Defense Contractor Faces Down World's Most Sophisticated Cyber Threats to Help Keep the Nation Safe

One of the world's biggest defense and aerospace contractors turns to Forcepoint for security solutions that offer best-in-class protection against the most well-funded, government-backed data thieves on the planet.

This defense contractor owns some of the world's most coveted military and aerospace data—the kind of information and military intellectual property (IP) that draws the attention of nation states. As a globe-spanning organization with a workforce numbering nearly 70,000, it needs IT security that won't slow down its daily business operations and meets the demands for easier data-sharing by customers like the U.S. government—but that can still protect national security-related data. Forcepoint's integrated suite of cybersecurity solutions provide behavior-centric protection from inside and outside threats, from the cloud to the data center.

CUSTOMER PROFILE:
Major U.S. defense contractor with concentrations in weapons, military, and commercial electronics and 67,000 employees.

INDUSTRY:
Aerospace

HQ COUNTRY:
United States

PRODUCTS:

- Forcepoint Web Security
- Forcepoint Email Security Secure Messaging
- Forcepoint DLP
- Forcepoint Insider Threat
- Forcepoint Behavior Analytics
- Forcepoint NGFW

Companies of all sizes and types must protect internal data against cyber threats, but very few face security stakes as high as this defense contractor does. Ordinary companies might have to deal with fines, lawsuits, and a loss of reputation following a data breach. This defense and aerospace giant knows there could be serious national security implications if the data it safeguards ever falls into the wrong hands.

"We build all the things that are key to protecting our warfighters in the field and keeping our nation safe. And if we lose those plans and those techniques to our adversaries, it's going to affect our national security," explained the company's CISO.

"It's not going to be good for your kids or my kids. So, we work very hard at security and we're deadly serious about it."

The attack surface the company must protect against threats is vast. The publicly traded, Fortune 500 company has a global workforce some 67,000 strong and had revenues of $27.1 billion in 2018. The contractor safeguards some of the world's most sensitive IP in its offices, on its manufacturing floors, and at military installations all around the world.

Meanwhile, the types of malicious actors threatening the company aren't just criminals looking to steal some personal financial information or run a ransomware scam. The bad actors the company has to deter can come from the world's most sophisticated criminal and nation state organizations.

The rising threat of the inside job, driven by outside forces

"The biggest change we've seen in cybersecurity in the last decade is the rise of the nation state threat," the CISO said. "In the early years, they were attacking us much less than they do today over the course of a year, a month, a day."

"And now as we've gotten better at defending against external attacks, the nation state has moved more towards trying to find other vulnerabilities in the supply chain and we've seen much more of a focus on trying to cultivate insider threats. Security is just a whole different job now than it was ten years ago."

A result of this has been the increase in attempts at data exfiltration over the past several years —stealing data via insiders rather than breaking into an organization from the outside.

The company sees this development as a natural evolution in the threat landscape. As IT security has become much better at preventing breaches that are launched externally, the most advanced attackers have shifted to trying to enlist witting or unwitting accomplices from inside organizations or within the ranks of their business partners.

The company's IT team uses Forcepoint Data Loss Prevention (DLP), Forcepoint Insider Threat (IT), and Forcepoint Behavior Analytics (FBA) as its shield against such exfiltration threats. Unlike reactive data loss products, which only initiate action after an exfiltration incident has occurred, Forcepoint DLP constantly monitors and analyzes an organization's users and devices to flag behavior that looks like it might lead to a data breach. When such an exfiltration threat is determined, DLP can block actions like unusual attempts to move files to a thumb drive or cloud storage platform.

The company has also deployed IT, which is designed primarily as a forensics tool but can also help detect and prevent malware infections.

"Forcepoint Insider Threat is a great investigation tool because it captures the video of what someone does and you can use it for evidence after a breach and say, right there, this is what you did, we can prove it," the CISO said.

The company has also used IT to identify anomalous behavior on critical systems and servers.

"IT has saved us many times," he said.

Challenges

Safeguard some of the world's most high-stakes IP in offices and manufacturing facilities around the world.

Adjust to increased threat of insider data exfiltration.

Adjust to increased use of cloud-based technologies by partners like the Pentagon.

Approach

Rely on a suite of Forcepoint solutions including Forcepoint Email and Web Security, DLP, IT, FBA, and NGFW.

Adding a strong perimeter defense against outside attackers

New challenges like internal threat protection may get the headlines, but CISOs understand that it's still just as important to maintain a strong perimeter against outside attackers. The company uses Forcepoint Next Generation Firewall (NGFW) in conjunction with Forcepoint Web Security and Forcepoint Email Security to make that perimeter more robust.

A big priority is to ensure that the crucial work the team does isn't made even more difficult by security products that require excessive hands-on administration or generate too many security alerts. That's why NGFW's rich central console capabilities, high-accuracy threat defenses, and superlative uptime and dependability were so appealing.

"We literally have hundreds and hundreds of firewalls around the world and we manage them all centrally to ensure they're consistent," the CISO said. "When we had Cisco firewalls, we had to touch each of those firewalls individually.

"And when you do that kind of manual administration, it's not just time-consuming, but you can more easily introduce mistakes and you can risk consistency. Once a firewall goes down, data stops flowing. Manufacturing lines come to a halt. Engineering comes to a halt. The customer can't get ahold of us. Proposals don't get uploaded. The risk to the business of a firewall going down is huge."

It's also critical to protect communication channels and the data exchanged within them. The cybersecurity team relies on Forcepoint Email Security's Secure Messaging for email encryption and a permissions-based secure end-user portal for the transmission and viewing of personally identifiable data in email.

Keeping pace with the cloud revolution, securely

Looking toward the future, the increased reliance on cloud-based technologies by the Pentagon and other organizations is a development that can create headaches for CISOs.

In the past, the company and its customers shared data with each other almost exclusively over dedicated, closed circuits. But the cloud revolution has changed how businesses operate and that means the company has had to adapt to customer needs.

"In the past, we just blocked services like Dropbox, right? Because no one needed them. They were just a risk."

"We can't block those services and applications anymore because our own customers are demanding to use them to share proposals and data. Instead, we have to have a way to maintain very tightly controlled access to this cloud storage, as well as to some other Software-as-a-Service tools."

The company is planning to answer some of the risks opened up by the cloud with Forcepoint Cloud Access Security Broker (CASB). A Proof of Concept proved out the use cases the company was most interested in, and the solution is scheduled to roll out next year. The key to CASB, the CISO said, is that it allows the company to more easily set rules for which employees can access different cloud applications.

"The biggest thing is that without CASB, you have to open up the entire company to the cloud or none of it. With CASB, we can make access to different cloud services role-based and thus limit our exposure to 2% of our population instead of 100% of our population," he said.

Results

Best-in-class security posture that allows employees, including 40,000 engineers, to go about their work productively, efficiently, and creatively.

[Defense-Contractor-Customer-Story-US-EN] 12May2020