Indian Power Distributor Stays Ahead of Evolving Privacy Regulations

This energy distributor fortifies its data security strategy and customer privacy protections with Forcepoint solutions that zoom in on user behavior and protect third-party data centers.

Millions of residents entrust their personal and financial data to this state power distributor. To retain their trust, the company sought to strengthen privacy protections and stay ahead of coming government regulations. After beginning with Forcepoint Web Security, the company is now integrating Forcepoint Data Loss Prevention (DLP) and Forcepoint Insider Threat to increase visibility and context into user-data interactions, and Forcepoint NGFW to provide strong network protection for data centers.

CUSTOMER PROFILE:
Provides energy to five power companies and millions of residents.

INDUSTRY:
Energy and Utilities

HQ COUNTRY:
India

PRODUCTS:

- Forcepoint Web Security
- Forcepoint Data Loss Prevention
- Forcepoint Insider Threat
- Forcepoint NGFW

This power distributor provides energy to five power companies across this Indian state with a population of more than 25 million people. Managing the state's power also means securing the personal and financial data of individuals and business customers. The company manages customer bill pay, consumer feedback, and more—which means that it acquires a sizeable amount of data, from customer names and contact information to invoicing details and power usage trends. In the wrong hands, this data can potentially be used to commit fraud or theft.

While the company's data stores increase, India's attitude toward data protection is evolving. In August 2017, the country's Supreme Court ruled privacy was a fundamental human right, spurring work on a nationwide personal data protection bill. While that bill has not yet been enacted, businesses see increased regulation of private data on the horizon and know they will likely need strong regulatory compliance processes very soon.

Conflicting security point products compromise web security

The power company first engaged Forcepoint after reaching an impasse with a web security solution that wasn't effective or flexible enough to meet its needs. The incumbent web security solution would bypass the URL filter, allowing users to access unauthorized sites. Separate URL filtering and web proxy point products caused a second challenge: the products were meant to work together but dependencies between them meant upgrades to one product would cause the other product to stop working—leading to support and management issues. In addition to these functionality and integration issues, the security product's category database was less than comprehensive, with multiple categories missing. And a complex update process made it difficult to revise.

The inadequacy of the existing solution led the company to search for a flexible, easy-to-update, combined URL filtering and web proxy solution that also delivered advanced real-time threat protection, according to the organization's executive engineer of network and security.

Creating a customized security infrastructure with individualized user policies

After exploring several vendors who proved unable to address all the company's needs, the organization turned to Forcepoint for comprehensive web security with real-time protection and seamlessly integrated URL filtering. With Forcepoint Web Security, the organization could apply policies by user role, content, and/or protocol instead of simply applying black-and-white policies. In addition, the solution has a powerful category database with more groups than the previous product, and ease of management makes it simple to add more.

The threat dashboard built into Web Security helps the distributor see the entirety of the threat and security ecosystem as well as understand its own areas of vulnerability. "Administrators are now able to easily see what sources are participating in malicious activities," said Forcepoint Sales Engineer, Brijesh Miglani. "They can then share that information with the endpoint team to make sure those machines are scanned and removed from the environment."

Shining a light on Shadow IT for more granular management

As a bonus, Forcepoint Web Security provides visibility into Shadow IT and allows the company to easily block or allow specific cloud applications on a case-by-case basis, to better protect data from the additional risks that come with moving data outside the network.

"Shadow IT features of Web Security help in reducing its administration overhead. If a user says he needs a particular application—for example, Dropbox or Google Drive—allowing that application previously would have required administrators to recategorize all cloud application URLs," said Miglani. "With Forcepoint, administrators can instead block or allow by specific application."

Challenges

Strengthen privacy protections and stay ahead of coming government regulations.

Approach

Integrated Forcepoint solution for network security and protection of critical data.

A risk assessment demonstrates data security issues

In providing continuing support, Forcepoint has proven itself a trusted partner, learning about the power distributor's particular challenges and educating its IT staff on the evolving threat landscape. And as new vulnerabilities and strategic security priorities are identified, the organization leverages its relationship with Forcepoint for new ways of strengthening data protection.

A recent risk assessment conducted by the organization and Forcepoint identified several incidents indicating data vulnerabilities. First, notes from a confidential meeting and stockpiled data had been sent to personal email addresses. Second, it was abundantly clear that data stored in data centers run by third-party contractors needed better oversight. "With a third-party, you need to have some tool to understand what those people are doing," explained Miglani. "If they are doing anything malicious or manipulating data on those servers, you need to know."

To prevent these issues in the future, the organization decided to get closer to user activity and better protect critical data, regardless of location, with Forcepoint Data Loss Prevention (DLP) and Forcepoint Insider Threat.

Gaining new insights into data movement and documenting suspicious user activity

With Forcepoint DLP, the organization will gain visibility into data movement and be able to prevent the kinds of incidents discovered in the risk assessment—confidential or proprietary information being sent to personal email addresses—and more. And Forcepoint Insider Threat provides more context into user interactions with data, so the organization can determine intent and better understand the level of risk associated with each event. Miglani provided an example: "Typically, the organization uses WinZip as its standard application," he explained. "If someone is trying to use WinRAR as an executable file in an attempt to encrypt and password-protect a file, we can detect the intent of the user. We have demonstrated that we can build that context."

The combined solution provides powerful visibility, context, and control, to better prepare to comply with future regulations. "If data is going outside the network, DLP controls will kick in," said Miglani. "And if something happens internally—for instance, if a piece of malware is trying to stop processes, or if someone intentionally attempts to delete files, the organization will be aware of that."

Ease of management, uptime, and strong intrusion prevention to keep the power flowing

Prior to adding these products, the organization used a competitor's firewall solution, but after seeing Forcepoint's strength in DLP and Insider Threat, and conducting a proof of concept, the company decided to add Forcepoint NGFW, partly because of the product's strong availability. It has resilience built in at every level: advanced clustering keeps the network running, even if there's a service interruption in any individual device, and updates and upgrades can be performed with zero downtime.

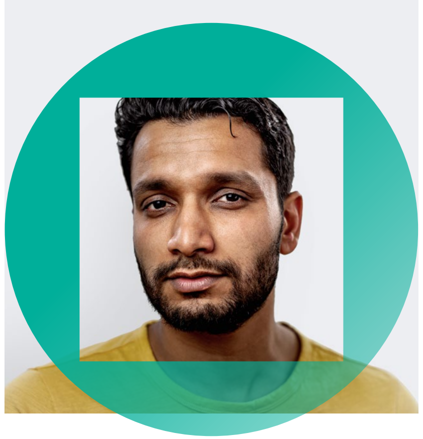
Forcepoint NGFW's integrated intrusion prevention system also proved more capable in blocking evasions (ways that hackers and thieves "camouflage" their attacks). Ease of management was also a factor: one-click policy updates enable IT staff to manage security at each data center from one central location. Finally, interactive dashboards—unlike the static reports the previous vendor provided—empower the organization to drill into events, respond to incidents more quickly, and better understand where network traffic is coming from and how much bandwidth each user is using.

Keeping the lights on and securing customer privacy with Forcepoint

The organization has been able to leverage its strong relationship with Forcepoint to evolve its security practices into a comprehensive strategy for data protection, implementing an integrated suite of products to protect the organization from the outside in. And with this comprehensive security strategy, it is confident in its protection of private customer data and stands

Results

Confident in its protection of private customer data and ready to meet privacy laws India may pass in the future.



[Indian-Power-Distributor-Customer-Story-EN] 20APR2020