How Nexagate strengthened SOC delivery for a Malaysian government agency

Nexagate needed to deliver a complex government security project quickly, securely and without disruption. With Kaspersky SIEM and Kaspersky Next EDR Optimum, it created a SOC-as-a-service platform that improved customer delivery while supporting MSSP growth across Malaysia and Indonesia.

kaspersky cybersecurity true to business

NEXAGATE

Kuala Lumpur, Malaysia

2008
Year founded

Kaspersky MSSP
partner since 2022

+80
employees

About the company

Nexagate has been at the forefront of Malaysia's cybersecurity sector since 2008. Today, it's one of Asia's fastest-growing cybersecurity solutions providers. Headquartered in Kuala Lumpur, Nexagate specializes in public sector, enterprise and SMB customers, providing SOC-as-a-service, cybersecurity consulting, offensive security and awareness training.

The business is built on one guiding principle: helping organizations access enterprise-grade protection without having to build and staff their own SOC.

When a major Malaysian government agency needed to improve its cyber defenses, it turned to Nexagate's SOC-as-a-service.

The challenge: stronger cyber defenses, no operational disruption

The requirement was ambitious. Nexagate needed to deliver a robust, multi-tenant SIEM and EDR deployment on a tight deadline, while ensuring no disruption to the agency's operations. The project also had to support sensitive data requirements, fit Nexagate's existing SOC platform and avoid expensive hardware upgrades.

For the client, the priority was clear: enhanced protection without operational friction. For Nexagate, the project needed to prove that high-assurance SOC services could be delivered quickly, securely and at scale.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Next EDR Optimum

The approach: a managed security model built around customer continuity

To meet those requirements, Nexagate chose Kaspersky SIEM and Kaspersky Next EDR Optimum. The decision reflected both the technical demands of the government project and the practical needs of Nexagate's SOC-as-a-service model: multi-tenant security, smooth integration, fast rollout and efficient infrastructure requirements.

Nexagate needed more than a standard technology rollout. The project required close collaboration between its SOC engineers and Kaspersky's global technical team to ensure smooth integration and fast time-to-value.

Kaspersky's engineering team worked closely with Nexagate's analysts from the start, troubleshooting integrations, fine-tuning performance and developing custom parsers for specific requirements. The MSSP program also offered workshops with R&D, architecture consulting and around-the-clock technical support, all designed for service providers.

Strengthening SOC-as-a-service delivery

Kaspersky SIEM was integrated into Nexagate's SOC-as-a-service platform to help collect and correlate events from firewalls, endpoints and other security tools within the project timeline. The familiarity of the platform also supported rapid onboarding for Nexagate's analysts.

For the SOC team, this created a more connected view of security activity across the agency's environment. For the government customer, it supported better visibility and faster access to actionable security insight without the need to build its own SOC capability.

Kaspersky SIEM delivers:

Built-in multitenancy for MSSP-ready service delivery

A single SIEM installation in an organization's main infrastructure enables the creation of isolated SIEM instances.

Lean hardware requirements

Up to 50% lower spend on hardware or virtualization installation, reducing total cost of ownership through a high-performance modular solution that can handle up to hundreds of thousands of EPS per instance with fault tolerance.

Predictable licensing

Average daily EPS is tracked after filtering and aggregation, giving users flexibility during spikes without cutting access, slowing operations or risking gaps. The result is a smoother, more predictable experience even when event loads fluctuate.

Broad integration support

More than 300 out-of-the-box connectors, API functions for third-party systems and 800+ correlation rules maintained by Kaspersky SOC experts.

To complement the SIEM deployment, Nexagate also deployed Kaspersky Next EDR Optimum across the government agency's endpoints, extending managed detection and response from central event correlation to endpoint-level visibility, investigation and containment.

Kaspersky Next EDR Optimum adds:

- Behavioral and ML-driven threat detection
- Seamless integration with Kaspersky SIEM
- Built-in response features across endpoints from Kaspersky SIEM
- Use of existing Kaspersky EPP agents to collect Windows and Linux events
- Full attack chain visualization for faster investigation
- One-click automated response to contain incidents
- Centralized control for consistent policy enforcement

Together, the SIEM and EDR deployment helped Nexagate improve managed detection and response for the agency, combining central event correlation, endpoint visibility and practical response capabilities in a model designed for managed service delivery.

The outcome: faster deployment, stronger service delivery

With Kaspersky SIEM products and services successfully integrated into Nexagate's infrastructure and managed services processes, a growing list of organizations in the region are already benefiting from:

- Fast, disruption-free deployment, live in time to meet the agency's deadline
- Greater SOC efficiency, supported by centralized visibility, dashboards and correlation
- Stronger SLA levels
- Stronger service economics, with no expensive hardware upgrades
- Scalable architecture for additional customers

With the government project live, Nexagate is already extending its Kaspersky SIEM-based services to other clients. Its roadmap also includes adding Kaspersky Threat Intelligence and NDR/XDR to the MSSP portfolio.

Kaspersky Next EDR Optimum

Learn more

Kaspersky Unified Monitoring and Analysis Platform

Learn more

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#truetobusiness

Kaspersky Next EDR Optimum

Learn more

Kaspersky Unified Monitoring and Analysis Platform

Learn more

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#truetobusiness