BITSIGHT

CASE STUDY

Mitigating Supply Chain Vulnerabilities

Like all government agencies, NASA takes cybersecurity very seriously, understanding that any security compromise can result in the postponement of multi-million-dollar missions and even loss of life. However, since the agency relies on more than 3,000 vendors to achieve its mission, threat actors have multiple pathways for infiltration.

Protecting this extensive supply chain has been a long-time challenge for NASA. To identify potential vulnerabilities, they have traditionally relied on manual risk monitoring procedures, public disclosure statements, and breach notifications—which were usually only reported by larger vendors.

According to Kanitra Tyler, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Service Element Lead at NASA and a 30-year veteran of the space administration, the team needed more in-depth, detailed, and real-time security information.

- Aerospace/Defense Industry
- Washington DC
- 18,000 employees

Challenge:

To gain visibility into the complete attack surface through real-time security data and to identify the most important risk areas to remediate.

Solution:

TPRM

> “We use Interos, one of Bitsight’s valued partners for third-party risk management, which provides great insights into things like geopolitical and financial risk. But we needed to take a much deeper dive into our suppliers’ cybersecurity postures.”

Kanitra Tyler

Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Service Element Lead at NASA

Deeper insights into NASA's extensive supply chain

In response to that need, enter Bitsight for Third-Party Risk Management (TPRM). With a deep integration with Interos—a leading governance, risk, and compliance (GRC) tool—Bitsight provides deeper insights into third- and fourth-party vendor risk profiles. Now, NASA can:

1

Uncover high risk vendors that may be using banned services under Section 889 of the National Defense Act.

2

Ensure vendors' cybersecurity postures meet the administration's specific requirements and guidance included in the NIST Cybersecurity Framework.

.

3

Accelerate cyber risk assessments with better focus and prioritization of supply chain risk management.

4

Measure exposure to cyber risk using data-driven security ratings.

5

Work with suppliers to reduce their own risk and, as a result, pose fewer threats to NASA.

> "At NASA, we focus on what we call the three P's—pedigree, providence, and position, Bitsight helps enormously with the first two. We can now easily identify the vulnerabilities associated with a particular vendor and how those vulnerabilities could impact our own security posture—before we begin working with them."

Kanitra Tyler
Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Service Element Lead at NASA

Improved efficiency, stronger security

NASA also struggled with taking proactive and corrective action when necessary due to the time it took to monitor its vendor portfolio. With countless vendors and the need to reassess and remediate vendor security issues, NASA needed a more efficient process.

Through Bitsight, NASA was able to improve its processes dramatically with daily alerts and easy-to-understand metrics on changes to vendors' security postures – to help them prioritize risk. Per Tyler, "Bitsight has allowed us to automate our security

monitoring process, resulting in about 50 percent time and efficiency savings. We can sign into Bitsight and get real-time information right from the easy-to-use dashboard." But for Tyler, Bitsight's technology and data is only the beginning of what makes NASA's relationship with Bitsight so valuable. The service and support Bitsight provides is equally important and has helped the agency remain protected from potential threats.

"I can think of at least three instances where Bitsight alerted us to major security issues that could affect NASA so that we would be better prepared," she said. "In each instance, Bitsight provided us with detailed reports and advice that allowed us to make better decisions while protecting our supply chain."

"I can think of at least three instances where Bitsight alerted us to major security issues that could affect NASA so that we would be better prepared," she said. "In each instance, Bitsight provided us with detailed reports and advice that allowed us to make better decisions while protecting our supply chain."

> "Flying to space is our primary mission and area of expertise, not cybersecurity. For that, we want to partner with someone who understands that discipline and how to manage it well. Bitsight is that partner.
>
> Kanitra Tyler
> Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Service Element Lead at NASA