Bringing a leading cyber threat solution to businesses in need

Silverfern makes 24x7 threat detection and response more accessible and faster to deploy with IBM Security QRadar

by Josh Young

6-minute read

You've just read your third article this week about another ransomware that's threatening your industry. One of your suppliers went out of business last quarter thanks to a data breach. And your IT team now needs a bigger cybersecurity budget. Who would've thought running a business was this risky?

"Like everyone else, we've seen cyberincidents, like data breaches, increase significantly over the last four or five years," explains Liong Eng, Chief Executive Officer at IBM Business Partner Silverfern IT (link resides outside of ibm.com)—a premier cybersecurity company. "Boards are becoming more and more aware of the risk and of their accountability for any potential breaches. And those companies that recognize that this is now a business challenge—not just a technology one—have started restructuring their budgets to do something about it."

> “[W]e wanted to better extend our knowledge and capabilities directly to our customers—to become an integrated part of their security team.”

Liong Eng, Chief Executive Officer, IBM Business Partner Silverfern IT

Boosts managed IT security revenues by

50%

compared to previous levels

Delivers 24x7 threat management to new customers in

3-4

weeks, on average

Typically, these funds are focused on purchasing new tools and hardware to protect company assets from outside attacks. But with the increase of threats, the number of cybersecurity offerings have also increased, making choosing the right option a bit of a challenge.

“And the complexity of these solutions is becoming more and more overwhelming to the internal risk teams of these businesses,” Eng continues. “It’s ridiculously difficult to actually staff up your workforce with the right people and the right expertise to effectively choose and use these solutions. And if you do, you face the risk of some other company poaching them for a higher salary—there’s a major problem with retention.”

Employing sufficient personnel to provide 24x7 coverage was equally challenging for these businesses. And these staffing complications opened up a door for Silverfern.

“We saw an opportunity to create a security operations center [SOC] service,” explains Eng. “Within Silverfern, we already have all this expertise. And we wanted to better extend our knowledge and capabilities directly to our customers—to become an integrated part of their security team. We wanted to be able to say to them, ‘You let us look after you, and we’ll help you eliminate that concern over finding and managing the right security resources.’”

> “From a single pane of glass, we can see log sources from across their business—from firewalls to endpoints to applications and databases. If it’s in the network, we can see it.”

Liong Eng , Chief Executive Officer, IBM Business Partner Silverfern IT

Better technology. Better security.

To properly launch this new service, though, Silverfern needed to make some adjustments to how it monitored client environments.

“Traditionally, the types of services that we ran for our clients were pretty much very standard security monitoring—like endpoint detection or firewall managing,” clarifies Eng. “We had all these great tools, but they each had their own interface—their own portal. So we needed a central control panel where our engineers could look at all of the client’s environment and look at everything all at once.”

A long-standing IBM Business Partner, Silverfern quickly chose to deploy IBM Security® QRadar® technology to run its new SOC service. “In the marketplace, every security vendor claims their product is the best,” notes Eng. “Which is fair enough, but we looked at the Gartner Magic Quadrant, and there was IBM. Not only was QRadar the number one product, it had consistently been a leader for the past several years. That and our deep relationship with IBM over the last 20-plus years made the decision a no-brainer.”

Named the QRadar Managed Detection and Response service, the new SOC offering provides a unified, end-to-end service for a company’s cyberthreat needs. “We can typically get a client started within three to four weeks—we only have to bring in their log sources,” says Eng.

He continues: “And after that we watch their environment 24x7 for any indicator of a potential attack. From a single pane of glass, we can see log sources from across their business—from firewalls to endpoints to applications and databases. If it’s in the network, we can see it.”

The new SOC service relies on IBM Security® QRadar SIEM technology to oversee event management, using real-time analytics to sift through contextual threat data and shift to a more proactive monitoring posture. The SIEM solution’s IBM Security QRadar Advisor with Watson® functionality, in turn, harnesses the capabilities of AI to map offenses against a security incident database and better contextualize individual security incidents quickly and accurately.

And if a threat is detected, Silverfern uses IBM Security QRadar SOAR to manage the entire security incident lifecycle from detection through remediation. Much of this happens automatically as the business aligns its response efforts with predefined use cases—such as threat hunting or security-alert triaging.

Both of these QRadar offerings are delivered under an IBM Cloud Pak® for Security license. And in the not-too-distant future, Silverfern intends to further explore the capabilities delivered by the IBM Cloud Pak.

Cooperation as a competitive edge

“The IBM Security team engaged with us at the very beginning of the project,” recalls Eng. “They gave us the knowledge to move forward that we initially didn’t have internally. They were very patient and passionate about it—training my team and making sure we were well-educated. They really helped us with getting certified on the new technology.”

Alongside this knowledge transfer, the IBM products selected to flesh out the Silverfern SOC service helped the firm build a more competitive, responsive service for its client base.

“One of the great things about QRadar,” adds Eng, “is that it already has hundreds of use cases built-in that we can utilize. So when we bring a new SOC customer on board, we can immediately demonstrate to our client a return on their investment because we can show them everything that we are now managing. They don’t have to wait for us to build it.”

He continues: “With the IBM software, we have a great portal for our security teams to see what’s going on. It reduces the amount of training that we have to give our internal engineers, and that directly impacts our ability to manage more clients under this new platform. We also have more information that we can share with our clients. So we can give them a better understanding of what is actually happening in their network.”

To streamline the delivery of its QRadar Managed Detection and Response service, Silverfern took advantage of its position as an IBM Business Partner and signed an IBM Embedded Solution Agreement (ESA). “The ESA was truly a godsend for us,” notes Eng. “It lets us bundle the IBM technology directly with our service, so we can go to the market with a clear pricing model that we control. We can make the overall investment in our SOC quite attractive—all without extending timelines to resolve licensing issues.”

> “One of the great things about QRadar is that it already has hundreds of use cases built-in that we can utilize.”
>
> **Liong Eng**, Chief Executive Officer, IBM Business Partner Silverfern IT

A confident tomorrow

Silverfern is already realizing value from its work with IBM, as Eng notes: “When we compare our managed IT services from before with the managed SOC service using IBM, we’ve increased the revenue from that part of the business by 50%. And I expect in the next 12 months, we’ll probably increase it to double our pre-SOC revenue. There’s so much potential, and I’m very excited about the future.”

Much of this growth comes from the ability of the more comprehensive, centralized SOC service to attract new customers—particularly smaller-sized businesses that may not have the internal resources to dedicate to around-the-clock monitoring.

“Cyberthreats aren’t going away, and every company—big or small—is going to require some type of detection and response,” adds Eng. “They’re going to need insight into their operating environment and a clear understanding of what’s going on. They’re going to need to demonstrate compliance with industry and government standards. And that’s some of the value we can deliver. We can help reduce their risks. We can help them report to their boards and auditors. We can help keep their information safe.”

He continues: “That’s the most important thing to our customers, that we give them peace of mind about the safety of their network when they go home at the end of the day.”

About Silverfern IT

Boasting a rich, 30-year history, IBM Business Partner Silverfern (link resides outside of ibm.com) provides cybersecurity and consulting services and solutions. The business is headquartered in Perth, Western Australia, and specializes in disaster recovery, managed security services and security awareness training.

Solution components

- IBM Cloud Pak® for Security
- IBM Security® QRadar® SIEM
- IBM Security QRadar SOAR

Produced in the United States of America, November 2022.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.