SecureTrust™
a Trustwave® division

CASE STUDY

Protecting telcos in a cloud-based world

As COVID-19 has created a work-from-home revolution, business phone systems and other communications applications are increasingly moving to the cloud. This growth in cloud computing is creating a transformation in the data centre business model, as hyperscale centre operated by large service providers act as electronic vaults for all that information. Telco companies are increasingly assuming responsibility for these cloud services' PCI DSS compliance, as well as for the compliance of the data centres. These companies must do everything from properly configuring VoIP firewalls and encrypting the personal information transmitted by the cloud-based systems to serving as network service providers and securing the data centres' physical environment and servers.

Client Spotlight:

A leading multi-service operator working across several continents, this telco provides mobile financial services, cybersecurity, operator services, connectivity solutions and digital transformation consulting for consumers and businesses. The telco, a multibillion-euro revenue business, has completed several acquisitions and adopted several new technology platforms over the past several years.

"SecureTrust's Compliance Manager allows us to meet the client's strict timeframes by offering an interactive tool to monitor status and provide fully transparent updates."

— Jon Rowland, Enterprise Account Executive

"As more and more people work from home during the pandemic, a lot of telcos have had to adapt to an online system and scale up quickly. As their client requirements expand quickly, they need a PCI DSS compliance partner that can handle the complexity."

— Jon Rowland, Enterprise Account Executive

The Challenge:

With a presence across several continents, this leading telecommunications company offers communications products and services to other global enterprises. Because the telco specialises in cloud computing, unified communications, big data and providing network services, it creates and runs numerous applications and technology platforms on behalf of clients that hold cardholder data and therefore required a complex PCI DSS compliance programme.

The company's presence in multiple countries introduced language barriers when discussing PCI requirements, which exacerbated the stress of extremely tight deadlines. The telco also has assets including fully owned as well as co-hosted data centres, which house servers that store and process cardholder data, so its PCI compliance had to be certified through a third-party validation exercise.

Furthermore, the client's role as a network service provider created additional PCI compliance challenges, as well. By providing data links across satellite, DSL and GSM channels for organisations ranging from gas stations to embassy networks in geopolitcally sensitive regions, and then routing the organisations' customer data through various networking components, the client ensures that no customer data is stored or processed by the organisation. But although the client uses strong transmission protocols—including IKEv1 and IPsec—and AES 256-bit encryption, this work nonetheless introduced new PCI requirements, including Reports on Compliance.

As the multinational corporation continued to expand, other PCI complexities increased. In addition to managing PCI compliance for client applications such as digital payment software packages, the company was also asked to manage compliance for the new communications environments it created from scratch. The client's small internal team wasn't equipped to handle the workload or unify the entire organisation's compliance approach. It needed external project management support to successfully complete assessments—all while sticking to a strict fixed budget.

The Solution:

Because it has the most QSAs of any security and compliance company in the world, SecureTrust was able to place multilingual experts onsite at the telco's international offices. By offering a centralised management team augmented by local QSA support, SecureTrust offered a unified approach as well as specific guidance on local regulations and payment processes. This strategy—along with SecureTrust's deep expertise in managing data centre compliance—made the process of managing enterprise-wide assessments and ROCs easier and more efficient, while also saving the company money by minimising QSA travel expenses across countries. The QSAs remained aligned by using SecureTrust's proprietary Compliance Manager, a real-time, cloud-based tool that provides clear, actionable information in a single, consolidated view.

In the end, SecureTrust assessed both the telco's client products and the newly created environments to ensure both the company and the clients that relied on it as a service provider were PCI compliant. It continues to reassess them annually, continually descoping the projects to make their compliance programs more efficient and offering quarterly "health checks" to ensure programs remain on-track between annual validations. What's more, a subscription-based pricing model spreads costs across 12 months to maximise cost efficiency and improve the telco's budget management.

Industry Threat:

As companies quickly shift to VoIP, digitised IT operations and other subscription-based cloud services, telcos are offering fully managed, secure hosting services and data centres that promise clients stability. Each of these avenues creates new cybersecurity vulnerabilities.

Like any other connected device, VoIP systems are vulnerable to hackers. Compromised phones and communications platforms can result in stolen customer information and company data, as well as eavesdropping on sensitive or high-level business meetings. As more companies rely on VoIP while employees work remotely, hacking efforts have increased. In August 2020, the FBI and the Department of Homeland Security warned of a spike in voice phishing, or "vishing," attempts to obtain enterprise login credentials.

Meanwhile, data centres—whether those owned by public cloud companies, private managed-hosting services, or co-hosted facilities—are vulnerable from both a hardware perspective, because they host rooms and rooms full of computers, and a software angle. Potential threats include DDoS attacks, ransomware attacks, application attacks and more. In fact, the massive 2017 breach of a consumer reporting agency that compromised the personal information of 148 million Americans began through an unpatched vulnerability in its front-end web services. Other major breaches, including the 2013 attack of a major retailer that affected 41 million customers, also involved data centres.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com