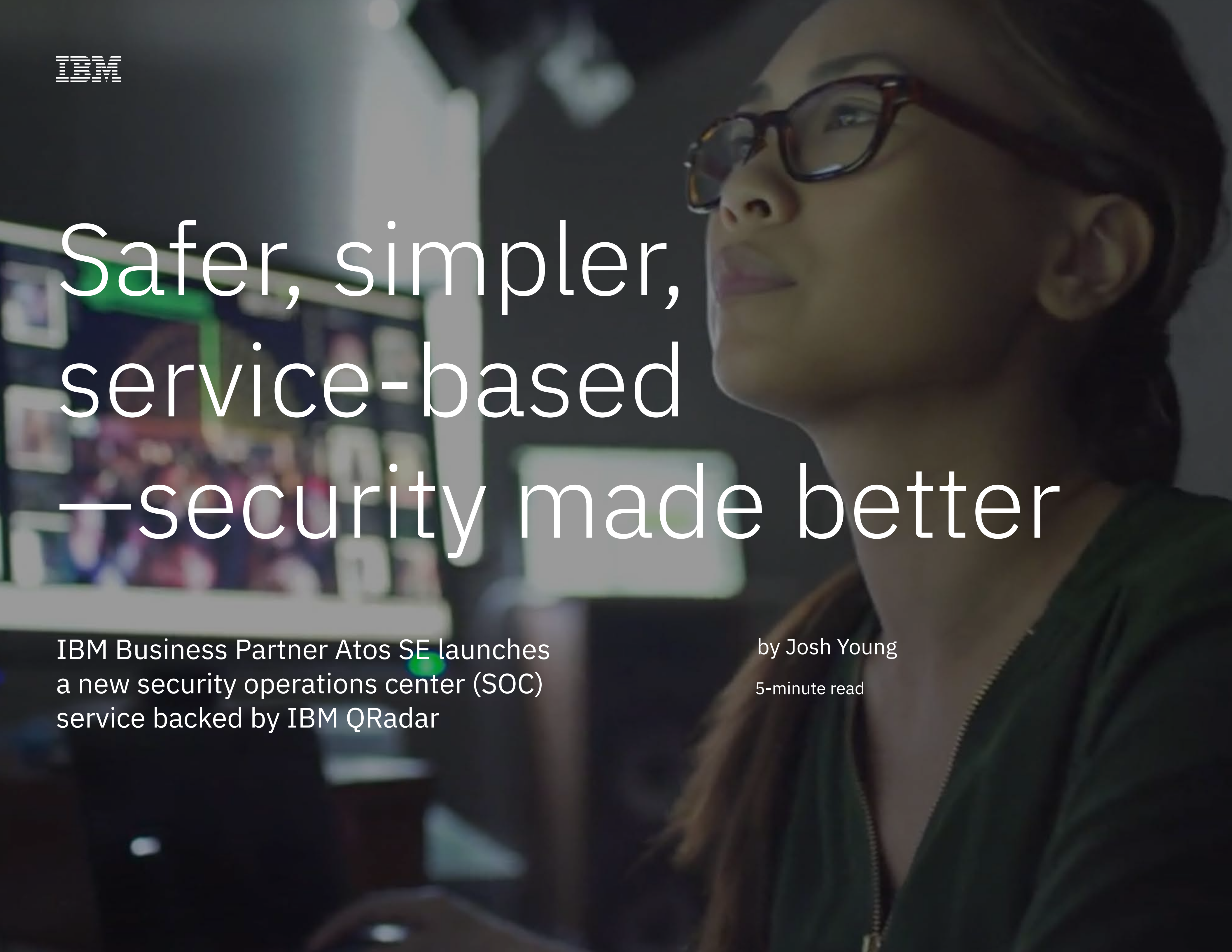

Safer, simpler, service-based —security made better

IBM Business Partner Atos SE launches a new security operations center (SOC) service backed by IBM QRadar

by Josh Young

5-minute read

Cybercriminals never take the day off, so your IT security needs to be ready to detect and fend off their attacks at any time. But for many businesses, staffing an around-the-clock security management team just isn't practical—or financially possible.

"Over the last two decades," explains Cheng Cai He, Head of Big Data and Security at Atos China, "I think we've all seen the increasing threats to security and data breaches. And the types of attacks—the types of viruses—have been evolving very rapidly in the Chinese region."

In response, many of Atos's customers had begun investing rather heavily in new security equipment and products. But frequently, these offerings weren't well integrated, limiting their ability to protect users.

"They weren't very efficient," adds Cheng Cai. "And businesses, starting with the manufacturing industry, began talking to us more and more about how we could really make sure that all of these products were working together. So we began exploring the idea of creating a cloud-based security operations center (SOC) service."

At this point SOCs had become more commonplace in the Chinese market. And through a SOC service, Atos could better centralize its customers' security data, offering a 360-degree view of overall network health and stability.

"Before, all of the SOCs we knew about had been built directly by the companies themselves," notes Cheng Cai. "And there weren't many of them because these SOCs are a big investment. You have to buy all types of security devices, and you have to invest in a dedicated support team if you're going to offer protection for seven days a week, 24 hours a day."

Delivers a SOC service at a price point of roughly

< 1.5 FTEs

while staffing an internal team would require 7 – 8 FTEs

Provides small- and mid-sized customers with

24x7

security monitoring and protection

In contrast, by choosing a service-based approach, Atos could extend the benefits of a SOC to smaller and mid-sized businesses that didn't have the available capital to invest in such a major IT project. And to make this service easy to deliver to multiple end-user environments, Atos also needed to rely on a cloud-based delivery model.

"The cloud industry has matured much in the past five years in China," adds Cheng Cai. "And many of our customers are moving their IT assets from on premises to the cloud. But this transition is a little complicated because we all need to comply with data protection laws that state critical information and customer personal data cannot be transferred out of the country. So the cloud solution for our new service needed to be hosted within China."

> "[W]e've all seen the increasing threats to security and data breaches. And the types of attacks—the types of viruses—have been evolving very rapidly in the Chinese region."
>
> **Cheng Cai He**, Head of Big Data and Security, IBM Business Partner Atos China

New technology. New delivery. New capabilities.

As Atos began considering how to deliver this planned SOC service, the business engaged in extensive marketing analysis, evaluating customer requirements and expectations for the offering. And at the same time, it began considering potential security products and tools that it could rely on to build the new SOC.

An IBM Business Partner, Atos quickly focused on IBM technology, particularly the IBM Security® QRadar® XDR suite. And after a successful proof of concept (POC) with the platform, the business chose the IBM Security QRadar SIEM solution to oversee the security information and event management (SIEM) needs of the new SOC service. Meanwhile, AWS provides the needed cloud environment in China.

The QRadar technology, in turn, offers Atos a holistic view of the customer networks that it monitors alongside AI-backed threat detection and log analysis. “It lets us see everything,” adds Cheng Cai. “We know what’s going on with our customers. We know what to prioritize and what isn’t a concern. It’s very useful.”

To streamline the deployment of QRadar for customers as they were onboarded, Atos signed an IBM® Embedded Solution Agreement (ESA). “We signed the ESA back in April,” recalls Cheng Cai. “It made the licensing easier as we built the QRadar product into our offering. And it better formalized our partnership with IBM—how closely we are working together.”

The new service was finalized in August 2022, initially working with three existing Atos customers for a pilot phase. And the following month, the Atos SOC service formally launched for the general public.

“We’ve also hosted two workshops at the IBM Innovation Center in Beijing,” notes Cheng Cai, “where we shared a demo of the SOC service. And from those discussions we are further building out our offering catalog.”

> “[QRadar] lets us see everything. We know what’s going on with our customers. We know what to prioritize and what isn’t a concern. It’s very useful.”

Cheng Cai He, Head of Big Data and Security, IBM Business Partner Atos China

Why IBM?

“We found that QRadar was the right choice for our SIEM,” explains Cheng Cai, “because it was already integrated with many of the policy and regulatory requirements imposed by the Chinese government that we needed to comply with. And it could be used Day 1 when we deploy the SOC platform for use with one of our customers.”

He continues: “Also, we’ve seen over the last decade that QRadar and IBM Security are constantly in the Gartner Magic Quadrant. And if we are going to offer a best-in-class service to our clients, then we need best-in-class security products.”

As an IBM Business Partner, Atos also valued the existing relationship that had been built with the global business over the preceding years. “Atos has been partners with IBM for a long time,” explains Cheng Cai. “But this is only the second project that we’ve teamed with IBM within China. We knew that if we were going to drive a new solution with outside support, the cooperation and trust of that other business would be an essential point to make the whole operation a success. And IBM provided that.”

Cheng Cai elaborates on the importance of this spirit of trust, noting: “We are an IT-service based company, and IBM China has a security service team. So in some opportunities, we are actually in a competitive position with IBM. But from the existing relationship with the global business and our direct experience from this project, we know we have a partner that we can fully rely on.”

Simple delivery, complex protection

With its new SOC service, Atos can offer comprehensive, robust security monitoring and management for small- and mid-sized Chinese businesses at a reasonable price point.

As Cheng Cai explains: "Our pricing puts the SOC service at around 1 – 1.5 full-time equivalents (FTEs). But for a business to build their own internal SOC, they would need to dedicate a team of 7 – 8 people. So this makes us competitive on just delivering 24x7 coverage without considering the capital expenditure they would need to gather for all of the security products."

"And threats and security technology are evolving very rapidly," he continues. "So they'd need to constantly be updating their policies and technology. But with the SOC, we do that for them. And we're doing that with a service that is the first of its kind in our market."

Assisted by built-in AI and automation, the QRadar platform helps to identify and resolve events more quickly. "Speed is everything when it comes to these attacks," notes Cheng Cai. "The sooner we can identify and quarantine abnormal behavior, the less potential damage that intrusion can cause."

About Atos SE

IBM Business Partner Atos (link resides outside of ibm.com) is a global provider of IT consultancy services, digital security solutions and decarbonization offerings. Headquartered in Paris, France, the business maintains offices and sites across 71 countries, employing more than 112,000 staff worldwide.

Solution components

- IBM® Embedded Solution Agreement
- IBM Security® QRadar® XDR
- IBM Security QRadar SIEM

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.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.