

CASE STUDY

How Arctic Security helped RAVENii scale its business without hiring extra staff

Arctic Security

If there's one principle in the world of cybersecurity that becomes more self-evident with each passing day, it's that response-only cybersecurity strategies don't work.

Smaller organizations, in particular, often learn this lesson the hard way. They assume that cyber criminals mainly target large businesses and institutions (which are usually more lucrative) and gain a false sense of security. This leaves them vulnerable, with a lot to lose and little protection.

This is one of the problems that cybersecurity solution provider RAVENii has been focusing on solving since 2014.

> *"We create security programs for our clients by monitoring the entirety of the IT environment and, in doing so, move beyond the sphere of security breaches," says Eric Helm, Security Engineer and Network Architect at RAVENii. "We provide the most comprehensive discovery, analysis, and mitigation of threats associated with an organization's presence."*

Arctic Security is a dark web expert

RAVENii became familiar with Arctic Security not only through extensive research into experts on the subject of the dark web but also through a direct referral.

At the time, RAVENii noticed an increase in data breaches related to Personally Identifiable Information (PII). "This, combined with the recycling of password and intel lists through dark web exchange, made us want to change the way we worked," says Eric. "Our ideal solution was going to be to customize internal scripts to data-mine the dark web."

And that's what Arctic Security did. It stands out because the solution it proposes requires minimal client requirements, and its dark web coverage is part of a comprehensive suite of web security monitoring features. RAVENii would be able to become more efficient and provide better services without having to do extensive in-house software development and maintenance. This event would enhance RAVENii's cybersecurity awareness.

"RAVENii has a great brand," says David Chartier, CEO at Arctic Security. "They wanted to achieve the understandable goal of scaling their business without having to increase personnel. Arctic EWS would enable them to see vulnerabilities that would otherwise go unnoticed, and this gives them another layer of security."

Enhancing the client's stack

RAVENii implemented the new scripts by layering them on top of its existing threat and vulnerability monitoring services.

"Implementation was actually very simple," says David. "RAVENii prices per endpoint, which allows them to more easily add clients. They send us client IPs, domains, and so on, and then we activate Arctic EWS."

Since implementation, Arctic Security's solution has increased threat information visibility for RAVENii's clients' assets. It has enhanced its stack by making it much easier to identify the early signs of a security breach or vulnerable service by using reliable data.

"After implementation, we have had proper support through onboarding," says Eric. "We love that this solution is efficient and versatile as a standalone but also adds value as a harmonizing unit alongside our current cybersecurity management measures. We also love that it's easy to deploy and easy to use."

"RAVENii has had results-based success since we implemented the solution," says David. "The other night at a city board meeting, they were able to show exact examples of vulnerabilities they've been finding, as well as passwords on the dark web that are easy to hack. It was quite eye-opening for the customer and was a valuable teaching opportunity."

RAVENii

- Formed in 2014, the company is a team of experts that includes former CISOs from various industries
- Provides customised vCISO consulting services to clients
- Helps clients create and facilitate a comprehensive suite of security programs
- Uses a process called 'maturity modelling' to identify gaps in security posture and provides data-driven solutions to address those gaps
- Offers a range of services, including security and network assessments, vulnerability assessments, application testing, wireless security assessments, social engineering, transaction security, security program evaluation and development, vendor management, regulatory and compliance issues, critical security controls, and more