Are your clients safe from the endpoint vulnerabilities lurking in their systems?

The evolving threat landscape puts businesses of every size at risk. But with the correct knowledge and toolset, your MSP business can capitalize.

What are endpoint vulnerabilities?

Endpoint vulnerabilities are what we talk about when discussing weaknesses or defects in the devices connected to a network. Every connected device is an endpoint and a potential entry point for infection. In addition to operating systems, every application on an endpoint – think Slack, Zoom and Outlook – can be vulnerable, meaning a business with even 50 machines can host myriad vulnerabilities.

Bad actors can exploit these unpatched vulnerabilities to penetrate an organization's network, leveraging one or more endpoints to harm IT infrastructure at large.

Endpoint vulnerability risks

The modern work environment is so distributed that entry points to a business's network can exist on every continent simultaneously. Bring your own device (BYOD) policies and online collaboration tools are the norm, and even small businesses are operating in a distributed manner. This increases the risk of endpoint vulnerabilities which, if poorly managed, can be exploited in malware attacks and zero-day exploits.

Such attacks can have severe **financial** and **reputational implications**. For example, a successful exploitation of an endpoint vulnerability may result in:

- **Compromised data** – endpoints often contain valuable data, such as customers' personally identifiable information (PII)
- **Company downtime** – bad actors can leverage vulnerabilities to deploy ransomware and conduct denial-of-service attacks, shutting down operations
- **Regulatory noncompliance** – the compromise of data will likely put an organization in violation of regulations and incur sanctions
- **Network vulnerability** – attackers can gain a foothold in a company's network by exploiting an endpoint and moving laterally, sowing the seeds for a long-term campaign

Remediation is expensive and customer trust can be permanently eroded, which can render a business financially unviable. There is thus **a broad market opportunity** to secure your clients from endpoint vulnerabilities – you just need to demonstrate the value of prevention.

> The WannaCry attack that downed the UK's National Health Service (NHS) in 2017 relied on a Windows vulnerability exploitation called EternalBlue. It cost the NHS around £92 million.[1]

Countering endpoint vulnerabilities to secure your clients

Endpoint vulnerabilities have threatened organizational security for decades. So much so, in fact, that in 1999 MITRE launched a dedicated repository, the CVE Program, which now contains hundreds of thousands of entries. The sheer volume of vulnerabilities means no business is secure without dedicated **endpoint protection**. By delivering this to your clients, you will unlock a fruitful and continuous revenue stream.

Clients to approach

Modern businesses require endpoint protection, whether they have 10 machines or 10 thousand.

> "How can we stay on top of patching and ensure that our devices are always protected?"

The solution: Kaspersky Endpoint Security for Business

You can protect your clients from dangerous vulnerabilities with the dedicated protection in **Kaspersky Endpoint Security for Business**, which has everything required to secure Windows desktops, Mac OS and iOS devices, and Android mobiles. Much of the protection is easily automated too, such as vulnerability patching, minimizing the legwork involved. What's more, our expertise in this area led SoftwareReviews to name us a **Leader** in its 2023 **Endpoint Protection Data Quadrant**[2] – so you can rest assured when deploying this solution!

To learn more about managing your clients' risk with Kaspersky solutions, email us at msp@kaspersky.com or click below.

Find out more

1. Kaspersky. (2024). What Is WannaCry Ransomware? Kaspersky.
2. SoftwareReviews. (2023). 2023 Data Quadrant Awards – Endpoint Protection. SoftwareReviews.

kaspersky