Novacoast Gains an Advantage for its Security Intelligence and Response Business

Novacoast helps organizations find, create, and implement powerful security postures through advisory, engineering, development, and managed services. Comprised of advisers and practical hands-on problem solvers, Novacoast approaches client security from the perspective of business goals and assesses, diagnoses, and solves the digital security issues unique to its customers' enterprise networks.

Business Challenge

As a company that manages digital security for other enterprises, Novacoast collects a lot of data about its customers. This includes identifying information, such as names and phone numbers, as well as the information Novacoast analysts gather during the course of their work, such as service desk tickets or even training materials the analyst might have accessed in order to respond to an incident.

"Since we provide and manage digital security for our clients, a digital security problem or data loss of our own would be extraordinarily detrimental for our reputation and business," said Adam Gray, Chief Technology Officer at Novacoast. "So, among our biggest priorities are risk avoidance and mitigation, as well as following security best practices. We don't fit neatly under a compliance umbrella in that we're not really regulatory driven. Rather, most of our standards are driven by customer requirements. Since they are driven by regulation, we have to comply to many of their requirements. In addition, protecting any data they give to us is a critical concern."

"But we wanted to take it a step further. Not only do we want to protect the data our customers give us, but we also want to protect the data we gather about them, which is distinct in itself. It's one thing if a customer sends us a document and we have to protect that through rights management. But it's entirely another thing for us to say that we also want our customers' privacy to be protected even if it's just the fact that they showed up in our service desk."

Novacoast Case Study

Technical Challenge

For Novacoast to appropriately track a customer security incident, it creates tickets in its security service ticketing system. Each ticket must be accompanied by case management information as it makes its way through the system, including customer name, contact details, and phone numbers. The ticket might also contain details regarding the request, and it usually will refer to an external system at the customer's site for additional information.

Novacoast wanted to protect this information, but, as Gray noted: "There are no off-the-shelf solutions for protecting this kind of data derived from our customer-related activities. So, we had to develop the solution ourselves."

Solution

In order to meet security best practices, Novacoast analysts had to do extensive modification, development, and automation within Novacoast's own security operation centers. That meant implementing a cryptographic solution to protect the business-critical information and applications.

Novacoast deployed Entrust nShield® Connect Hardware Security Modules (HSMs) to provide the root of trust for its data protection solution. Whether deployed on-premises or as-a-service, Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations.

Every time Novacoast reads or writes data from an application to the various systems that hold that data, the application uses the HSMs behind the scenes to transparently encrypt or decrypt that data at the record and row level. So, if someone ever broke in and stole the databases or got access to those systems, they still wouldn't have access to the unencrypted data – making that data useless to anyone who didn't have the encryption keys.

The Novacoast team built out the technology and partnered with Entrust to provide the cryptography. Entrust nShield HSMs are a critical part of the solution, protecting the encryption keys and providing the root of trust for the whole system.

"I'm a strong believer that if you don't do your cryptography in hardware, you don't own your cryptography," explained Gray.

> **"All of our cryptographic keys are locked in hardware, in Entrust nShield HSMs, and every time we write data about a customer, that data is encrypted everywhere it goes, whether in use, in transit, or in storage."**
>
> Adam Gray, Chief Technology Officer at Novacoast

Learn more about nShield HSMs at entrust.com/HSM

Novacoast Case Study

Hardware security modules are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. Entrust nShield HSMs are tested, validated, and certified to the highest security standards including FIPS 140-2 and Common Criteria. HSMs help enable organizations to:

- Meet established and emerging regulatory standards for privacy and cybersecurity, including GDPR, eIDAS, PCI DSS, and HIPAA.
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility

One of the reasons Novacoast selected Entrust nShield HSMs was the high standard of pre-sales technical knowledge and support. "Even before we were a customer, the Entrust team stepped up and helped us with some of the design and support criteria that we had questions about. They also provided guidance on sizing and infrastructure, information about how we were going to operate, and what we were going to build. They simply stepped in and provided us the attention and the expertise we were looking for," said Gray.

In addition, Entrust provided Novacoast with the PKCS#11 libraries it needed to trade information between disparate systems. The Entrust libraries adhered to pre-existing standards, and Novacoast didn't need to do anything extra to make them work. Gray observed that, "The crypto-libraries have been around for decades. But it's super important that you follow the standard, because that's what helps ensure your data will remain properly secure."

« Even before we were a customer, the Entrust team stepped up and helped us with some of the design and support criteria that we had questions about. They also provided guidance on sizing and infrastructure, information about how we were going to operate, and what we were going to build. They simply stepped in and provided us the attention and the expertise we were looking for. »

Adam Gray, Chief Technology Officer at Novacoast

Learn more about nShield HSMs at entrust.com/HSM

Novacoast Case Study

CUSTOMER PROFILE

Business need

- Protect business about customer security incidents and operations around them
- Meet best practice security standards
- Achieve competitive edge

Technology need

- Develop a ticketing and case-management security system, because no off-the-shelf solution existed for Novacoast's industry

Solution

- In-house development
- Entrust nShield Connect HSMs
- Entrust expertise and support

Result

- Efficient, effective protection of information collected around customer incidents
- Best practice security
- Competitive advantage

Result

Novacoast achieved its business goal of protecting the information it collects about its clients.

"We've streamlined our ability to properly protect the data we collect around our customers and, for us, that's by far the most important piece. But this has also given us a competitive advantage in the marketplace, because our competitors don't treat their data this way," concluded Gray. "But to us, the most important thing is knowing that our data is properly protected."

> **"But to us, the most important thing is knowing that our data is properly protected."**

Adam Gray, Chief Technology Officer at Novacoast

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223