

Schutz sensibler Daten in der Cloud: Eine DLP-Erfolgsgeschichte einer nordeuropäischen Regierung

FALLSTUDIE

KUNDENPROFIL

- Branche: Regierung/Öffentlicher Sektor
- Region: Nordeuropa
- Abgedeckte Nutzer: 17.000
- Lösung: Symantec DLP Core
- Umgebung: Netzwerk, E-Mail, Endpunkt

HERAUSFORDERUNGEN

- Organisatorische Initiative zur Migration zu Office 365 ohne bestehenden Datenschutz
- Fehlende DLP-Abdeckung für Cloud-Anwendungen, dringender Bedarf an Transparenz und Kontrolle über Cloud-App-Daten (OneDrive, SharePoint, Outlook)
- Budgetbeschränkungen und dringender Handlungsbedarf vor Auslaufen der Verfügbarkeit von Mitteln
- Das Risiko eines Compliance-Verstoßes

BROADCOM-LÖSUNGEN

- Bereitstellung von 17.000 Lizenzen für die Symantec DLP Cloud
- Bereitstellung fachkundiger Beratung durch DLP-Spezialisten, um eine reibungslose Einführung und langfristige strategische Ausrichtung zu gewährleisten

VORTEILE

- Schutz sensibler Daten in Office 365-Anwendungen (OneDrive, SharePoint, Outlook) mit Echtzeit-Transparenz und Kontrolle
- Vermeidung von Compliance-Risiken durch Implementierung der DLP Cloud, bevor sensible Workloads in die Cloud verlagert wurden
- Ermöglichung einer sicheren Cloud-Einführung unter Beibehaltung des bestehenden Security-Governance-Modells
- Aufbau einer Grundlage für zukünftige Investitionen, einschließlich DLP Core vor Ort und umfassender Erweiterung der Abdeckung

1. SORGENFREIER DATENSCHUTZ IN DER CLOUD

Die Einführung von Office 365 veranlasste diese nordeuropäische Regierungsbehörde, schnell zu handeln. Da OneDrive, SharePoint und Teams als zentrale Produktivitätswerkzeuge etabliert werden sollten, rückte der Datenschutz in den Fokus – insbesondere im Hinblick auf strenge Compliance-Vorgaben und den Umgang mit sensiblen Daten aus dem Gesundheits- und Bildungsbereich. Symantec DLP Cloud, integriert über API, bot nahtlose Transparenz und Kontrolle, ohne die Produktivität der Benutzer zu beeinträchtigen. Die Lösung wurde reibungslos implementiert – dank eines hochgradig kooperativen Proof of Concept und umfassender Unterstützung, wodurch kritische Daten geschützt blieben, ohne zusätzlichen operativen Aufwand zu verursachen.

2. EINE BEWÄHRTE SICHERHEITSSTRATEGIE, DIE ÜBER DIE JAHRE HINWEG GEFESTIGT WURDE

Diese Behörde war bereits seit der Blue-Coat-Ära mit Symantec vertraut und setzte somit früh auf die Technologie. Im Laufe der Jahre führte die Behörde Endpunkt-, Web- und E-Mail-Sicherheit ein und wurde so zu einem der größten und loyalsten Symantec-Kunden in Europa. Das bestehende Vertrauen in die Marke bildete eine starke Grundlage für die schnelle Einführung von DLP Cloud. Es ging nicht nur um Vertrautheit, sondern darum, eine Strategie fortzusetzen, die sich als sicher, stabil und skalierbar erwiesen hatte.

3. KOMPLEXITÄT, UND KOSTEN REDUZIEREN

Verschiedene DLP-Lösungen wurden intern diskutiert, doch die Cybersicherheitsleitung der Behörde wusste aus Erfahrung, dass andere Tools nicht nur teurer waren, sondern in Bezug auf Abdeckung, Kontrolle und die Qualität der DLP-Erkennungsfunktionen oft auch weniger boten. Mit Symantec war es möglich, mehrere Datenströme über eine einheitliche Plattform zu schützen – zu fast 40 % niedrigeren Kosten als die nächstbeste Alternative. Die Entscheidung wurde nicht nur im Hinblick auf technischen Aspekten getroffen, sondern war auch finanziell und strategisch motiviert und passte perfekt zu den langfristigen digitalen Zielen.

4. VOM PILOTPROJEKT ZUR INSPIRATION FÜR ANDERE REGIONEN

Das Projekt begann mit einer Testumgebung mit 17.000 Benutzern und wurde schnell zu einer vollständigen Produktivbetrieb hochskaliert. Dank der fachkundigen Unterstützung durch Symantec und Arrow sowie der guten internen Abstimmung zwischen den Rechts- und Sicherheitsteams konnte die Behörde schneller vorgehen als erwartet und die Investition bereits Monate vor dem ursprünglichen Zeitplan abschließen. Der Leiter der Cybersicherheit nimmt regelmäßig an Referenzgesprächen mit anderen Organisationen teil und spricht dort über die eigene Erfahrung und rät zur Einführung.