Protecting digital businesses from a world of cyberthreats

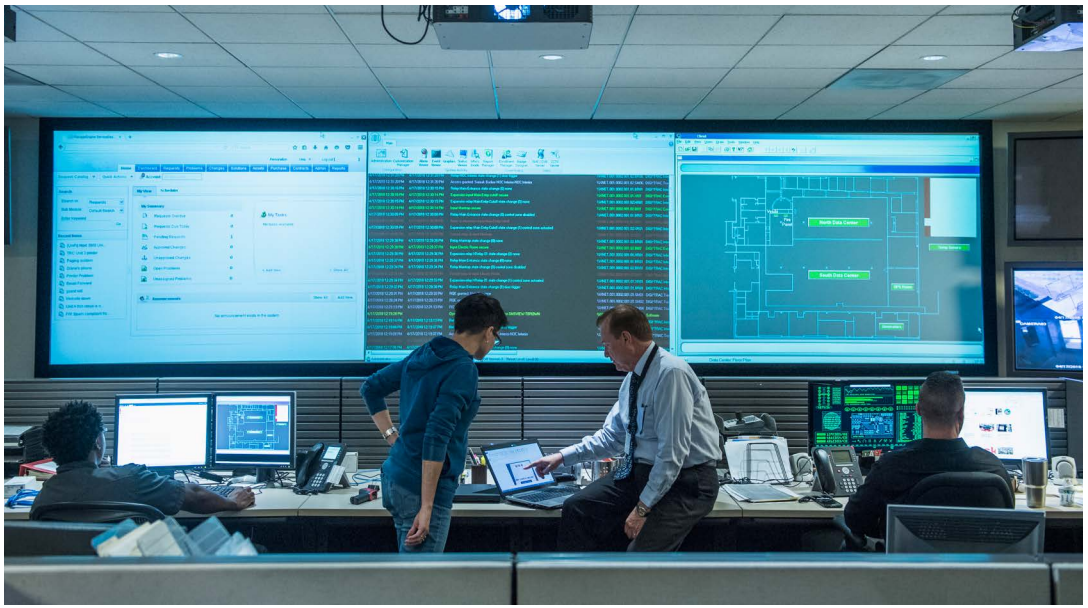
IBM Business Partner Netox uses the IBM Security QRadar SIEM solution and IBM Storage to power a SOC that delivers trusted security services

by Tom Farre

5-minute read

Netox Oy is one of Finland's great technology success stories. An IBM Business Partner delivering IT services and solutions with a specialty in cybersecurity, Netox grew 70% in 2021 and is poised to achieve 30% annual sales growth through 2026.

Such growth stems from strong demand for the company's cybersecurity services, along with able management and the right vendor partnerships.



"As customers' digital environments become more and more complex, they find it hard to understand all the different interactions and connections," says Marita Harju, Senior Manager, Cyber Security at Netox. "Our Netox Trust cybersecurity services provide visibility into their unknowns, and our playbooks help them respond when an attack happens. We enable business continuity so our customers can focus on their core business."

Netox Trust applies AI to integrate cyberthreat intelligence, data protection and preventive technologies into the customer's network and cloud infrastructure. With service levels tailored to each customer's size and digital maturity, Netox Trust relies on the IBM Security® QRadar® Security Information and Event Management (SIEM) platform, foundational technology that powers the security operations center (SOC).

The company didn't always use QRadar, however.

"Early on, Netox supported almost all the different security technologies our customers used," says Harju. "This approach gave inconsistent results and couldn't scale as our business grew." Netox's former SIEM solution also was subpar. Its main function was collecting and storing security log files, rather than helping analysts monitor, analyze and respond to critical threats.

Clearly, for Netox to grow and upgrade its service offerings, it needed to standardize on a leading security vendor.

Netox delivers multitenant cybersecurity services to

200

customers using the QRadar SIEM platform

QRadar's broad scalability means that

1

platform can serve any class and number of customers

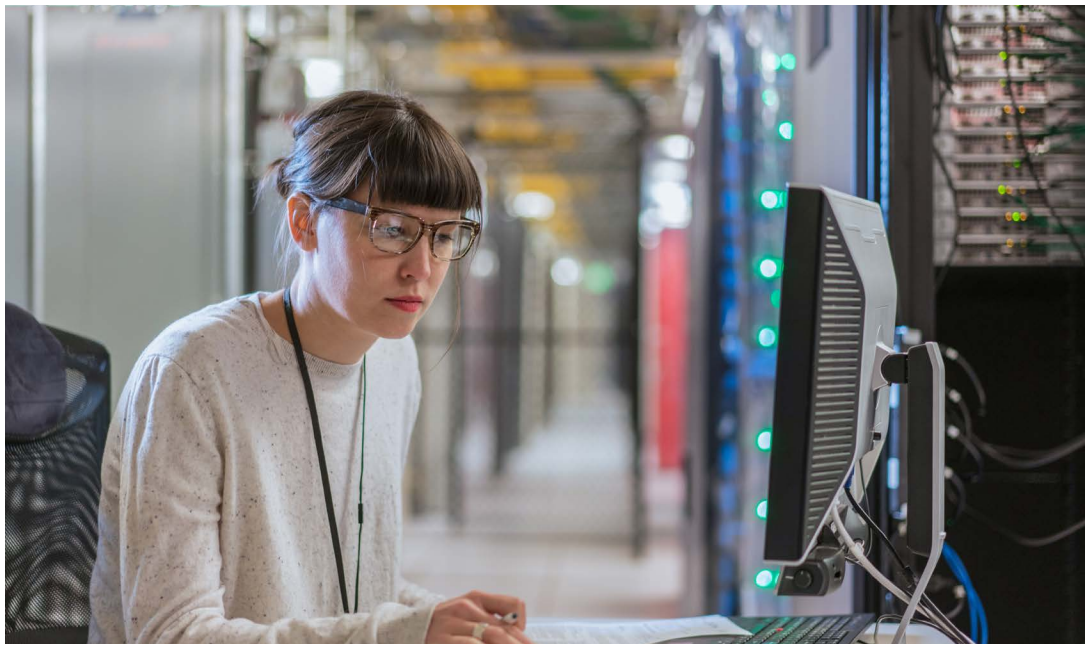
"We evaluated quite a few solutions, and QRadar was the only SIEM that could provide true multitenant services."

Marita Harju, Senior Manager, Cyber Security, IBM Business Partner Netox Oy

QRadar powers scalable, multitenant cybersecurity services

The Netox team began an evaluation to select a best-of-breed SIEM solution. Key requirements included the following:

- Multitenancy, so that one platform could serve multiple customers
- Scalability to support customers as they grew and as Netox extended its reach
- Support for data protection and compliance regulations
- A collaborative vendor relationship that would add value over time



These criteria led Netox to IBM QRadar. "We evaluated quite a few solutions, and QRadar was the only SIEM that could provide true multitenant services," says Harju. "We also liked QRadar's scalability. And it easily integrates with third-party security products and services, so we don't need to develop our own APIs."

Almost immediately, customers started to benefit from QRadar. It gave Netox engineers better visibility into customer operating environments, and with that visibility came the ability to react with speed. Says Harju, "With visibility, it's easier to quickly resolve any issues."

Netox deployed QRadar in its own data center, which was built using VersaStack converged infrastructure servers. Cisco and IBM had jointly developed VersaStack, which features IBM FlashSystem® storage.

In addition, Netox began storing customer backups on IBM Cloud® Object Storage, with storage management provided by IBM Storage Insights software.

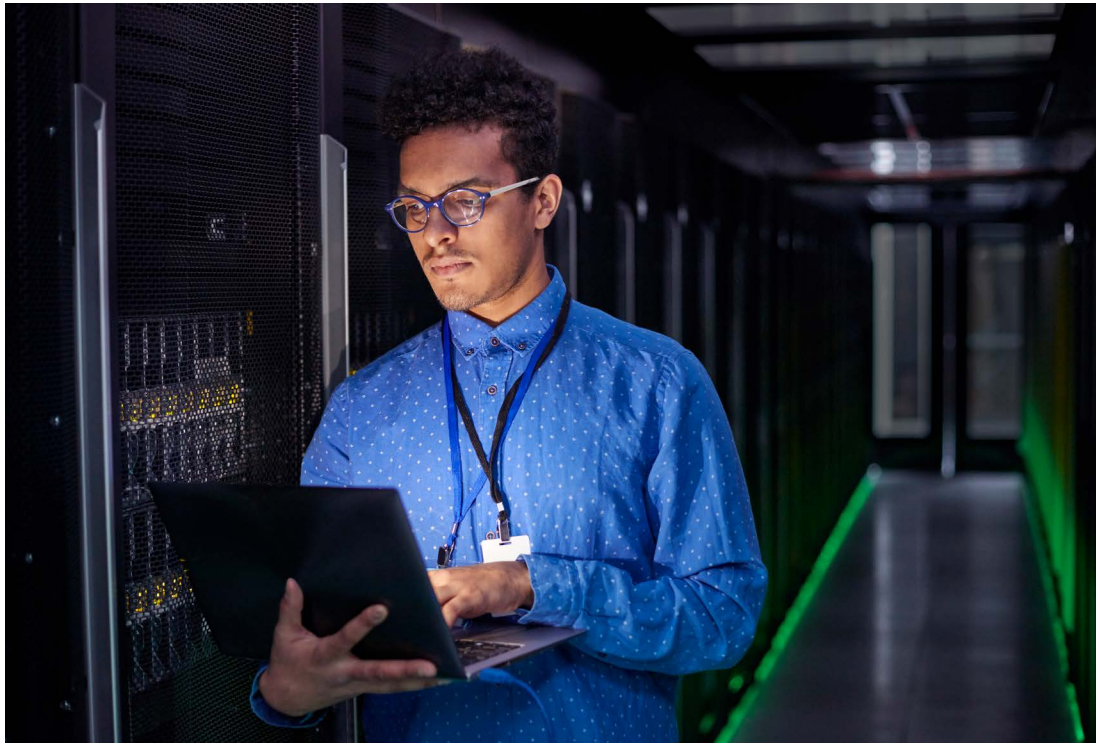
"We based our storage choices on IBM's long experience in the field and its strong product development," says Tommi Laurila, Lead Datacenter Architect at Netox. "The storage just works."

"Early on, Netox supported almost all the different security technologies our customers used. This approach gave inconsistent results and couldn't scale as our business grew."

Marita Harju, Senior Manager, Cyber Security, IBM Business Partner Netox Oy

Comprehensive visibility into customer environments

Today, Netox SOC analysts manage cybersecurity for around 200 customers. They use QRadar functions such as the customizable anomaly detection engine, network traffic monitoring, and AI-powered analytics to help identify and resolve threats their customers face.



Especially valuable are QRadar's Custom Rules Engine and User Behavior Analytics for automatic anomaly detection. Using Log Activity and Network Activity views, the analysts investigate threats by searching through related event data, and the

automated report function creates metrics and visualizations that provide comprehensive insights into both on-premises and cloud deployments.

"QRadar gives our analysts a single view into the threats across all our customer environments," says Harju. "And with its customizable dashboards, we get a quick view of system performance, unusual patterns and other anomalies."

Surprisingly, customers don't have to pay extra for such capabilities. "QRadar is known as the best-of-breed SIEM, but there's no premium—our service prices are well in line with the competition," says Harju. "Why not choose the best, instead of a low-end solution and having to upgrade later?"

> "QRadar is known as the best-of-breed SIEM, but there's no premium—our prices are well in line with the competition."
>
> **Marita Harju**, Senior Manager, Cyber Security,
> IBM Business Partner Netox Oy

Profiting from a collaborative vendor relationship

Netox receives considerable benefits from standardizing on IBM technology. QRadar's multitenancy and scalability lets SOC analysts support customers large and small from a single platform. And customers appreciate the speed with which analysts can detect and remediate threats—due to QRadar's ability to reduce the number of false positive alerts.

"QRadar makes it easier to focus on the most important threats, which lets our analysts identify and resolve threats in the shortest possible time," says Harju.

On the business side, QRadar's excellent reputation helps the Netox sales team, and the company also profits from IBM support. Specialists from IBM Finland help introduce customers to new services, such as advanced threat protection (ATP) from complex, slow-evolving threats. And IBM engineers are quick to respond to security and storage glitches. "The collaboration with the IBM team has been amazing," says Laurila. "When we need help, we know we're not alone."

Looking forward, Netox plans to expand its IBM relationship. The roadmap includes implementing IBM FlashSystem CyberVault snapshots for restoring customer data. But perhaps most importantly, IBM can help Netox achieve its heady growth projections.

Its strategy entails expanding internationally, opening new offices and acquiring larger customers—while exploring IBM solutions for security orchestration, automation and response (SOAR), identity management, and endpoint detection and response (EDR). Says Harju, "As we enhance our core platform with advanced IBM solutions, all customers will benefit."

About About Netox Oy

Founded in 2004, IBM Business Partner Netox (link resides outside of ibm.com) delivers all-inclusive IT solutions with a strong focus on cybersecurity. With offices in Oulu, Helsinki and Tampere, Finland, Netox combines international research, leading vendors, strong support and industry best practices to serve customers of all sizes and industries. Netox employs 120 people and in 2021 had revenues of EUR 15.7 million.

Solution components

- IBM Cloud® Object Storage
- IBM FlashSystem® Storage
- IBM Security® QRadar® SIEM
- IBM® Storage Insights