



From reactive to resilient

How Quantico improved visibility, reduced manual effort and cut incident response times from hours to minutes



Digital and IT services
Central Italy

2019

year founded

1,000+

managed hosts

2,000+

total assets

Supporting digital transformation across Central Italy

Founded in 2019 from the merger of two companies with twenty years of experience, Quantico Srl is a digital and IT services company based in central Italy. With a team of 50 employees, Quantico operates across a hybrid IT environment that includes Windows, Linux and macOS endpoints, primary on-premises VMware infrastructure, cloud servers for proprietary applications, and vulnerability management.

The company collects log data from endpoints, firewalls, servers, connectivity systems and applications, with an average volume of around 1,500–2,000 events per second. Across more than 2,000 total assets and over 1,000 managed hosts, Quantico needed a more integrated way to monitor, manage and protect its infrastructure, and the necessary expertise to handle and respond to all types of threats.

The cost of fragmented security operations

The decision to invest was driven by the need to centralize security operations, reduce management complexity and gain a more complete view of the infrastructure. Rather than expanding its security stack with multiple point solutions, Quantico wanted a single platform that could simplify operations, improve visibility, extend response capabilities and at the same time reduce the burden on internal teams.

Automating control across a hybrid environment

Quantico chose Kaspersky MXDR Optimum for its ability to **combine extended detection capabilities** with expert-led managed protection in a single solution. Alongside smooth integration with existing tools, ease of use compared with competitors, the company valued the support for a mixed operating system environment, scalability and strong vendor support.

These requirements were especially important in a mixed environment spanning Windows, Linux, macOS, VMware and cloud infrastructure.

The **Kaspersky MXDR Optimum** implementation included endpoint monitoring, advanced detection and response features, security controls and patch management, as well as tools to help the team identify, prioritize and mitigate risks more effectively. These capabilities were complemented by continuous monitoring and response support from Kaspersky SOC experts.

k

Before adopting Kaspersky Next MXDR Optimum, Quantico relied on a more limited security setup that provided essential endpoint protection and managed protection but lacked the broader visibility and investigation capabilities needed to efficiently manage a growing hybrid environment. That's why the internal team relied on manual incident response processes, faced too many alerts without clear prioritization and spent significant time on routine operational tasks.



Kaspersky Next
MXDR Optimum

Kaspersky Next MXDR provides 24/7 monitoring and expert support from Kaspersky's globally renowned SOC team, while keeping essential XDR capabilities in-house.

Faster response, clearer control and less manual effort

With Kaspersky MXDR Optimum, Quantico moved from fragmented, manual processes and largely manual security operations to a more centralized and proactive security management model.

By combining broader XDR visibility with continuous monitoring and response support from Kaspersky SOC experts, the company has improved day-to-day workflows and reduced manual effort.



Scalable deployment across a mixed operating system environment



Centralized visibility across endpoints and infrastructure



System hardening, controls and patch management



Easy-to-manage interface with low ongoing maintenance requirements



Expert recommendations to support security operations

Automation capabilities, centralized control and patch management have further streamlined operations

The solution is intuitive to operate and maintain, requiring minimal effort after the initial setup while being easy to scale

For Quantico, this translated into significant time savings, increased operational efficiency and a lower workload for the team

The impact is also visible in incident response. Improved visibility across different endpoints, aggregated and prioritized alerts, and continuous support from Kaspersky SOC experts have enabled Quantico's teams to identify, investigate and respond to incidents more efficiently.

Additional outcomes

1

Activities that previously took hours can now be completed in minutes, allowing the team to focus only on higher-priority incidents.

2

Detection coverage has also improved, with increased endpoint coverage and better alignment with the MITRE ATT&CK framework.

3

Quantico can now detect activities that were previously difficult to identify, including lateral movement, suspicious use of PowerShell and unauthorized software execution.

Key takeaways



Visibility is the foundation for faster response

Quantico's results show how stronger endpoint visibility and centralized security operations can help teams understand what is happening across the environment, prioritize threats and act faster when incidents arise.



Automation reduces pressure on lean teams

By combining easy-to-handle extended detection and response features, automation, centralized management and expert support, Quantico reduced manual effort, improved workflows and lowered the day-to-day workload on the team.



Better patching strengthens security and efficiency

Improved patch management helped Quantico reduce operational risk while giving the team clearer control over routine security and IT operations.

Overall, Quantico has gained stronger visibility, capabilities for faster and accurate response, simpler security operations and reduced risk through improved patch and endpoint management.



Ugo Viti

Co-Founder and Board Member —
Quantico



Our experience with Kaspersky has been extremely positive, particularly in terms of reliability and comprehensive threat protection. The platform provides high visibility across the entire environment and significantly improves our ability to quickly detect and respond to security incidents. What's more, ease of management and centralized control helped to simplify operations and reduce the overall workload. Overall, Kaspersky has strengthened our safety posture while supporting our efficiency goals.