BlackBerry | CYLANCE

CASE STUDY

SSP Worldwide Takes on Cybersecurity

The Company

SSP is a global provider of technology systems and solutions across the entire insurance industry, including distribution and trading capability and advanced analytics. SSP works with eight of the top 10 U.K. insurers, four of the top 10 global insurers, and over 40% of U.K. brokers. Behind the scenes, SSP software and services handle several petabytes of data and has the capacity to process up to four million quotes an hour. To deliver at this scale, the company has invested heavily in information technology that spans its large team of developers, multiple data centers, and systems that include on-client-premises software installations, SaaS, VDI, and cloud. SSP solutions underpin some of the most well-known and respected insurance organizations worldwide, such as Legal & General, Direct Line Group, Endsleigh Insurance Services, and Zurich.

The Situation

Over 30 years, SSP has grown consistently, both organically and through acquisition. Today, the company has a team of over 700 and offices on four continents, spanning 24 time zones. As part of a board-level initiative to ensure that SSP can scale its infrastructure while ensuring that security is at the heart of its business, in 2017, SSP appointed its first dedicated Chief Information Security Officer, Paul Ogden. Having come from a background of working in oil, gas, fintech, and telecoms, Paul began a program to benchmark, test, and standardize the entire security framework across SSP in line with ISO 27001 and PCI-DSS.

As a software company with systems, services, and clients that handle large amounts of financial data within highly regulated international markets, it was vital that SSP had a true multi-layer and best practice security architecture. “We began a process of checking and enforcing isolation along with least privilege access across our entire estate, as well as evaluating all of our key technical controls such as vulnerability management and anti-malware,” says Paul.

With such a diverse IT infrastructure plus several acquisitions, endpoint protection is a major area of concern for SSP. “We had a number of different vendors spread across countries and client installations, and gaining an accurate picture was challenging,” says Paul. “So, we began looking at unified endpoint protection solutions that could span our entire server and client estate, including around 5,000 servers.”

Industry

- Financial Services

Environment

- Server, SaaS, and Cloud
- Over 7,000 endpoints
- Staff of 700 with operations on four continents

Challenges

- Reduce the risk of malware, including zero-day events
- Protect diverse server estate across on-premises, cloud, and hybrid
- Reduce management overhead and complexity
- Deal with complex and bespoke scripts and applications
- Protect against coin miners
- Protect against ransomware attacks

Solutions

- Deep testing, included simulated zero-day attack scenario
- Deploy the BlackBerry Cylance AI Platform™ across entire estate
- Support by SecureLink MSSP

SecureLink

The Process

After a visit to InfoSec Europe to meet with several potential vendors and watching a series of demonstrations, Paul created a short list of solutions. “Signature-based tools are simply obsolete with the current generation of threats, so I looked at several of the next-gen offerings, including BlackBerry Cylance, but I remained pretty sceptical,” he comments. “There seemed to be more style than substance with some products, so we created our own in-depth testing process.”

After building an isolated server cluster to host several SSP applications, Paul began a series of tests using both common and rare malware examples. “Both the next-gen and legacy anti-malware solutions could spot and block all these, but when I used basic techniques to repack and obfuscate the malware, the signature-based solutions started to fail.”

To go one step further, Paul built an intentionally vulnerable application then built a bespoke piece of malware to attempt to exploit the vulnerabilities left in that application. The intention here was to simulate a zero-day attack by a targeted attacker. “The legacy malware solutions and most of the next-gen offerings failed to stop the attack, but BlackBerry Cylance stood out,” says Paul. “CylancePROTECT was able to stop the malware from executing the exploit and then triggered an alert. In effect, it had prevented our worst-case scenario of a zero-day attack.”

Paul admits that such a test is way beyond a normal product evaluation, but the unique success of CylancePROTECT® was enough to make it the number one choice and for SSP to start a full-scale implementation.

The Results

The first phase was to deploy CylancePROTECT in monitor mode to observe SSP network traffic and inspect workflows. “This was actually a multi-month trial and during this phase, it spotted a number of potential issues that had been overlooked by our legacy product,” says Paul.

In the next phase, an active deployment was initiated on around 4,000 servers with Paul’s team looking at queries and alerts created by CylancePROTECT. “This did require a bit of detection work as some of the systems we run are a decade old, and we have a lot of custom software that performs very specific tasks that could be tagged as unwanted apps,” says Paul. “This took a few days, and at the end, we had effectively created a comprehensive picture of our core executables across the entire infrastructure.”

Next, the team began testing memory protection capabilities and scripting support. “Although we could be considered as cautious in our approach, the system analyzed 142 million files and encountered 15 files that we had to place into quarantine.”

The success of CylancePROTECT led to SSP installing it on a further 2,000 endpoints and extending the protection to its new cloud AWS instances. “Because of the BlackBerry Cylance design, we managed to massively reduce the amount of repetitive scanning on files going to and from the cloud,” explains Paul. “This led to a 3x throughput performance increase compared to our legacy anti-malware software and across the estate, CylancePROTECT has proven far less resource hungry and more reliable than all of the old platforms, meaning a net benefit of lower AWS running costs.”

SSP is now recommending its clients that have on-premises installations of its systems to switch to CylancePROTECT. In addition, SSP has strengthened its ability to deal with 24x7 security issues through an ongoing MSSP relationship with SecureLink, a highly regarded service provider and BlackBerry Cylance solution provider.

“With any new technology, there are always a few teething troubles,” says Paul. “But, how BlackBerry Cylance has dealt with any issues has been both professional and prompt.”

“The end result is that we now consider CylancePROTECT as a fundamental part of our future information security architecture, and to date, it has not only met but exceeded our expectations,” Paul concludes.

©2019 Cylance Inc. Trademarks, including BLACKBERRY, EMBLEM Design, CYLANCE, and CYLANCEPROTECT are trademarks or registered trademarks of BlackBerry Limited, its affiliates, and/or subsidiaries, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees’ home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 19-0537-20190808