Maintaining operationality and embracing IT–OT convergence securely

at global OLED pioneer

kaspersky BRING ON THE FUTURE

Founded in
1993

20
subsidiaries worldwide, including the US, UK, Japan and Brazil

90,000+
patent applications submitted

About Customer

The client, founded in 1993 in the APAC region, is a leading IoT company providing intelligent interface products and professional services for information interaction and human health. It owns numerous large manufacturing sites and boasts subsidiaries in 20 countries and regions, including the US, UK, Japan and Brazil.

This enterprise is a true innovator and has to date submitted more than 90,000 patent applications. Notably, its OLED displays feature in one in four smart terminals worldwide.

Facts

- For over 30 years, the customer has been providing intelligent products and professional services for information interaction and human health.
- Its "1+4+N+Eco-chain" structure centers on semiconductor display and integrates IoT innovation, sensors, MLEDs and intelligent medical and industrial products.
- Today, every fourth smart terminal globally has a display from this client.

Cybersecurity partner

The customer has been using Kaspersky's IT–OT integrated cybersecurity solutions since 2017.

Challenge

As an Internet of Things (IoT) pioneer, the client relies heavily on its IT business application system for production, research and development, sales, and supply chain work. The bottom layer of this system comprises a virtualized environment. Internal work, on the other hand, is executed through an integrated cloud platform.

The client's existing defenses for its office terminals were ineffective against cyberattacks, and security incidents had become commonplace. This was hindering efficiency. The issue was that traditional virtualization platform security was deficient and could not guarantee uninterrupted protection of virtual machines (VMs).

The company's manufacturing environment – including industrial control systems (ICS) – was also at risk of attack. This was problematic because the business has a low tolerance for downtime. It was therefore crucial to protect not only the corporate infrastructure from attack but also production control hosts, programmable logic controllers and other industrial control devices.

Kaspersky Anti Targeted Attack

Endpoint Security

Kaspersky Hybrid Cloud Security

Kaspersky Industrial CyberSecurity

Kaspersky Security for Storage

Kaspersky solution

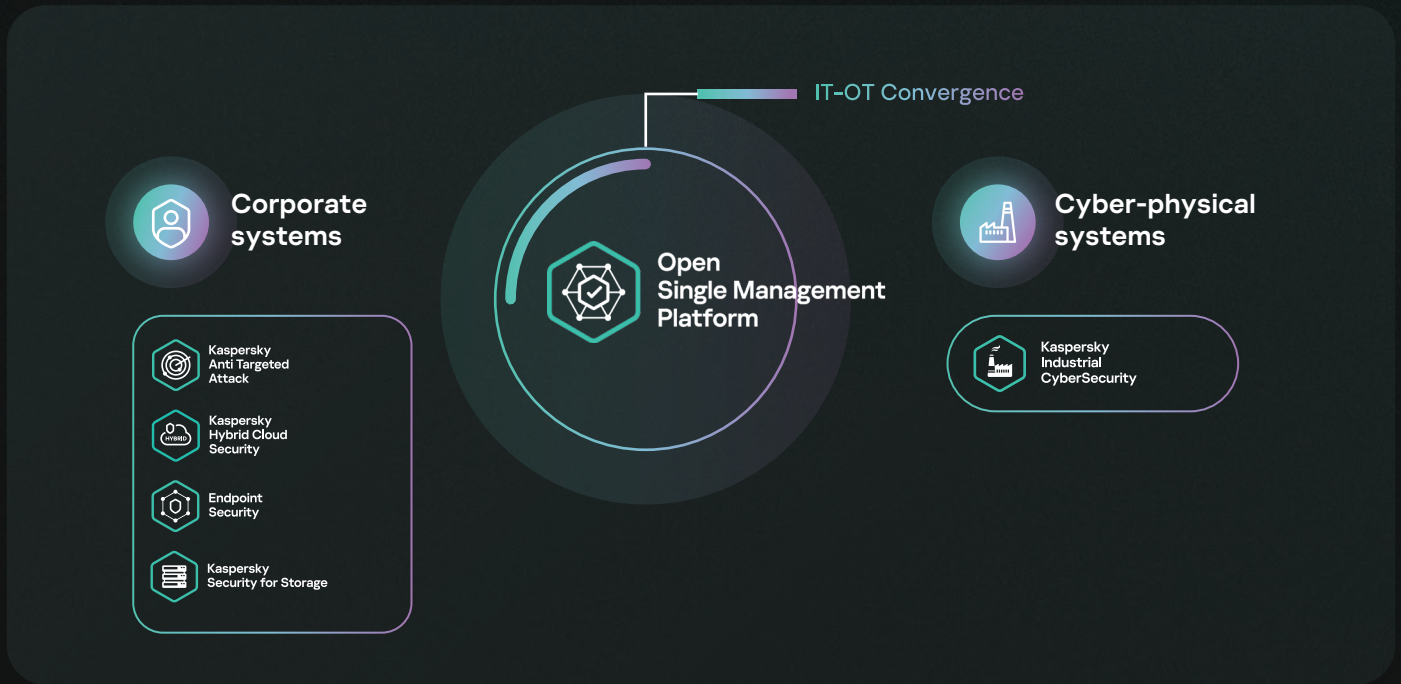
The client chose Kaspersky to protect its corporate and industrial infrastructure and facilitate safe IT–OT convergence. This would enable it to benefit from data-driven operations securely.

Kaspersky thrives at the corporate–industrial security intersection and was perfectly placed to implement sustainable protection through its IT–OT integrated solutions. This began with the deployment of **Kaspersky Endpoint Security for Business,** which delivered comprehensive security features and ensured the integrity of sensitive business information. **Kaspersky Security for Storage** was implemented to protect critical and sensitive data in network-attached storage devices and file servers, making it unencryptable by ransomware – perhaps today's greatest threat.

Kaspersky Hybrid Cloud Security was installed to protect the organization from unknown threats and maximize host performance, while **Desktop Virtualization Security** mitigated the risks posed by antivirus storms (poor system performance when VMs have simultaneous scans).

Kaspersky Industrial CyberSecurity protected the client's industrial control system from common malware and cyberattacks while mitigating human factor risks. The solution is designed for industrial environments and is certified in compatibility by automation vendors, meaning it was light on resources, compatible with legacy systems and could be deployed with limited operational impact.

To stop the most advanced attacks, the client purchased the **Kaspersky Anti Targeted Attack Platform.** This solution combines endpoint sensors with sandboxing technology and integrated global threat intelligence, which ensured the client was a step ahead of the hackers eyeing its IT infrastructure.



From Client Spokesperson

We have deployed Kaspersky Industrial CyberSecurity in many factories of our group. With its excellent compatibility and stability, it has achieved stable operation under various industrial control brands and equipment environments, and has the ability to quickly analyze and warn of threats on industrial networks to realize the transparency of industrial network threats, which has guaranteed the continuous and stable operation of production lines.

Outcomes

Kaspersky's integrated security solution solved the problem of virus propagation at the client's network storage level and provided nonstop protection for the virtualization platform. Not only did it guarantee performance but it also improved protection at the IT–OT intersection, reducing the impact of human factors and attacks on the corporate environment while guaranteeing the stable operation of the business system. It protected the firm's critical infrastructure in both production and office environments at all times while providing centralized management to improve IT–OT visibility.

The bottom line was reduced spending on operations and maintenance and a strong return on investment.

Kaspersky Industrial CyberSecurity

Learn more

www.kaspersky.com

@kaspersky
#bringonthefuture