjährigen IT-Partner IF-Tech. Statt neuer Einzelprodukte von unterschiedlichen Anbietern brachten die Experten der IF-Tech schnell ein grundlegend anderes Konzept ins Spiel. Sie empfahlen Sesotec, Netzwerk- und Security-Funktionen in einer integrierten, Cloud-basierten Architektur zusammenzuführen – nach dem Prinzip des Secure Access Service Edge (SASE). Verteilte Standorte, Cloud-Anwendungen und mobile Endpoints werden bei diesem Modell über eine zentrale Plattform abgesichert und vernetzt.

„Die Idee, Netzwerk- und Security-Funktionen zentral aus der Cloud bereitzustellen, hat für uns sofort Sinn ergeben“, sagt Alexander Graßl. „Uns war vor allem wichtig, dass wir den operativen Aufwand reduzieren und weltweit einheitliche Sicherheitsstandards etablieren können.“

Für die technische Umsetzung dieses Ansatzes schlugen die Experten der IF-Tech die SASE Cloud-Plattform von Cato Networks vor. Die Plattform bündelt Funktionen wie SD-WAN, Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG) und Zero Trust Network Access (ZTNA) in einer Cloud-nativen Architektur und ersetzt damit klassische, standortgebundene Punktlösungen. Cato gehört zu den Vorreitern auf dem Markt für SASE-Lösungen und wird im Gartner Magic Quadrant als Leader geführt. Auch die IF-Tech setzt die Plattform schon seit einiger Zeit erfolgreich in Projekten ein und konnte so entsprechende Praxiserfahrung einbringen.

Die Bewährungsprobe für die Lösung erfolgte mit der Anbindung des ersten Standorts. Für das Pilotprojekt wählte Sesotec eine neu gegründete Niederlassung in Indien. Um die neue Niederlassung anzubinden, musste das Projektteam lediglich ein Cato Socket Device vor Ort einrichten.



Dieses verbindet sich automatisch über den nächstgelegenen Point of Presence (PoP) mit dem globalen Backbone von Cato. Durch redundante WAN-Verbindungen im Socket ist dabei jederzeit eine zuverlässige Konnektivität zwischen dem lokalen Standort und den zentralen Cloud Services sichergestellt.

„Unter den bisherigen Bedingungen wäre das für uns mit erheblichem Aufwand verbunden gewesen. Mit der Cato-Plattform und der Unterstützung der IF-Tech konnten wir den neuen Standort aber in kürzester Zeit in Betrieb nehmen. Von der Entscheidung bis zur Umsetzung vergingen nur wenige Wochen“

~ Alexander Graßl, Head of IT, Sesotec

Die Vorteile im Fokus: Effizienz und maximale Sicherheit

Schneller Rollout und Ablösung von Einzelprodukten.

„Im Pilotprojekt haben wir gesehen, dass die Lösung von Cato im realen Betrieb wirklich gut funktioniert“, berichtet Alexander Graßl. „Wir hatten von Anfang an eine sehr stabile Anbindung und konnten alle Sicherheitsrichtlinien und Netzwerkeinstellungen für die neuen Niederlassungen über die zentrale Management-Oberfläche konfigurieren. Die gesamte Intelligenz der Cato-Plattform liegt ja letztlich in der Cloud.“

Schritt für Schritt stellte Sesotec anschließend auch die weiteren Unternehmensstandorte auf die neue SASE-Architektur um und löste damit vorhandene Firewall-, VPN- und Endpoint Protection-Lösungen ab. Dank der Zero Touch-Installation von Cato waren für die Umstellung praktisch keine Vor-Ort-Einsätze erforderlich. Sobald ein Socket Device an das Internet angeschlossen ist, erscheint es automatisch in der Cato Management App und kann sofort einem Standort zugewiesen werden.



Um auch mobile Anwender zu integrieren, wurde der Cato Client auf rund 700 Endgeräten ausgerollt. Dieser ermöglicht sicheren Remote-Zugriff auf alle benötigten Geschäftsanwendungen und schützt die Endgeräte gleichzeitig zuverlässig vor Malware, Ransomware und anderen Cyberrisiken. „Egal, ob unsere Beschäftigten in der Zentrale, in einer internationalen Niederlassung oder im Homeoffice arbeiten: An jedem Ort greifen heute dieselben Sicherheitsrichtlinien“, betont Alexander Graßl.

Sesotec profitiert zudem von der engen Verzahnung von Sicherheits- und Netzwerktechnologie innerhalb der Cato-Plattform. Funktionen wie WAN-Optimierung, intelligentes Routing zum nächstgelegenen PoP sowie integriertes Failover sorgen für stabile Verbindungen und eine hohe Verfügbarkeit – auch in Regionen mit weniger zuverlässiger Netzanbindung.

Sicherheit der nächsten Generation – proaktiv, integriert, KI-gestützt.

Mit der Cato-Plattform hat Sesotec die Sicherheit und Verfügbarkeit der gesamten Infrastruktur immer im Blick. „Wir sehen heute sehr genau, was in unserem Netzwerk passiert, welche Zugriffe blockiert werden und wo möglicherweise Optimierungspotenzial besteht“, sagt Alexander Graßl. „Die Cato Management App liefert uns unter anderem Echtzeitinformationen und historische Auswertungen zu Bedrohungen, Netzwerkleistung und der Nutzung spezifischer Anwendungen.“

Mit wenigen Klicks kann das IT-Team heute auch den Ursachen von Fehlermeldungen und Sicherheitswarnungen auf den Grund gehen. Kurz nach der Implementierung der Plattform schlug etwa das Intrusion Detection System (IDS) von Cato Alarm. Es hatte verdächtige Zugriffe auf Sesotec-Systeme in den USA registriert und blockiert. Letztlich stellte sich heraus, dass diese durch ein Tool für Penetrationstests ausgelöst wurden.

Für die Erkennung von Anomalien und die bessere Absicherung der Umgebung nutzt die Cato-Plattform inzwischen zunehmend künstliche Intelligenz (KI). Die Plattform analysiert kontinuierlich Netzwerkverkehr, Benutzerverhalten und Sicherheitsereignisse, korreliert diese Daten miteinander und erkennt dadurch auch ungewöhnliche Muster oder verdächtige Aktivitäten, die mit klassischen, regelbasierten Systemen kaum aufzuspüren wären.

KI-gestützte Mechanismen bewerten darüber hinaus die Sicherheit der genutzten Anwendungen. Steigt der Risiko-Score einer Applikation – etwa aufgrund neu entdeckter Schwachstellen –, kann der Zugriff automatisch eingeschränkt oder blockiert werden. Für Sesotec bedeutet das einen deutlich verbesserten Schutz vor bislang unbekanntem Bedrohungen und Zero-Day-Attacken.

Die Cato-Plattform kann zudem Risiken eindämmen, die durch die unkontrollierte Nutzung von generativer KI entstehen – Stichwort „Schatten-KI“. Mit Hilfe der Data Loss Prevention (DLP)-Funktionen von Cato verhindert Sesotec beispielsweise, dass sensible Informationen wie Konstruktionspläne oder interne Dokumente in öffentlich zugängliche KI-Tools hochgeladen werden. „Gerade im Kontext von KI gibt uns das ein gutes Gefühl“, unterstreicht Alexander Graßl. „Wir können neue Werkzeuge zulassen, ohne die Kontrolle über unsere Daten zu verlieren.“ Die DLP-Funktionen werden daher bei Sesotec schrittweise weiter ausgebaut und bilden eine wichtige Grundlage für die regelkonforme KI-Nutzung im Unternehmen.

Effiziente Verwaltung und automatisierte Updates ohne Downtime.

Der operative IT-Betrieb ist durch den Wechsel zu einer SASE-Architektur sehr viel einfacher geworden. Ein wesentlicher Faktor ist dabei die intuitive Benutzeroberfläche der Cato Cloud-Plattform. Netzwerk-, Security- und Zugriffsrichtlinien lassen sich einfach verwalten, ohne dass dafür tiefgehende Spezialkenntnisse erforderlich sind.

„Ich bin kein typischer Administrator, der gerne in Konfigurationsmasken oder auf der Konsole arbeitet“, sagt Alexander Graßl. „Die Oberfläche von Cato verstehe ich. Und wenn es darauf ankommt, kann ich auch selbst Regeln anpassen und muss dabei keine Angst haben, etwas kaputtzumachen.“

~ Alexander Graßl,
Head of IT, Sesotec



Diese Einfachheit erleichtert nicht nur die tägliche Arbeit, sondern reduziert auch die Abhängigkeit von einzelnen Spezialisten.

Ein weiterer Vorteil ist der hohe Automatisierungsgrad der Cato-Plattform. Neue Security-Funktionen und Updates der einzelnen Plattform-Komponenten werden heute zentral in der Cloud eingespielt – ohne geplante Wartungsfenster oder manuelle Eingriffe. „Ich muss heute nicht mehr am Freitagnachmittag einen Administrator abstellen, der sich um Updates für Firewalls, VPNs oder andere Sicherheitslösungen kümmert“, berichtet Alexander Graßl. „Das passiert jetzt alles automatisch und ohne Einschränkungen des laufenden Betriebs.“

Die Arbeit des IT-Teams wird auch durch Cato XOps erleichtert. Der integrierte Security Operations-Service der Plattform fasst sicherheitsrelevante Ereignisse zusammen, setzt sie in einen Kontext und bildet daraus nachvollziehbare Incident-Stories. Für die IT-Abteilung bedeutet das spürbar weniger Analyseaufwand und eine deutlich geringere Alarmflut. „Wir bekommen keine riesige Menge an Einzelmeldungen mehr, sondern klare Zusammenhänge“, so Graßl. „Das entlastet unser Team enorm.“

Cato XOps filtert irrelevante Signale heraus, priorisiert Vorfälle automatisch und liefert konkrete Handlungshinweise. Das Ergebnis ist ein stabiler, gut kontrollierbarer Betrieb – und mehr Freiraum für strategische und wertschöpfende Tätigkeiten.



Ausblick: Intelligente Sicherheit – auch innerhalb des Netzwerks

Für die Zukunft plant Sesotec, die KI-Funktionen der Plattform noch intensiver zu nutzen. Perspektivisch sollen sich beispielsweise Firewall-Regeln in natürlicher Sprache beschreiben lassen, so dass administrative Aufgaben weiter vereinfacht und beschleunigt werden. Ziel ist es, Sicherheitsrichtlinien noch schneller an neue Anforderungen anzupassen – ohne zusätzliche Komplexität.

Parallel dazu rückt die interne Absicherung stärker in den Fokus. Bestehende Systeme zur Netzwerksegmentierung sollen schrittweise abgelöst und durch die integrierten Funktionen der Cato-Plattform ersetzt werden. So will das IT-Team nicht nur zwischen den Standorten, sondern auch innerhalb des eigenen Netzwerks eine konsistente Sicherheitsarchitektur aufbauen.

Bei all diesen Schritten setzt Sesotec weiterhin auf die enge Zusammenarbeit mit der IF-Tech. „Ganz gleich, ob es um die strategische Weiterentwicklung unserer Umgebung oder um kurzfristige Support-Anfragen geht – wir können uns jederzeit auf die Unterstützung der IF-Tech verlassen“, fasst Alexander Graßl zusammen. „Wenn wir uns melden, erhalten wir immer sofort eine kompetente Rückmeldung. Genau so stellen wir uns eine gute Partnerschaft vor.“



Jetzt zur IF-Tech wechseln und spannende Einblicke in die Welt der IT erleben.

Wir sind EMEA Technical Competency Partner of the Year 2026 von Cato Networks und ebnen Unternehmen den Weg zu einer modernen SASE-Architektur.

Wer auf individuelle Beratung, technisches Know-how und praxiserprobte Lösungen setzt, findet mit der IF-Tech einen starken Partner für moderne IT-Sicherheit.

- » Individuelle Analyse
- » Strukturierter Projektablauf
- » Enge Zusammenarbeit

Kontaktieren Sie uns bei allen Fragen rund um IT-Sicherheit – wir begleiten Sie gerne.

**E-Mail: vertrieb@if-tech.de
Tel.: +49 89 2000 669-10**