

Italian Defense Contractor Centralizes, Standardizes Security for a 'Galaxy' of Merged Companies

Following major corporate consolidation, this Italian aerospace and defense company teamed up with Forcepoint to wrangle a half-dozen different cybersecurity frameworks into a single, integrated system.

This leading aerospace and defense contractor faces a major, ongoing cybersecurity challenge as it acquires other companies and folds them into a security framework that must safeguard vital, global security-level IP and corporate data at more than 180 physical sites worldwide. The company recently underwent a complete reorganization of its subsidiaries and new acquisitions, placing everything under one corporate umbrella to create more centralized direction for its various business units, as well as to foster more synergy between them. It partnered with Forcepoint for a universal solution integrating web and email security, firewall protection, and data loss prevention.

CUSTOMER PROFILE:

Leading aerospace and defense contractor producing aircraft and other military products for NATO members and other customers.

INDUSTRY:

Aerospace

HQ COUNTRY:

Italy

PRODUCTS:

- › Forcepoint Web Security
- › Forcepoint Email Security
- › Forcepoint Next Generation Firewall
- › Forcepoint Data Loss Protection

Maintaining robust IT security during corporate restructuring is a difficult undertaking in the best of circumstances. When the stakes are as high as they were for this leading European aerospace and defense contractor during its recent reorganization, there's next to no margin for error.

The intellectual property (IP) and other sensitive data the company must protect includes intelligence vital to the national security of its NATO customers and other clients. When it recently began a massive restructuring to reorganize all of its subsidiaries and acquisitions into four main business areas and seven operational divisions, it was vital to make sure there was no interruption to network and data security during that process.

In addition to maintaining the highest security levels during the reorganization, the company also wanted to deploy an integrated security solution that would deliver a single, cohesive blend of web and email security, firewall protection, and data loss prevention across all of its business units to safeguard IT operations at more than 180 physical sites around the world.

Turning a 'galaxy' of independent business units into an integrated company

When the company first undertook its consolidation project, the IT security team was faced with a 'galaxy' of different business units, all operating under one umbrella but many with their own customized, siloed approaches to cybersecurity. Migrating all of these business assets to a single, integrated, centrally controlled security architecture was going to be a challenge, said the head of marketing for Cyber Security, Intelligence, and Digital Infrastructures.

"You can imagine the complexity of the process of merging all these businesses together as a whole, and consequently, the difficulties at the IT level of maintaining security and service levels,

especially considering that the company manages contracts and information for a great many critical customers in the government, security, and military arenas," he said

The first step was to install a new organizational and operational governance model to convert the enterprise from a "federation" of mostly independent companies to a single, harmonious, integrated company. IT security leaders were tasked with building a company-wide security posture that could accommodate the reorganization of assets into five main areas of activity:

- Electronics
- Helicopters
- Aircraft
- Aerostructures
- Cybersecurity

The company was further divided into seven operational divisions made up of subsidiaries grown organically and acquired, with origins—and security cultures—both Italian and foreign. Each of these divisions maintain offices, factories, and other physical locations around the world that needed the best cybersecurity to protect against cyberthreats and data breaches.

Unifying and centralizing cybersecurity governance

The company decided to build on the fact that the majority of its business units were already using Forcepoint Web Security. The company's security team selected Forcepoint Email Security, Forcepoint Next Generation Firewall (NGFW), and Forcepoint Data Loss Protection (DLP) for company-wide deployment, in part because those solutions would be easy to integrate alongside Web Security, which would also be deployed throughout the business divisions not yet using it.



Challenges

Consolidating and centralizing cybersecurity as a single, company-wide solution across previously independent business units.

Safeguarding data with the highest level of security across the world.



Approach

Building on existing Forcepoint Web Security installations across the company, added Email Security, NGFW, and DLP to create a robust, integrated cybersecurity platform.

Equally important were the capabilities of those solutions, the cybersecurity lead said. For example, the company selected Forcepoint NGFW to make it possible to unify and centralize the governance of the company's network security infrastructure, which helped reduce the number of tasks and incident responses being managed by the IT security team and simplified operational processes.

It picked Forcepoint DLP after a Proof of Concept demonstrated that the solution was the best available to align with an overall security strategy towards data exfiltration and data loss, the cybersecurity lead said. In particular, Forcepoint DLP was the best of all competitive solutions in three key areas:

- Scaling with the company's growth
- Protecting foreign branches from data loss
- Integrating seamlessly with the Web and Email solutions

Flexible but strong protection exceeds expectations

Comfortably into their Forcepoint deployment, the IT security team reports that their goal of centralizing control over the security protecting all of their business units and physical locations has been a success. The team has especially appreciated the flexibility and customization capabilities of Forcepoint Web and Email Security, NGFW, and DLP.

"Forcepoint was the answer to our need to align our posture against external and internal security threats."

CYBERSECURITY LEAD, ITALIAN DEFENSE CONTRACTOR

Specifically, with Web Security and DLP, the company has been able to customize policies for different users in response to the specialized needs of R&D, manufacturing, sales and marketing, and other business disciplines. The team's appreciation for Email Security was established when they found out they were able to seamlessly maintain and augment the email rules established by the previous solution with no interruption to the level of email flow in the transition process.

The upshot is that the company has been able to harness its galaxy of businesses without losing any of its star power to data leakage or theft.

"The strategic direction we wanted to take was to move from simple web security to a much more integrated, comprehensive data loss prevention strategy including web, email, and data protection. Forcepoint was the answer to our need to align our posture against external and internal security threats," the cybersecurity lead said.



Results

Accomplished centralization of control over cybersecurity.

Reduction of tasks and incident responses for internal IT team.

Foreign branches now protected from data loss.

Platform allows for easy scaling to accommodate future growth.

