ZERONORTH™ | CyberProof™

CASE STUDY

Leading Telecommunications Provider Supports PCI DSS and NYDFS Compliance

A Joint Solution from ZeroNorth and CyberProof

Background

Telecommunications companies remain a prime target that hackers look to exploit. It makes sense considering they control and construct critical infrastructure, on top of possessing mammoth amounts of both personal and business data. For these reasons, it's pivotal that companies have rock-solid defenses to detect and respond to attacks both inside and outside the perimeter. But just as important, they need to start investing more resources to proactively secure software and infrastructure in order to strengthen their overall security posture and minimize the potential attack surface for attackers to exploit.

However, being proactive about addressing security is always easier said than done. Telco companies in particular have to place a strategic focus on developing and implementing software as quickly as possible. And the increasing speed of software development can bring on a series of challenges if it can't be done in a secure way that ensures vulnerable code isn't being rolled out and compliance requirements are being met.

Situation Analysis

Recently, a leading telecommunications provider was up against a daunting challenge. It had to strengthen its robust cybersecurity program while addressing the Payment Card Industry (PCI) Data Security Standard (DSS) and New York Department of Financial Services (NYDFS) Cybersecurity Regulation.

As a large organization with distributed application development teams, the company struggled to maintain a clear and consistent picture of secure coding methodologies and the scanning and testing applications in place across the enterprise. Overall, the disparate workforce made collaboration among security and development teams difficult, if not impossible.

The fragmented setup and lack of visibility made it increasingly challenging to demonstrate to internal and external auditors that the company's processes were meeting the PCI DSS and NYDFS compliance requirements. In addition, the telco did not benefit from leveraging consistent security best practices across its siloed development teams.

At-a-Glance

Goals

- Gain visibility into coding methodologies and the scanning and testing applications in place across the enterprise
- Address the PCI DSS and NYDFS) Cybersecurity Regulation requirements
- Implement cybersecurity controls that would better position the telco in the eyes of its PCI Qualified Security Assessor (QSA)

Results with CyberProof and ZeroNorth

- Assessment and recommendations ranging from an inventory of software and general best practices, to gaps in processes and a roadmap for addressing potential vulnerabilities
- Ability to manage vulnerabilities and risk across a suite of software development teams and infrastructure
- Strengthened security posture and the ability to meet PCI DSS and NYDFS compliance requirements quickly and effectively.

The Solution

To address these challenges, the company tapped CyberProof to lead a project in assessing how the organization could improve its processes and security posture. The goal was to develop go-forward recommendations and implement cybersecurity controls that would better position the telco in the eyes of its PCI Qualified Security Assessor (QSA).

To begin, CyberProof worked closely with internal teams to identify more than two dozen applications that fell within the scope of their compliance requirements, specifically PCI DSS. From there, they identified project leads for each of these in-scope applications – assigning subject matter experts able to help drive the process and identify common ground across distinct development teams.

After a thorough discovery process, CyberProof delivered specific recommendations, ranging from an inventory of software and general best practices, to gaps in processes and a roadmap for addressing potential vulnerabilities.

As a key recommendation within the roadmap, CyberProof suggested leveraging the ZeroNorth platform to help the company manage vulnerabilities and risk across its suite of software development teams and infrastructure. Given the diverse nature of the company's scanning and testing tools, ZeroNorth provided the only solution capable of ingesting, normalizing, correlating and prioritizing vulnerabilities across the software development life cycle (SDLC). In addition, as a cloud-based technology, ZeroNorth provided an easy-to-deploy and platform-agnostic solution that can scale with the telecommunication provider's needs now and in the future.

"It was critical that the solution we developed for this large telco be delivered as a single pane of glass that both provided consistency across disparate applications and eased the burden of remediating vulnerabilities. The ZeroNorth platform is the only solution that enables us to consistently apply security across applications and infrastructure in the context of the diverse applications portfolio our customer has in place."

—Brian McGraw,
Head of Advisory Services, CyberProof

Results

For CyberProof, ZeroNorth offered the ability to help the telco bridge the gap between application security and security operations, while streamlining the process of addressing risk and vulnerabilities across the SDLC. Together, CyberProof and ZeroNorth have helped bolster the organization's overall security posture, leaving the customer confident in its ability to meet the PCI DSS and NYDFS compliance requirements quickly and effectively.

About ZeroNorth

ZeroNorth is the security industry's first provider of orchestrated risk management. Organizations that rely on software as a competitive advantage trust ZeroNorth to manage risk by orchestrating the continuous and comprehensive discovery and remediation of vulnerabilities. ZeroNorth is headquartered in Boston and was created by and for security leaders. For more information, follow ZeroNorth on Twitter (@ZeroNorthSec) or LinkedIn, or visit **www.zeronorth.io**

About CyberProof

CyberProof is a cyber security services and platform company that gives organizations a faster and smarter way to stay ahead of security threats and create secure digital ecosystems. CyberProof's advanced cloud-based orchestration and automation platform drives operational efficiency allowing our nation-state cyber experts to remain focused on each individual threat. In the face of a hostile and evolving threat environment, CyberProof integrates all the key elements you need to detect & prioritize threats early while both rapidly and decisively responding. CyberProof is part of the UST Global. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services. For more information, see: **www.cyberproof.com**

© 2019 ZeroNorth, Inc. ZeroNorth is a trademark of ZeroNorth, Inc. All other brands and products are the marks of their respective holders.