Would your clients survive a ransomware attack?

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

What is ransomware?

Ransomware is a prevalent form of malware that modifies data on a victim's computer so that the victim can no longer use the data or fully run the computer. Once the data has been blocked or encrypted – essentially taken hostage – the user receives a ransom demand telling them to send money. The bad actor promises to send a program to restore the data and/or computer's performance on receipt of the cash. However, payment does not always guarantee a positive outcome.

Today, there are entire cybergangs dedicated to the **ransomware-as-a-service** (RaaS) business model, which enables them to sell packages to lesser-skilled affiliates who do their bidding at scale, with profits being shared. A RaaS subscription may include around-the-clock support, dedicated forums and other perks one would expect from a legitimate software-as-a-service business.

Ransomware risks

Ransomware attacks can harm businesses of every size and industry. In recent years, ransomware operators have upped the ante by threatening to share or auction stolen corporate data, thus making victim businesses liable to their shareholders and customers. This is known as **double extortion**. It has severe **regulatory implications** – just consider the General Data Protection Regulation (GDPR) – and, in turn, **financial implications**. Customers whose data has been affected may also seek damages from the victim.

The morality of paying ransoms is a source of debate, as the money undoubtedly funds more criminal activity. Ransomware is therefore accompanied by the risk of **reputational harm** on two fronts: if an organization pays and this becomes public knowledge, it may be perceived as weak or morally bankrupt; if an organization doesn't pay and the result is a data breach, customer trust will be eroded. Implementing anti-ransomware defenses is therefore crucial for all businesses – and for you, this is a **market opportunity**.

> The number of targeted ransomware groups rose 30% globally between 2022 and 2023[1]

Countering ransomware to secure your clients

Ransomware will plague businesses as long as victims continue to submit and pay. And in that sense, it isn't going anywhere. Cybersecurity protection is the answer – but not all solutions are made equal. For a solution to be effective, it has to use a multi-layered protection model and detect ransomware at both the delivery stage and the execution stage of the attack. If you can deliver this to your clients satisfactorily, they will be safe, and you will have a continuous revenue stream.

Clients to approach

Business of every size and industry require ransomware protection – even charities have been attacked. But while ransomware operators historically targeted large enterprises owing to their obvious wealth, they are increasingly targeting smaller businesses with double extortion tactics, knowing that such businesses may have no choice but to pay in order to survive. The Federal Office for Information Security (or BSI) in Germany, for example, identified ransomware as the nation's main cybersecurity threat in 2023,[2] noting the shift from "big game hunting" to the targeting of smaller companies and municipal administrations.

> "If hackers stole our customer data and held our business hostage, I'm unsure we would be able to recover. How can we protect ourselves?"

The solution: Kaspersky ransomware protection

You can mitigate your clients' vulnerability to ransomware by delivering them the elite ransomware protection within **Kaspersky Endpoint Security for Business**. This deep protection has been proven **100% efficient against ransomwar**e by AV-TEST during dedicated testing ,[3] so you and your clients can rely on it to get the job done.

> "Our Advanced Threat Protection tests are designed to assess the true ability of EPP solutions to counter full-scale ransomware attacks, using the latest techniques employed by threat actors. It is a challenge for many EPP products to perform successfully in the tests, so it is outstanding to see the 100% protection rates that Kaspersky delivers."
>
> **– Maik Morgenstern, ex-CEO, AV-TEST[4]**

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, May). The State of Ransomware in 2024. Securelist.
2. German Federal Office for Information Security. (2023, November). The Situation of IT Security in Germany 2023. German Federal Office for Information Security.
3. AV-TEST. (2021). Advanced Endpoint Protection: Ransomware Protection test. AV-TEST.
4. Kaspersky. (2023, April). AV-TEST Confirms 100 Percent Effectiveness of Three Kaspersky Products Against Ransomware. Kaspersky.

kaspersky