Powering the Industry that Powers the World - Securely

RANDORI RECON | CASE STUDY

OVERVIEW

NEED

To support digital transformation efforts and reduce their risk, NOV needed continuous visibility into their external attack surface.

SOLUTION

Randori Recon enabled NOV to gain continuous visibility into their external attack surface and proactively identify unknown or misconfigured systems, such as Log4j, before attackers.

BENEFIT

NOV now has continuous visibility into their attack surface and has been able to reduce their external risk including shadow IT, misconfigured systems, unapproved services, and legacy applications.

NOV is a leading supplier to the global energy industry. Founded in 1862, the company conducts operations at more than 500+ locations across six continents and develops cutting edge technology for the energy industry. To remain competitive and ensure the security of energy operations, it's essential that NOV have a firm understanding of its external attack surface at all times.

With a third of successful breaches now originating from Shadow IT and ransomware attackers increasingly targeting exploitable applications, having a firm understanding of their attack surface has never been more essential. To meet this need, NOV relies on Randori Recon to provide an external perspective of their environment.

While attacks against energy companies have recently been in the news, NOV's security leadership team has been incredibly proactive - recognizing the threat posed by unknown assets years ago. An early adopter in attack surface management - NOV first partnered with Randori in 2019.

> "As a critical part of the global energy supply chain, our families and our customers depend on NOV to securely deliver products and services. Randori allows us to be proactive - identifying risks before they become issues. As our eyes and ears to what's exposed, Randori is our first line of defense against unapproved services and evil."
>
> **- John McLeod**
> Chief Information Security Officer at NOV

PW220128

BUSINESS PROBLEM TO BE SOLVED

To ensure its global team could stay connected, NOV has invested heavily in digital transformation - migrating legacy workloads and applications to the cloud and adopting SaaS based applications. With multiple data centers, a hybrid cloud environment, and a highly complex corporate IT environment, assembled through multiple mergers and acquisitions over the years – IT environments were a constant challenge.

Critically important to an organization the size of NOV is Randori's unique ability to identify external facing assets and prioritize them by attackability. Leveraging our patented Target Temptation technology, NOV has been able to dramatically reduce the number of high and critical issues requiring attention - from tens of thousands of issues to a few dozen. This allows the NOV team to take action faster and ensure they remediate the most critical exposures first.

> "It's not enough to just have asset management anymore. You have to have a way to find assets and risks you don't know about - especially those that are externally facing. Randori allows us to get ahead of the next attack by reducing risk and cutting off attack vectors."
>
> **- Casey Lee**
> Director IT Security at NOV

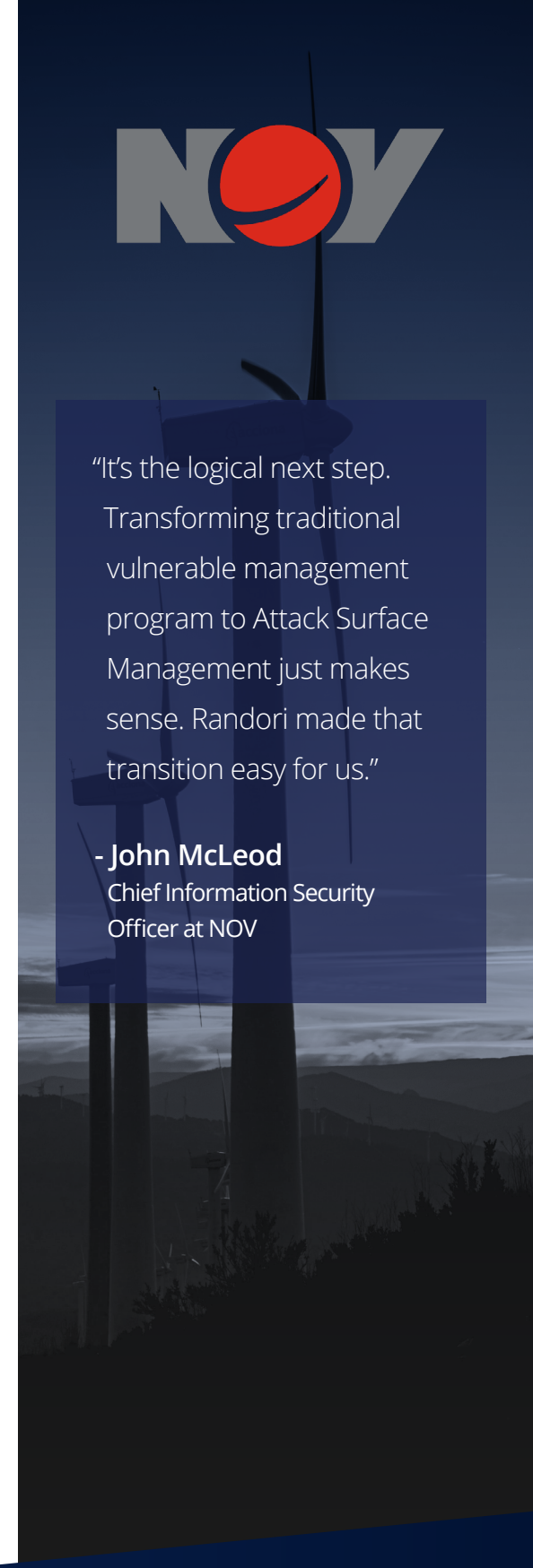
BUSINESS BENEFIT OF RANDORI

Armed with continuous visibility into their external attack surface, NOV now has a firm grasp on external assets and has been able to take steps to reduce their risk and respond quickly to emerging threats, such as Log4j.

"Before Randori Recon, we were struggling to maintain a continuous view of our external assets. It was incredibly time consuming and a never ending battle. When Log4j exploded onto the internet, I was able to pull data from Randori Recon in seconds and provide my team with actionable information. The way Randori Recon prioritizes targets, allowed us to remediate within hours, not days."

- Casey Lee
Director IT Security at NOV

NOV is now looking to expand their partnership with Randori to their internal network - extending the same visibility they get from Randori Recon to the inside and to begin testing the efficacy of their defenses with Randori Attack.



"It's the logical next step. Transforming traditional vulnerable management program to Attack Surface Management just makes sense. Randori made that transition easy for us."

- John McLeod
Chief Information Security Officer at NOV