Customized Data Protection Keeps up with This High-Speed Enterprise

This Fortune 50 telecommunications provider found itself in an untenable position—choose between speed to market or locking down its most sensitive data.

This global telecommunications enterprise knew every minute counts in their hypercompetitive market. The race to 5G is relentless—winners and losers are chosen by how quickly companies can take their proprietary ideas to market. Safeguarding data and intellectual property is paramount. Yet, most of today's security solutions are known to disrupt business and slow down progress. The security team knew they needed to protect their data with a solution that allowed fast, open access and movement.

CUSTOMER PROFILE:
This telecommunications enterprise is a Fortune 50 company with hundreds of billions in annual revenue.

INDUSTRY:
Telecommunications

HQ COUNTRY:
United States

PRODUCT:
Forcepoint DLP

Data breaches don't just impact business operations—they are a huge factor in customer trust. So, when this global telecommunications enterprise was fined for a breach of customer data that its existing DLP product neither prevented nor detected, its security team knew it was time to take additional safeguards.

Balancing safety and value creation

Today's telecommunications industry is a hyper-competitive market, particularly as the enterprise races against competitors to lock down market share of the next big technology. Keeping business moving is, perhaps, the top priority for enterprise leadership—and that puts extra pressure on the security team to do their jobs without slowing things down.

The high level of competition in the industry means that the enterprise is under constant pressure to innovate, share information, and move quickly—so much so that they lean toward freeing the business with fewer data controls over completely shutting down data loss, even if that means taking some risks.

> "We knew that with a strong partnership, we could calibrate the product to meet their specific needs."
>
> **STEVE WALLSTROM**, FORCEPOINT ACCOUNT EXECUTIVE

"Customer data and intellectual property make up the lifeblood of their business," said Forcepoint Account Executive Steve Wallstrom, "so that's why DLP is such a critical technology for them. But that's also what makes it so challenging—their rapid pace of growth means data access and movement must be as frictionless as possible."

To achieve a better balance between securing data and IP without interfering with progress, the enterprise needed more than a product—they needed a partner to help them balance safety with the speed of innovation.

Cultivating a solution that keeps up with high-stakes, high-speed growth

Sensing the need to get data protection closer to their users, the enterprise security team sought a data loss prevention solution that could safeguard their endpoints, stopping exfiltration incidents without blocking access to vital information. After investigating several competitive solutions, the enterprise turned to Forcepoint DLP endpoint technology for its ability to do just that within a very large enterprise environment—inclusive of reporting and visibility into hundreds of thousands of endpoints.

"With the enterprise's complex needs, a static, one-size-fits-all environment was never going to cut it," Wallstrom said. "But we knew that with a strong partnership, we could calibrate the product to meet their specific needs."

One differentiating feature of Forcepoint DLP that has proven successful within the enterprise is its real-time employee coaching on safe handling of sensitive data. Pop-up windows appear to help guide employees to make better decisions when interacting with sensitive or regulated data. In this way, the enterprise is making data protection part of its internal culture.

Reducing data vulnerabilities and optimizing staff time

Overall, in its first two months of deployment, Forcepoint DLP detected and prevented more than 200,000 data violations. "That's estimated at millions of dollars a month in risk that we're helping them to avoid," explained Wallstrom.

Challenges

Safeguard sensitive personal data and valuable intellectual property without slowing down business growth and innovation.

Approach

Implement a data loss prevention (DLP) solution continually tuned to the needs of a large enterprise with thousands of users.

"The enterprise says that we're not just a great technology provider, we're a great partner. We bring both to the table."

WALLSTROM, FORCEPOINT ACCOUNT EXECUTIVE

On top of that, the real-time employee coaching—pop-up windows that appear to help guide employees to make better data handling decisions—included with Forcepoint DLP has resulted in a 34% decrease in potentially compromising data being shared in and out of the enterprise. Employee coaching educates users to re-evaluate distribution of sensitive content.

"This gives them more time to focus on other strategic efforts to move the business forward," said Wallstrom.

220,000+

data violations blocked in the first two months

34%

decrease in employees sharing potentially compromising data

Evolving data protection for whatever tomorrow brings

As the enterprise continues to tune DLP policies for its complex environment, the collaboration continues. The teams meet on weekly "tuning calls" to exchange best practices and unique insights around additional policy optimization.

"The enterprise says that we're not just a great technology provider, we're a great partner. We bring both to the table," said Wallstrom.

Moving forward, the security team is exploring Forcepoint Dynamic Data Protection for the added value of behavioral analytics, individualized policy enforcement, and automated policy adjustments based on risk.

"We're confident that these security solutions will contribute to fast-paced business growth safe from vulnerabilities, and we'll be right beside them as they continue to fine-tune their environment. We're proud to be a part of their success."

Results

- More than **200,000 data violations** blocked in first two months of deployment, avoiding millions of dollars per month in risk.
- **34% reduction** in sensitive data movement when employees were encouraged to re-evaluate via pop-ups.
- **Fewer false positives**, allowing for focus by security team on the truly risky activities.
- **Long-term partnership** fine-tuning the solution as new challenges emerge.

Forcepoint