Materials Science Research and Development

This case study is based on a global materials science company with a long history of developing materials that are critical to the defense of the United States. They pride themselves on their ability to take on difficult technical challenges and solve them in a way that delivers the highest quality products to their customers throughout the military/ defense supply chain.

This research and manufacturing organization has tens of thousands of employees and works with thousands of vendors around the world. Their suppliers range from raw materials and commodities brokers to speciality engineering consulting firms which help assure that the company provides the highest quality materials and products to their customers.

Company At-A-Glance

80,000+
global employees

10,000+
suppliers

$25 billion
2019 Revenues

Customer Challenges

Many of the chemical formulas and manufacturing processes involved in the creation and production of the materials that this company delivers are governed by strict export control regulations. These laws, established by the US Department of Commerce and enforced in partnership with the Departments of State and Justice, restrict how specific technologies must be protected from both intentional and unintentional exports.

As with many multinational enterprises, this industrial conglomerate worked to reduce their IT operations costs by outsourcing and offshoring many of their technology and engineering functions. Most of their export controlled data was stored in SharePoint sites and on legacy network file shares which had very strict end-user privileges applied to them. They had also transitioned to use Office 365 for messaging and collaboration. Unfortunately, most of the system administrators who had privileged access to those SharePoint sites, file servers and Office 365 Global Administrator privileges were no longer US citizens residing in the US. This created a significant compliance problem for the company.

This created a significant compliance problem for the company.

Customer Challenges

> ...meaning that global administrators (all located in India) could gain access to every bit of information shared...

In addition, when engineering work was outsourced, most of the documents and design files were sent over email to and from the outside engineering consultants. Both the company and the engineering consultants are Office 365 subscribers, meaning that global administrators (all located in India) could gain access to every bit of information shared through email, OneDrive or any other Microsoft service. This left significant gaps in the protection of critical intellectual property throughout the engineering and production lifecycle of the company's products.

In many cases, development projects would proceed so quickly that team members (both employees of the company and outside suppliers and contractors) would resort to the use of WhatsApp and other consumer-grade messaging platforms. The use of these technologies has resulted in significant regulatory and compliance risks for the company, as there is no traceability of information shared through these channels, nor ability to track precisely who is and is not sharing information.

HighSide's Solution

HighSide partnered with this customer to develop a **collaboration solution** which solved both the regulatory and intellectual property protection risks. The enterprise wanted to deploy a system which would **protect the intellectual property** from non-US citizen/resident IT administrators as well as provide **end-to-end encryption** to share engineering information with outside partners and suppliers.

By choosing HighSide's **ultra-secure** messaging and distributed-identity platforms, the organization was able to **reduce the risks** associated with internal privileged user access to information as well as enhance the security of sharing data with outside engineering and supply chain partners.

HighSide's Solution

HighSide
Ultra-Secure Messaging Features:

- End-to-end encryption
- Mutual authentication for every user session
- No Active Directory account required for outside users
- Integration with Active Directory for internal user provisioning
- All information shared through the system is retained in compliance logs
- Access can be revoked immediately when users leave the project

HighSide
Distributed Identity Multi-Factor Authentication Features:

- Integration with Next Generation Firewalls to protect applications or servers
- Location-based restrictions to prove the actual location of all users accessing application data
- No single-point-of-failure for backend operations
- Only company users' identities are provisioned, avoiding the problems of shared identity platforms like Okta and Microsoft Azure

Results

By using HighSide messaging and identity services, the company has improved the protection of their critical intellectual property and significantly reduced the likelihood of regulatory compliance problems. These goals have been accomplished while simultaneously giving users much greater flexibility to communicate with each other on both thick clients (desktops and laptops) as well as mobile devices (iOS and Android).

By providing easier-to-use collaboration tools to team members, research and development activities have accelerated, leading to the delivery of improved materials which are used to protect US military service personnel and their allies. HighSide's strong security controls combined with compliance logging functions, make team administration tasks easier and have reduced the overhead associated with regulatory reporting and other compliance tasks.

All of these improvements and enhanced capabilities have been delivered to the company by HighSide at a fraction of the cost of competing cloud-based and less-secure offerings. HighSide's zero-trust architecture combined with ease-of-use have enhanced the organization's collaboration efficiency and significantly reduced the likelihood of the loss of critical intellectual property or regulatory compliance problems.

For the first time in my 30 years working here, we have a reliable and secure way to communicate with team members and suppliers without having to worry about loss of our intellectual property or regulatory compliance problems.

Director Research and Development IT at a global materials science company