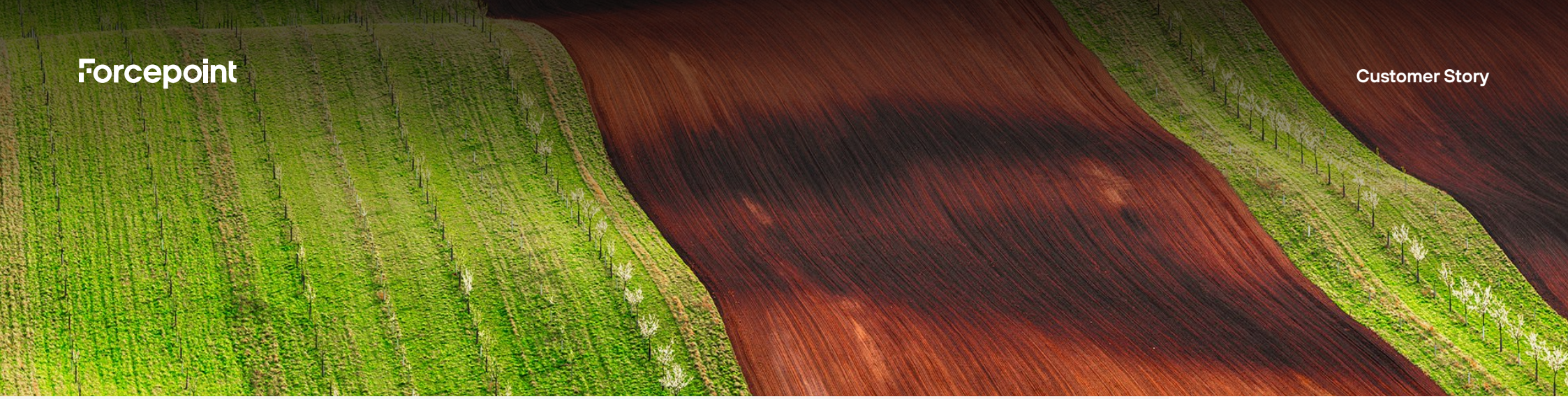

Forcepoint

Customer Story

In the World's Hottest Agriculture Market, this Indian Farm Equipment Manufacturer Protects Its Engineering Edge with Forcepoint

This innovative Indian tractor producer relies on Forcepoint DLP to secure valuable intellectual property while keeping collaboration with its global engineering partners flourishing.

In the thriving Indian agriculture industry, farm equipment manufacturers must stay ahead of demand for innovative solutions to stay competitive. This manufacturer collaborates with global engineering leaders to bring next-generation solutions to the market and partners with Forcepoint to safeguard that IP without stifling collaboration.

CUSTOMER PROFILE:
Leading Indian engineering company operating in the sectors of agri-machinery, construction and material handling equipment, and railway equipment.

INDUSTRY:
Manufacturing

HQ COUNTRY:
India

PRODUCTS:
› Forcepoint Web Security
› Forcepoint Data Loss Prevention

In India, agriculture is big business. It accounts for 18% of the country's GDP, employs 50% of the workforce, and has made India the second largest food producer in the world. To support the industry, the country's government is striving to double farmers' income by 2022, with initiatives from seed to marketing. As incomes increase and competition for the workforce becomes more intense, Indian farmers are adopting mechanization more quickly—driving demand for farm equipment. The result is the world's largest tractor market, with sales expected to grow up to 8% every year until 2030.

A market this hot can be expected to attract global leaders, but it's tough to go up against established players. Kubota, for example, started exporting tractors to India in 2008, but despite attracting buyers with fuel efficiency and low noise, and seeing 50% growth in 2018, the company still only owns 1% of the Indian tractor market. To better compete, in 2019 Kubota announced a joint venture with one of India's largest tractor producers.

This manufacturer is known for being a leader in innovation; for example, it recently introduced India's first electric tractor. This makes it an ideal partner for global engineering and manufacturing leaders such as Ford Motor Company, J.C. Bamford Excavators, Yamaha, Claas, and Jeumont Schneider, in addition to Kubota.

The combination of the manufacturer's ambitious growth plans and high-stakes partnerships like these required IT to transform into a true business partner—one that could support business changes including the move to online operations, multi-factor increases in data, and a significant ramp-up in collaboration with customers and vendors, extending the organization beyond its physical boundaries.

"The CIO is no longer perceived to be a technologist alone, he is expected to be an active member of the business team who enables business priorities and helps create new opportunities through relevant IT interventions," said the Group CIO. Because these business initiatives would drive an increase in critical data overall, as well as an increase in data being shared outside the network with partners, the IT team needed to rethink its data security to ensure that sensitive information would be protected wherever it is located.

Nourishing collaboration while securing intellectual property

The company's significant research and development focus—both internally and with partners—created a large store of intellectual property in the form of blueprints and designs for innovative farming equipment. Audits on the company's network found a surprising amount of critical data across a range of servers, workstations, laptops, and desktops in multiple formats, with users often not realizing the value of data, according to the CIO. The company's global business also meant a dispersed marketing and sales workforce that is largely mobile, requiring secure access to this IP both on and off the official network.

The IT team's challenge was to maintain the seamless flow of data across the organization, especially research and development, and the company's partners in order to support collaboration, while ensuring the security of critical IP.

The first step was to gain support from the executive team. The CIO made his case for a DLP solution because, as he put it, a solution of this nature requires complete buy-in by the top management before it can be rolled out. It was going to create a major change within the organization, and everyone had to be prepared for that. Once the benefits of a DLP solution were understood by senior management, they became the project's core sponsors.

From there, the team was able to conduct an evaluation of multiple solutions against various parameters, including the effective blocking of IP transfer, cost, feature scalability, product roadmaps, ease of use, and whether or not the solution had any predefined industry standards that could be easily managed for swift deployment. Based on these thorough evaluations and a proof-of-concept (POC) with three major vendors, the company found that Forcepoint DLP met all its requirements.

Challenges

The hot Indian agricultural market is driving demand for innovative farm equipment.

This tractor manufacturer partners with global engineering leaders creating valuable intellectual property that needed to be secured, while also allowing collaboration to continue.

The global partnerships require sales and marketing to travel off the corporate network and yet still access sensitive data.

Approach

Implement Forcepoint Data Loss Prevention to find and protect sensitive and valuable data on endpoints and servers, in the cloud, and on-premises.

Increasing data security and raising awareness of its value

With the deployment of Forcepoint DLP, the team was able to find and secure data wherever it was in the company—stored on servers or desktops, moving across email, being edited, or being copied, uploaded, or downloaded across the extensive corporate network. With the addition of Forcepoint DLP Endpoint, data could also be discovered and protected on endpoints such as laptops, whether they were on or off the corporate network. While the primary focus of the security project was the protection of intellectual property, Forcepoint DLP also gave the company the power to secure other valuable information including financial records, personally identifiable information, including (PII), and other sensitive data wherever it lives.

A third-party classification tool implemented as part of the same project also allows Forcepoint DLP to automate the management of data using customized policies. The moment the user sends the information, the email/data connects to the DLP engine, which then immediately scans the information and declares it either appropriate for sharing or it will not deliver the information. The notifications the DLP engine sends to users have also helped them become more aware of the significance of data they have stored on their endpoints and are sharing. For example, a user may never have considered a document to contain sensitive information until attempting to send it outside the company and is notified that the send is blocked.

More focused data security means a drastic reduction in false positives and a more agile workforce

Shortly after implementing and fine-tuning policies in the Forcepoint DLP solution, the team saw a surprising result: a "drastic" decrease in the number of false positives recorded in a given week. This was made possible by replacing very restrictive policies that alerted on non-risky activities with policies more focused on restricting movement of data that actually needed protecting and activities that were actually troubling. After confirming the results via a network audit, the company felt comfortable allowing users to access sensitive data they needed while on and off the corporate network, without the risk of data leakage. A year after implementing the solution, a subsequent audit on the company's network further enhanced the value for the company. According to the CIO, whatever minor issues found in the system were fixed immediately.

During that year, the company also saw a cultural shift to increased data awareness. "Post DLP implementation, the end-user started to realize the importance of his data," according to the CIO. "Now, if any employee sends an email to his personal email, he instantly receives a notification regarding policy violation. I often get calls for clarification of the breach. DLP has brought in a big cultural transformation within the company and made everyone extremely sensitive to information security."

For a company that thrives on partnership, it's unsurprising that the team now sees Forcepoint as a valued partner. "Since the project was implemented, there is strong visibility of our organization within Forcepoint," explained the CIO. "Most of the Forcepoint leadership team is well known to us."

The partnership recently expanded with the addition of Forcepoint Web Security. The company was previously simply using a firewall for web security, but Forcepoint was able to demonstrate that Forcepoint Web Security integrates well with the Forcepoint DLP solution and provides another channel where data protection is enhanced.

Results

Drastic reduction in false positives.

Employees freed to access sensitive data off the corporate network, without risk of data loss.

Increased employee sensitivity to the value of the data stored on their endpoints.

"DLP has brought in a big cultural transformation within the company and made everyone extremely sensitive to information security."

GROUP CIO