TRUEFORT™

SUCCESS STORY

Leading insurance firm uses TrueFort to segment legacy environment and demonstrate PCI compliance

TrueFort High-Profile Insurance Client Relies on Microsegmentation for Legacy Systems Protection, PCI Compliance, and Avoiding Costly Penalties

Taking a digital transformation journey while managing legacy systems
Like many Financial Services firms, our client has been using some of its IT infrastructure for more than 30 years and has an ongoing need to prioritize security for the large volumes of sensitive data they manage. As they actively modernize their IT infrastructure and undergo digital transformation, they need to introduce new products and functions while keeping critical legacy systems secure. To achieve this, our client created a dedicated security team. Their CISO explained to us that to manage legacy systems and onboard new products, they planned to expand the team to meet the need. The CISO rightly pointed out that when the security function becomes another responsibility for the systems and network people, it doesn't get the focus it requires. Growing a dedicated team is essential to ensuring security gets sufficient priority in the organization.

Satisfying PCI compliance and ensuring effective legacy system protection

We work with this client to overcome two specific challenges. The first of these emerged from the need for PCI compliance. There are about 800 employees in our client's home office. They have at least one office in every county in the state in which they operate and over 200 branches overall. In the home office, they run a 20-employee call center that takes credit card payments from customers. Naturally, there is a plethora of strict requirements necessary to ensure PCI compliance. PCI DSS 4.0 enables organizations to use microsegmentation to isolate sections of the environment for audit scope. Without the microsegmentation functionality TrueFort provides, the entire environment would need to be audited to enforce strict PCI requirements for all 800 employees in the home office, rather than just for the 20-person call center.

They could have done it with VLANs, but that is obsolete, and their eyes are on a long-term and sustainable solution, so they used TrueFort microsegmentation to ensure PCI compliance. They already had CrowdStrike agents installed throughout their infrastructure. TrueFort, the only approved microsegmentation solution in the CrowdStrike store, made it easy for them to focus on segmenting the call center. At that point, we enabled them to reduce their required PCI compliance audit scope to the call center.

THE CLIENT

Leading insurance specialists with 75 years of legacy data and an 800-employee home office protects IT infrastructure for their call center and over 200 branch offices in the state where they operate.

THE CHALLENGE

Ensure the maintenance and protection of legacy systems and achieve efficient PCI compliance, while onboarding new products as a part of digital transformation.

THE SOLUTION

Our client deployed the TrueFort Platform, the only approved microsegmentation solution in the CrowdStrike Store, to segment off their legacy systems and identify anomalous system traffic – even traffic they thought was decommissioned – to stop serious threats.

THE RESULTS

- **On-track to achieve PCI compliance and avoiding costly penalties**
- **More efficient and complete legacy systems protection**
- **Dramatically reduced attack surface and control over rising cybersecurity insurance costs**

The second challenge was our client's need to efficiently manage legacy applications while adopting and onboarding new products. For example, one of their legacy systems uses SMBv1, a network-layered protocol mainly used on Windows for sharing files, printers, and communication between network-attached computers. This protocol has been deprecated and is vulnerable. Without TrueFort microsegmentation, they would have to enable SMBv1 on their domain controllers for their entire network. Once they microsegmented the legacy workstations and servers, they felt comfortable continuing to use SMBv1. The more they learn about and deploy the capabilities of TrueFort microsegmentation the more efficient they get on both PCI compliance and managing legacy applications.

TrueFort's role in optimizing the CrowdStrike firewall

Years ago, when our client's operation was smaller, they adopted the Symantec anti-virus software. Over time, they fine-tuned that software to the point that they used it in place of their Windows firewall. When they decided to onboard the CrowdStrike solution, they faced a dilemma. They were compelled to dismantle the Symantec solution that they had spent years configuring. They knew out of the gate that they planned to use the CrowdStrike firewall. During the CrowdStrike implementation process, they learned that trying to identify and optimize the authorized interactions and protection – is a real nightmare. TrueFort has been huge in helping manage this, because TrueFort's platform is extremely adept at identifying and gaining insight into interactions. TrueFort discovers and understands applications, users and their interactions with core systems and provides real-time behavioral insight into interactions; enabling users to determine the validity of the communication. This makes the configuration process an order of magnitude easier and has also helped this client lock down what it learns over time.

TrueFort's microsegmentation is helping avoid $5,000 per month in PCI non-compliance penalties

The biggest selling job for a security team is making the CFO see the value in the solution. In this case, our client's CFO has his finger firmly on the pulse of the PCI compliance issue. In December last year, the PCI acquirer responsible for building and managing their PCI compliance program told them they needed to demonstrate full PCI compliance by June to avoid a costly penalty. The introduction of a hard deadline gave both the security team and the CFO a clear goal. PCI-DSS 4.0 includes parameters around microsegmentation. By microsegmenting cardholder data, the audit scope may be reduced. With instant ROI from our TrueFort platform, the company is now on track to meet its critical PCI compliance requirements.

"Growing a dedicated security team is essential to ensuring security gets sufficient priority in the organization."

"Without the microsegmentation functionality TrueFort provides, they would have had to satisfy these strict requirements for all 800 employees in the home office, rather than the 20-person call center."

"Using firewalls and switches alone to isolate legacy applications and control cybersecurity insurance premiums is costly and insufficient. TrueFort's microsegmentation solution is the best long-term solution for controlling premium costs."

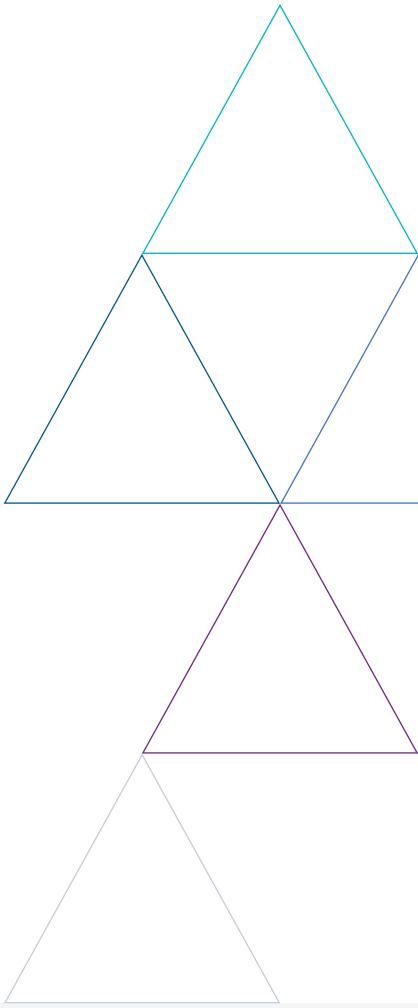
TrueFort's microsegmentation keeps cybersecurity premiums under control

Our client's CFO was also aware that PCI compliance helps keep cybersecurity insurance premiums under control. As more cybersecurity breaches happen, cybersecurity insurance premiums are rising to meet the costs of more claims being filed. One of the specific requirements that directly affect cybersecurity insurance premiums is a company's ability to microsegment legacy applications. The "path of least resistance" of using firewalls and switches alone to isolate legacy applications is no longer sufficient, not sustainable, and costly. Using TrueFort's microsegmentation solution is the smart long-term solution to keep cyberinsurance premiums under control.

TrueFort helps find issues the company thought was resolved or didn't know about

The TrueFort Platform has uncovered countless issues that would otherwise have been very difficult for our client to find. For example, in 2019 they were using several Solar Winds products. After the Solar Winds breach was made public, they didn't want to take any chances, so they decommissioned all Solar Winds products and never turned that server back on. This was huge, because they used Solar Winds for all of their monitoring. When they deployed the TrueFort platform, the microsegmentation solution discovered and mapped applications, users, and their interactions with core systems to create an automated baseline of accepted activity. TrueFort found that the servers were still trying to connect to the Solar Winds products by sending SNMP traps to the old internal Solar Winds IP address. While not a crisis, it is not good hygiene. The TrueFort Platform identifies anomalous traffic – even traffic thought to be decommissioned, which is very valuable to our client's infrastructure team. They know now that if TrueFort enables them to see anomalous SNMP traps being sent to a non-existent server, they also have the confidence to identify a far more serious threat like a command and control (C&C) trap through which a threat actor could deliver malicious instructions. They realized that TrueFort has unprecedented capacity to reduce the impact of security incidents and shrink their attack surface.

"The TrueFort platform has proven it can detect serious threats like command and control (C&C) traps through which a threat actor could deliver malicious instructions."



ABOUT TRUEFORT

TrueFort puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

Learn how TrueFort can enable zero trust application protection for your organization through microsegmentation and other application-centric controls.

Contact us at sales@truefort.com

TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM