Banks Trust CPP Group with Credit Card Data and CPP Trusts Forcepoint to Help Safeguard It

CPP Group is a partner-focused, global product and services company, specializing in the financial services and insurance markets. They rely on Forcepoint for data loss prevention while taking on the twin challenges of meeting new compliance requirements in global markets and transitioning to the cloud.

CPP Group has a lot of data to protect—both direct-customer data generated by its life assistance business lines and the ultra-sensitive data that banks and credit card companies trust CPP to safeguard as part of its card protection and fraud prevention services. The company needs a flexible data protection framework capable of safeguarding decentralized, cloud-distributed data in multiple countries.

CUSTOMER PROFILE:
CPP develops and delivers insurance and credit protection products for consumers.

INDUSTRY:
Financial Services

HQ COUNTRY:
United Kingdom

PRODUCT(S):
- Forcepoint Web Security Cloud
- Forcepoint Data Loss Prevention

Founded in the United Kingdom in 1980, CPP Group now generates about 65 percent of its revenue in India, mainly through its card protection, extended warranty, and mobile phone insurance businesses. The geographic shift of its business operations has created new challenges for CPP's IT security team.

CPP's card protection and phone insurance services are particularly sensitive to security risks. These businesses involve safeguarding people's sensitive financial information for third-party payment card issuers like banks and credit card companies. As a UK-based company, CPP must comply with the European Union's General Data Protection Regulation (GDPR) when handling such data. But the company must also comply with the Payment Card Industry Data Security Standard (PCI DSS), ISO 27001 guidelines, and national data protection standards in the individual countries where it operates.

For example, India recently enacted laws that require financial data like people's payment card information to be stored locally by financial services companies operating in-country. Other countries where CPP operates, such as Turkey, are in the process of creating similar rules for financial data.

Meeting the challenges of new data residency rules in India

This has put pressure on CPP to secure that data locally while still allowing it to be transferred securely as needed between its UK headquarters and other international offices, says CPP IT Operations Manager Patrick Viner.

Up until recently, the company maintained all of its card data at its UK data center and ran all its databases on its UK policy system. But now this data must be secured across an Amazon Web Services (AWS) cloud environment, as well as locally in the UK, India, and other global locations, while database policy is still maintained and set in the UK.

The challenge is to maintain smooth workflow while accommodating a "more complex data security policy as more countries start insisting on data residency within country," Viner said. "We're in the middle of quite a big project to develop a new platform to accommodate the model so that all data is housed in-country in nations where the company operates payment card services."

Moving onsite security standards to the cloud

CPP has been a long-term customer of Forcepoint, using Web Security on-premises appliances to secure web traffic via VPNs and web proxies through its UK data center. But this approach of routing traffic began leading to delays in information transmission and lost productivity as more of CPP's day-to-day business happened outside of the UK, and particularly in India.

The company wanted to recapture that lost productivity with a move to more cloud-based IT operations while still safeguarding data to protect its customers and for compliance and business continuity reasons. CPP teamed up with Forcepoint to do this.

"First, we moved to a hybrid architecture where we put Web Security endpoint clients in a few of our countries of operation," Viner said. "Then we decided to decommission our data center here in the UK and moved to a VPC [virtual private cloud] environment. At which point, I made the decision to take out physical appliances altogether and moved to full cloud, where we are currently headed for all of our operations."

Challenges

Routing traffic through the UK data center in order to secure it began causing delays and lost productivity.

Operating in multiple countries required compliance with multiple data protection standards.

Approach

Move to Forcepoint Web Security Cloud to improve traffic flow while maintaining security.

Implement Forcepoint Data Loss Prevention to increase visibility to data movement and comply with complex regulations.

Forcepoint DLP pinpoints the behavior putting data at risk

During a trial of Forcepoint's Data Loss Prevention (DLP) solution, CPP's security team discovered that there was a possibility that colleagues and business partners in India could potentially engage in risky practices such as colleagues emailing spreadsheets of customer data without oversight, meaning sensitive data could be accidentally or intentionally sent to the wrong audience. CPP's security team also noticed that there were no provisions in place to prevent colleagues from uploading prospect files to unsecured websites.

Forcepoint DLP helped CPP to bring visibility to such potentially risky behavior, while at the same time avoiding a loss of productivity with time-consuming, workflow-interrupting data traffic routing and security checkpoints.

And perhaps best of all, Viner said his team has been able to tune its DLP policy based on what they learn from the users themselves. Forcepoint DLP's robust out-of-the-box policy library includes predefined policies that comply with regional and industry-specific regulations like GDPR and PCI-DSS. Other commonly used predefined policies are built to comply with protected health information (PHI) regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and Basel Committee on Banking Supervision-derived financial regulations in the EU.

> "With Forcepoint's help, we've found the right balance between safety and productivity."
>
> **PATRICK VINER,** IT OPERATIONS MANAGER, CPP GROUP

With the appropriate DLP policies in place, CPP has been able to do some minor fine-tuning to reduce false positives and meet all compliance requirements without impacting employee productivity, Viner said.

"You can set the policy to where it's too restrictive and the users can't be as productive. But if you've left yourself too open without being able to monitor and alert, then you're causing yourself security risks," he said. "With Forcepoint's help, we've found the right balance between safety and productivity."

Results

Identify and stop risky data movement while allowing the right balance between safety and productivity.