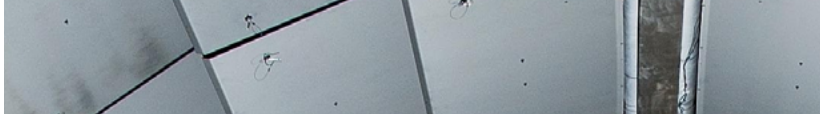
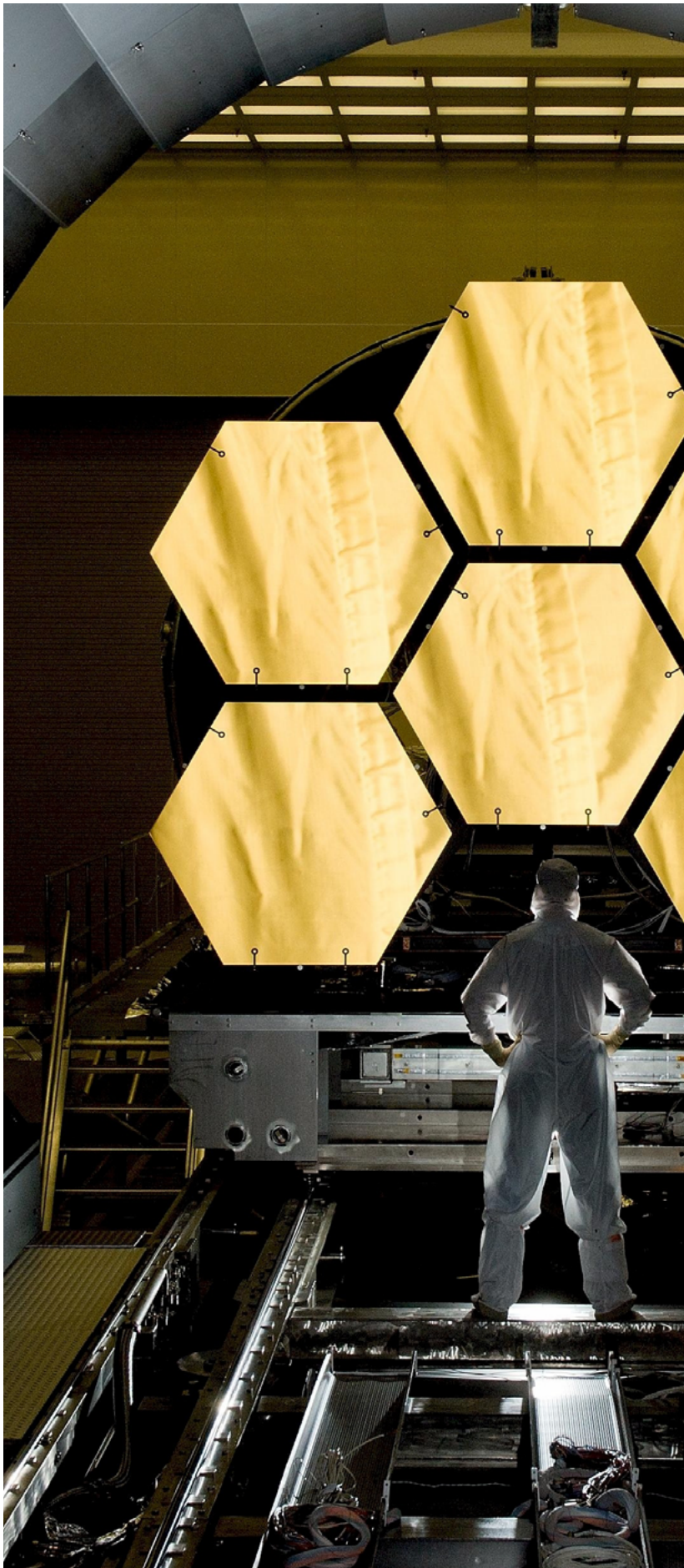
CUSTOMER STORY



RAPID7



Exponent

Secures Clients' Data With Rapid7 InsightVM Platform and Managed Detection and Response Service

Products

- InsightVM
- Managed Detection & Response

Size

- Enterprise (Mid-Size)

Overview

The Company

Exponent is an engineering and scientific consulting firm whose customers include corporations, insurance carriers, government agencies, and law firms. The firm is best known for its analysis of accidents and other failures to determine their root causes. NASA hired Exponent to examine possible causes of the Space Shuttle Challenger disaster. FEMA contracted with the firm to examine the damage in the aftermath of the deadly Oklahoma City bombing. Exponent was also called in to investigate the infamous Exxon Valdez oil spill. More recently, Exponent has expanded its services to analyze new products or processes to help avert potential future problems.

The Challenge

With 1,500 employees distributed across more than 30 locations supporting clients in the U.S., European Union and Asia, Exponent's major security challenge is keeping its data safe and secure. That responsibility falls on the shoulders of Daniel Shuler and his information security team. Reporting directly to the CFO, Shuler was brought onboard in 2019 to formalize the way Exponent addresses security.

"We focus on protecting our clients' data to the best extent that current technology will allow and do it in a concrete way that allows us to demonstrate we have the right security tools in place," explains Shuler. With its constantly evolving roster of clients and projects, new field offices, and diverse technologies, a large part of Exponent's security challenge is related to the need for greater visibility across its diverse environment.

"Our challenges are related to the visibility of assets in use, the networks in use, and our diverse offices," notes Shuler. "It's all standardized, but it's constantly changing. We have a standard technology stack in each office with the same servers and network gear." But Shuler points out there are many variables required to accommodate each client's work; it could be adding a new work location or new technology. "We need to make sure we're at the table for the right conversations; the technologies we're specifying and requiring are being leveraged correctly and that everybody is operating within our policies," continued Shuler.

The Solution

Visibility Into a Constantly Changing Environment

Shuler's solution for visibility was implementing Rapid7's vulnerability tool, InsightVM, along with Rapid7's Managed Detection and Response (MDR) service. "Our consultants are very mobile," says Shuler. "A large percentage of our work can happen offsite; at a client site, a hotel, or a home office. We needed a technology stack that followed our users. Rapid7 fits right into that bucket because it offers a light-weight agent that can be deployed on end user devices and be with them wherever they go. Our whole strategy was to move with the user. We 100 percent rely on the Rapid7 agent deployment to carry this through."

In addition to providing vulnerability information, Rapid7's vulnerability management solution, InsightVM, performed asset discovery scans that identified each node on Exponent's network. Now Shuler's team also relies on InsightVM scans to identify any new devices that are added to the network.

"Rapid7's InsightVM technology is rock solid. It does exactly what we need it to do," continues Shuler. "It integrates with the MDR service through a shared light-weight agent that provides a rich source of data. The agent has multiple capabilities, and we like that very much."

24/7 Security Team

When Shuler first joined Exponent, the company did not have an in-house security team. Shuler knew from experience it would be all but impossible to provide around-the-clock security coverage on their own. While becoming a round the clock operation is difficult for teams of many sizes, he mentioned that one of his previous companies had a large, in-house SOC (Security Operation Center) and coverage was a challenge. "Then, we had to rely on our SIEM and other technologies to make enough noise during off hours. Think about it – a big team couldn't do 24/7. That's why we purchased Rapid7 MDR service on day one. We knew we couldn't do it with a small team."

Our clients' entrust their data to us. They want to know what we do for security; do you operate a SIEM? Do you correlate data? Do you manage or monitor 24/7? Rapid7 checks all those boxes for us. The correlation expertise through both the technology and the people in the SOC has proven many times over to be accurate and valuable

Daniel Shuler

"Rapid7's MDR gives us visibility. We understand where the users are, where the devices are. One of my favorite aspects of the MDR service is the ability to get into the console and look at the map showing where our incidents, events and devices are operating from – it's powerful to be able to pull that up and see, 'There are five people working in a different country than they usually do and they are connected to our VPN in Phoenix."

Shuler works very closely with the Rapid7 MDR SOC. "We've worked with the Rapid7 team to define what metrics need to be gathered, such as firewall logs, web proxy or mail gateway, whatever it takes to give the system enough data points to correlate and give us good results. It's not a static environment. It's been consistently updated and changed to adapt to our changes and to adopt new capabilities available within MDR, like cloud support. We were not an AWS customer when I got here and now we are. There has been a transition of log sources and agent deployments. The MDR service continues to monitor and give us visibility into our environment."

A Security Platform that Evolves Along with Exponent's Mission

Over the past three years, Exponent's security program has expanded and matured alongside Rapid7's products and services. "Rapid7 reporting is consistent month after month. With InsightVM we look at the number of devices and the number of vulnerabilities we have. On the MDR side, we monitor the number of events. It is super valuable to our security program. Rapid7 can consistently show us what is going on in our environment."

As for compliance measures, Rapid7's InsightVM and MDR meet the security criteria desired by the firm's clients. "Our clients' entrust their data to us. They want to know what we do for security; do you operate a SIEM? Do you correlate data? Do you manage or monitor 24/7? Rapid7 checks all those boxes for us. The correlation expertise through both the technology and the people in the SOC has proven many times over to be accurate and valuable."

On a personal level, Shuler credits Rapid7's around-the-clock support with giving him downtime. "I enjoy my sleep. So, if somebody says I'm going to give you 24/7 support and only wake you up when it's necessary, that works great for me. The MDR SOC only escalates the critical alerts we need to act on." Security, visibility, expert support, and a solid sleep schedule. Solutions and then some for Exponent's information security team.

24/7

MDR Team Coverage

RAPID7

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/