# CASE STUDY CHALLENGE: SECURITY AS BUSINESS ENABLER

APRIL 2016 | US$25

Channel Partners™

# TABLE OF CONTENTS

Channel Partners™

# SECURITY MAKES BUSINESS POSSIBLE

**SECURITY EXPERT BRUCE SCHNEIER FAMOUSLY SAID, “AMATEURS HACK SYSTEMS, PROFESSIONALS HACK** people.” The ransomware that recently hit hospitals hard proves his point. Even the most basic security policy addresses the ways that this malware gets in — for example, outdated OSes or corrupt files in email. But dig deeper, and nine times out of 10 the reason Windows XP is still running is because people need an application that won’t run on a modern OS, or because XP is part of the firmware for a critical device, like an MRI machine. That emailed malware disguised as a spreadsheet? It was part of a spear phishing scheme, cleverly designed to appear to come from a trusted business partner.

What do you expect people to do, stop performing MRIs or ignore communications from important third-party providers? Forget it.

Look, when your customers’ employees skirt security rules, they’re rarely doing so because they want to. They defeat systems put in place to protect the business because they need to get their jobs done, and your carefully designed controls are seen as roadblocks, not enablers.

Instead, you as a trusted adviser must empower people to be secure without undue risk.

Among our three Case Study Challengers profiled in this issue, our Champ, CryptZone, took this to heart. The company realized that electricity provider Polskie Sieci Elektroenergetyczne (PSE S.A.) needed to open up access to its systems and resources for many user groups: employees, electricity traders, contractors and third-party suppliers, all of them with their own understanding of “here’s how we get work done." To protect its mission-critical systems and sensitive information while giving these constituencies the tools needed to keep power flowing, the utility had to think differently about security.

## 3 Best Practices to Steal

1 **Think before you link.** Control access to critical systems. In utilities, avoid having Internet-facing servers, especially Web servers, directly connected to SCADA management systems. No matter what your customer's business, use rules and roles to control which network resources any user can access and under what circumstances. For example, Cryptzone ensures that only corporate-owned devices can connect to a particular application.

2 **Disaster recovery IS security.** Effortless bundles backup and disaster recovery with its security and protection. If ransomware hits, the only way to ensure that data is fully restored — and that the attackers didn't leave an unlocked back door — is to nuke the affected systems and restore on bare metal.

3 **Fast and proactive always wins.** Using its dashboard and SIEM data, Hawaiian Telecom was able to spot an attack in progress, contact the customer, launch an incident response plan and block outbound traffic for affected workstations. That's the kind of service customers remember when it comes time to renew.

Our other Case Study Challengers also recognized the human element. AlienVault helped Hawaiian Telcom's business customers, which represent a range of industries and security needs, stay safe and compliant while keeping costs under control. Effortless Office worked with Starwood Hotels & Resorts — a big player in the ultimate people-focused vertical, hospitality — to successfully offer personalized but secure services.

The constant is the human element. The most recent Verizon Data Breach Index Report says that for two years running, more than two-thirds of cyber-espionage incidents have featured phishing. Attackers that launch a campaign of just 10 emails can expect a greater than 90 percent chance that at least one person will fall for the scam. Who are these rubes? Mostly, employees in the communications, legal and customer service departments. The common denominator: Opening email is a central component of their jobs. Get our point?

# CRYPTZONE CONNECTS ELECTRIC COMPANY WITH POWERFUL, FLEXIBLE NETWORK SECURITY

Channel Partners
CASE STUDY CHALLENGE
WINNER

## THE COMPANY

Cryptzone™

[Cryptzone](Cryptzone)

linkedin.com/company/cryptzone-ab-publ-

@cryptzone

Cryptzone is a leader in network security and protection, offering data security, content governance and app security solutions for data protection to global corporations across a range of industries, as well as government agencies.

## THE CLIENT

PSE Polskie Sieci Elektroenergetyczne

Polskie Sieci Elektroenergetyczne (PSE S.A.) is the transmission system operator for Poland, responsible for meeting the country's domestic and cross-border demands for electricity. As well as managing and developing the extensive network of power transmission lines and substations across Poland, the company's responsibilities also include the national security of the electric supply, managing cross-border connections and operating the power market "balancing mechanism": buying and selling energy effectively in real-time to balance power flows in the transmission system.

## THE CHALLENGE

The complex nature of the business means that many user groups need access to PSE S.A.'s systems and resources: employees, electricity companies/traders, contractors and third-party suppliers. To protect the company's mission-critical systems and protect the sensitive information being handled on the electricity market, PSE S.A. needed powerful yet flexible network security.

To provision access for a large number of users with diverse requirements, administrators needed to be able to define many individual roles quickly and easily, and have precise control over individual access rights — for example, electricity market players submitting bids to buy/sell electricity, employees needing access to mail and office applications, and third-party suppliers providing online remote system support and maintenance.

Unauthorized access to some areas of the network could have potentially catastrophic results, from manipulation of the energy markets to control of substations leading to blackouts across the country. Therefore, all communications needed to be encrypted and strong user authentication would be required to protect critical systems.

"We needed secure access 24/7," said Tomasz Szudejko, deputy director of PSE S.A.'s Department of Operator Services. "SCADA and EMS applications are working 24 hours a day. No downtime is allowed, so it is important for our employees at home or after hours to be able to log in and fix any problems — and to be able to do it in a secure way."

## Utilities a Hot Target

Recently attackers hit Ukraine's energy distribution infrastructure, taking down multiple substations and cutting power to 80,000 customers. Michael Assante, the SANS lead for Industrial Control System and Supervisory Control and Data Acquisition — SCADA — **recently wrote** that this was a sophisticated and coordinated attack. The adversary took steps to "blind" dispatchers, damage the SCADA system hosts and cover their tracks. Partners serving U.S. utility clients should study the attack and ask, "Could it happen to my customer?" The answer is, yes. In 2015, attackers gained access to a water utility's operational network, manipulating the system to alter the amount of chemicals that went into the water supply, according to **Verizon's March Data Breach Digest.**

## THE SOLUTION

PSE S.A. determined that Cryptzone's AppGate met their full set of requirements, combining strong authentication, authorization, encryption and access control in one comprehensive solution.

AppGate technology is flexible and scalable, making it easy and cost-effective for PSE S.A. to start with a smaller installation and then add more servers as requirements changed. Initially one AppGate security server was installed, but that has now been upgraded to support increasingly complex requirements. Two clustered Ax2 security servers provide internal access to key systems such as SAP and the energy market. A second cluster provides external access for electricity market traders, and for technical support personnel so they have remote access in case of emergency. A third cluster provides remote access for employees to access the mail server and office applications when working away from the office.

AppGate is designed to cluster several servers together for high availability. Alternative IP addresses for the other clustered servers are automatically distributed to users' machines so, in the event that the usual server is unavailable, connections are immediately routed to the good server. It is also possible to connect two different ISPs to the clustered servers so if one ISP fails, users can still access the network through the other ISP/server.

Powerful rules and role management provides administrators with precise control over which network resources each user can access and under what circumstances. Endpoints can be measured so, for example, only corporate-owned machines can connect to particular applications. Services that the user is not authorized to use are invisible, thus making it impossible for them to see or attack other corporate assets. In addition, AppGate can automatically configure machines that have never connected to the PSE S.A. network before. So if an external trader or supplier uses a different PC, the client is provisioned and configured without having to wait for an administrator's input.

## THE RESULTS

Following the successful initial implementation of AppGate at PSE S.A., the organization has adopted AppGate as the main system for controlling access to important systems. AppGate has been integrated into the new control systems and technologies at the company's award-winning headquarters in Warsaw. Other areas of the business, including branch offices, that need access to data exchange, email and other applications are also using AppGate for secure access.

"The AppGate system is relatively easy to use, but the key issue is that it is very powerful," says Szudejko. "It is possible to define so many different people with very different needs. We couldn't find any other system that allows us to define such a variety of different profiles for all our different users."

Azudejko adds, "We work very closely with the AppGate team in Sweden and have found them to be very responsive, for instance when we have needed them to develop additional functionality. We think it's a very flexible, powerful and stable system for the professional and demanding environment. So we would be happy to recommend it."

## CASE STUDY IN BRIEF

| | |
|---|---|
| BUSINESS CHALLENGE | Necessity to protect mission-critical systems and sensitive information, while providing secure access to necessary resources by a variety of users and maintaining 24/7 operations. |
| OLD SOLUTION WEAKNESS | Not able to provide the required security, flexibility and stability. |
| NEW SOLUTION | AppGate, which met the full set of requirements by combining strong authentication, authorization, encryption and access control in once comprehensive solution. |
| IMPACT | Having proven to be powerful and easy to use, the solution has been adopted as the main system for controlling access to important systems and has been integrated into operations in other areas of the business. |

# ALIENVAULT PROVIDES HAWAIIAN TELCOM WITH A FLEXIBLE, AFFORDABLE SECURITY PLATFORM

## THE COMPANY

AlienVault

linkedin.com/company/alienvault

@alienvault

AlienVault, a leading provider of unified security manager and community-powered threat intelligence required to detect and act on today's advanced threats, was founded to provide organizations with security that's affordable and simple to use. In 2012, AlienVault created the Open Threat Exchange, the world's largest crowd-sourced computer security platform with more than 37,000 participants in 140 countries who deliver more than 3 million threat indicators daily.

## THE CLIENT

Hawaiian Telcom, headquartered in Honolulu, is one of the state's technology leaders, providing integrated communications, broadband, data center and entertainment solutions for business and residential customers. With roots in Hawaii beginning in 1883, the company offers a full range of services including Internet, video, voice, wireless, data network solutions and security, colocation, and managed and cloud services, supported by its next-generation fiber network and aa 24/7 state-of-the-art network operations center.

## THE CHALLENGE

When Hawaiian Telcom launched managed network and security services in 2010, they quickly realized that they needed a security management platform that could support them effectively in monitoring and maintaining network security for their business customers.

Hawaiian Telcom's business customers represent a range of sizes and industries, and each one has a unique set of security needs. Many of them collect sensitive or personally identifiable information (PII) and must maintain compliance with Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability (HIPAA) and other standards. As a provider of managed network and security services, Hawaiian Telcom helps customers ensure compliance and protect themselves from data theft, malware and other cybersecurity threats.

Shortly after Hawaiian Telcom started providing managed network and security services, they began to notice a couple of key trends. One was that many customers were in need of a log tracking solution that could allow them to keep a close eye on exactly who was logging into their systems, what they were doing and how they were getting in. Although the need came about largely because of PCI DSS mandates, which require companies to exhibit this capability, it also happens to be an extremely important indicator of overall security — according to a Verizon report, more than 90 percent of companies that have been breached did not have these controls in place.

Another trend they noticed involved the rising cost of the individual security solutions necessary to serve their customers. Hawaiian Telcom needed to have different point solutions in order to take inventory of assets, scan for and address vulnerabilities, update and guard against a rapidly growing list of security threats and respond to any intrusions as they were happening.

## Knowledge Is Power, Sharing Is Daring

Security information and event management is a hot area, and no wonder. In the era of big data and IoT, where companies are collecting information at unprecedented rates, it only makes sense to mine data for security insights. The problem is, firms have traditionally been reticent to share intel on how attackers are trying to penetrate defenses, and sometimes succeeding: Just 15 percent of respondents to PwC's 2015 State of Cybercrime Survey have made cybersecurity knowledge sharing a priority.

The U.S. government is looking to break down these walls via the Cyber Incident Data and Analysis Working Group, a collection of insurers, CIOs and CISOs from the private sector tasked with figuring out how to collect and use incident data in an anonymous but effective way. You can weigh in on the effort through May 24.

## THE SOLUTION

After exploring a series of options, Hawaiian Telcom identified AlienVault's Unified Security Management (USM) platform as the best solution for their unique needs. The USM platform offered a combination of tools to monitor and manage customer networks on a single dashboard, which enhanced their team's efficiency and reduced their operating expenses.

The USM platform gives Hawaiian Telcom a solid security information and event management (SIEM) platform, while also providing a number of critical security capabilities built into the system, such as asset discovery, behavioral monitoring, vulnerability assessment, managed firewalls and intrusion detection. All of this functionality is integrated into a single, unified platform that is easy to use and backed by a dedicated customer support team.

## THE RESULTS

AlienVault's solution enables Hawaiian Telcom to offer their customers the most up-to-date network security services supported by AlienVault Labs, which actively tracks and analyzes millions of threats to deliver the latest intelligence directly to the USM platform.

In a recent case, Hawaiian Telcom's managed network and security services team saw some unusual activity appear on the dashboard of a customer who subscribes to their network monitoring service. They quickly identified it as potential malware and found that the entry point was email-based and that the threat was affecting workstations at five different locations across multiple Hawaiian islands. Hawaiian Telecom immediately contacted the customer and initiated their incident response plan, blocking outbound traffic for those workstations at the switch level and helping the customer trigger their cleanup procedures. Thanks to the SIEM alarms, intrusion detection system and the quick action of their team of security experts, damage to the customer's system was minimal.

AlienVault's USM platform has enhanced Hawaiian Telcom's managed network and security services operation. They've accelerated their detection and response capabilities, reduced their operating expenses and improved efficiencies. Businesses of every size and scope can turn to Hawaiian Telcom for assistance with their managed network security needs and industry compliance concerns.

## CASE STUDY IN BRIEF

| | |
|---|---|
| BUSINESS CHALLENGE | An affordable security management platform that could support monitoring and maintaining network security for business customers, some of whom were subject to PII, PCI DSS and HIPAA mandates. |
| OLD SOLUTION WEAKNESS | Existing system could not keep pace with requirements of new services and products being offered to customers. |
| NEW SOLUTION | USM platform offers a combination of security tools, including SIEM and IDS, on a single dashboard to monitor and manage customer networks. |
| IMPACT | Accelerated detection and response capabilities, and improved efficiencies enable client to help customers achieve compliance and solid security, while client realizes reduced operating expenses. |

# EFFORTLESS PROVIDES SEAMLESS TECHNICAL OPERATIONS FOR ELEMENT BY WESTIN

## THE COMPANY

### Effortless Office

linkedin.com/company/effortless-office

@eocloud

Effortless Office offers businesses a cloud-based computing platform with all-inclusive software licensing. Companies of all sizes can operate like enterprise-level companies without large overhead costs for hardware, software and communications systems. IT-as-a-service delivered from a private, hybrid cloud provides more flexibility and responsiveness, while improving efficiency and controlling costs.

## THE CLIENT

Element Las Vegas Summerlin is the first non-gaming extended stay hotel in the upscale Las Vegas community of Summerlin. The $25 million, 123-suite hotel in The Gardins village is a project of Starwood Hotels & Resorts Worldwide Inc. (which owns Westin Hotels & Resorts) and LaPour Partners Inc.

## THE CHALLENGE

From the blueprinting stage to the go-live, Element needed a trusted partner to oversee the technical operations of their new development. Element wanted a secure, user-friendly computing experience to allow different users access to different data. The hotel required a high-speed, efficient computing network that would allow for scaling up or down, had access to qualified IT support for multiple locations, provided backup and disaster recovery and had advanced security and protection for sensitive client data. Element had tight corporate and compliance guidelines. The system had to be working in a few short months.

## THE SOLUTION

Effortless Office provided Element with:

- Effortless Desktop, a centralized cloud-based desktops-as-a-service (DaaS) solution that was compliant with Payment Card Industry Data Security Standard (PCI DSS) requirements
- Advanced security with Effortless Defense
- Secure sending and receiving of emails with Effortless Encrypt
- Remotely managed Effortless Wi-Fi in each guest room

In addition, the system gave Element the ability to synch with Starwood's point-of-sale (POS) system, including PCI-compliant credit case processing.

The migration to Effortless' solution took approximately two weeks.

## THE RESULTS

According to James Coleman, chief development office and co-owner of Element, the Effortless suite of cloud computing solutions "allows us to be more efficient and focus on delivering an outstanding guest experience."

Being able to log into the company's applications from any location or device allows managers and staff to spend more time working with clients. Staff now have an all-in-one resource, which builds accountability, expedites communication and helps to ensure uninterrupted work flow. All users are on the same software and operating system versions, with updates applied globally, keeping everyone in synch. In addition, users can be added and deleted quickly and easily.

Staff surveys reveal an increase in job satisfaction attributable to the Effortless DaaS solution; staff also feels that Effortless has provided them with tools to complete projects faster.

While the cost of Effortless' solution, compared to others, was significantly lower, Coleman said saving money month-to-month on tech costs was not the main reason they were selected. "Working with Effortless may save us some money, but for us it was not the leading factor in our choice of IT providers," Coleman said. "For Element, we had a customer

## Companies Willing to Spend on Security

Among the 500 U.S. executives, security experts and public and private sector stakeholders participating in PwC's 2015 US State of Cybercrime Survey, 76 percent said they are more concerned about cybersecurity threats this year than in the previous 12 months, up from 59 percent the year before. Press accounts of ransomware, attacks on utilities and other cybersecurity coverage has finally made security front of mind with customer executives — and that translates into spending. U.S. information security budgets have grown at almost double the rate of IT budgets over the last two years, the report says, adding that 38 percent of retail and consumer companies increased their security spending by 20 percent or more over the year before, higher by far than any other industry.

experience that had to be carefully created to be in line with the Starwood's brand initiatives. Effortless provides so many technical disciplines which come together to meet our needs. And the staff supporting us at Effortless all have the same 'customer first' attitude that we have."

## CASE STUDY IN BRIEF

| | |
|---|---|
| BUSINESS CHALLENGE | Scalable, secure network that could provide a user-friendly experience for hotel guests while meeting strict corporate and compliance guidelines. |
| OLD SOLUTION WEAKNESS | Not all locations had access to IT support, DR and backup plans were not reliable, network speed and efficiency were inadequate and more security for client data was needed. |
| NEW SOLUTION | A centralized PCI-compliant DaaS solution with advanced security, encryption, plus remotely managed Wi-Fi. |
| IMPACT | The Effortless solution provides Element with the scalability, security, disaster recovery and backup it needed to meet corporate and compliance requirements. Just as importantly, it improved the efficiency of operations for the hotel plant and its employees, resulting in increased staff and guest satisfaction. |

## 3 Lessons Learned

### PSE S.A.: MANAGE ROLES, NOT INDIVIDUALS

Cryptzone enabled PSE S.A. to scale access for a large number of users with diverse requirements while retaining control over the assets and actions associated with individual users by defining roles.

**To Do:** While each end user likes to think of himself or herself as a unique snowflake, in reality, even small firms can and should adopt the principle of role-based access control. The idea is gaining new importance as use of cloud increases.

### ELEMENT BY WESTIN: BUNDLING ADDS STICKINESS

Effortless provides a unified monthly license payment — and contact point — for a bundle that includes PCI-compliant cloud-based desktops-as-a-service, security, email and remotely managed Wi-Fi. Why would the customer buy any one service from a different supplier?

**To Do**: Think carefully about the mix of services that most customers need, and deliver them all under one bill. This removes complexity from the customer and frees them to grow the core business and, in theory, purchase more seats. One caveat: You must price bundles properly. As we discuss here, that involves clients fully understand what they are paying for and the ROI they are receiving. Also pay attention to customer lifetime value.

### HAWAIIAN TELECOM: IF YOU THINK PCI COMPLIANCE IS EXPENSIVE ...

Hawaiian Telecom's customer base and portfolio are diverse, ranging from broadband to hosted data center and entertainment for business, wholesale and residential customers. What all have in common: They make payments.

**To Do:** You might be surprised how many of your customers should be complying with PCI-DSS but aren't. Any merchant that accepts payment by credit cards, by any mechanism, must be compliant, and the federal government is starting to pay attention. Last month the FCC used its Section 6 authority to order nine companies, including Verizon, to file Special Reports detailing how they assess their clients' compliance with Payment Card Industry Data Security Standards. They have 45 days to provide documentation on compliance assessments from 2015, as well as all related notes, test results, and client and third-party communications. If you have customers putting their heads in the sand about PCI, it's time for an intervention. Here's a list of myths vs. reality. Remember, fines begin at $5,000 per month.

*Do you have a success story you'd like to share? The Channel Partners* Case Study Challenge *is accepting submissions on a rolling basis. They will be published in a special section on the Channel Partners site, and the best ones will be awarded a Case Study Challenge Winner logo for use on their own websites. The best of the best will be invited to share their stories during a live session at a Channel Partners event. Case studies should be 1,200 words or less. You can* download the form*, send responses directly to* Lorna Garey, editor-in-chief *or use our* Web submission process*. Let us hear from you!*