

POINT OF VIEW

Real-world Peer Insights on Ransomware

Ransomware Recurrence and Risk-reduction Perspectives



Organizations of All Sizes, Industries, and Locations Speak on Ransomware

Fortinet recently commissioned a [global survey](#) of organizations of all sizes on their experiences related to ransomware. While the report covers a wide range of related issues, there are three findings that stand out as worthy of deeper discussion.

- Two-thirds of respondents reported having been the target of a ransomware attack, with nearly half being targeted multiple times.
- Secure web gateway technology was the most cited (48%) security technology organizations planned to invest in.
- Nearly all respondents (81%) viewed integrated products as extremely or very important to their ransomware strategy.

Here's why we believe more discussion in each area is warranted.

1. 46% of organizations have been a target of ransomware multiple times.

It is important to point out that almost half of survey respondents reported having been successfully targeted multiple times by ransomware campaigns. And more than half (52%) indicated that they contracted with an incident response firm to help with their response. While we know from the FortiGuard Labs Global [Threat Landscape Report](#) that the overall volume of ransomware increased tenfold from mid-2020 to mid-2021, discovering this high rate of recurrence at the same organization was unexpected. It is something we see periodically, often when the initial investigation and remediation never found patient zero. But we had not realized that being serially targeted by different ransomware attacks was so common.

One key takeaway is that whether you pay a ransom or restore your systems from backup, it is essential to have the teams and technologies in place to identify the initial point of entry as well as the full scope of the incident to reduce the risk of recurring ransomware incidents. Of course, this can be difficult, as today's campaigns are often multi-stage, multi-component, multi-outcome efforts.

Been Target of Ransomware Attack

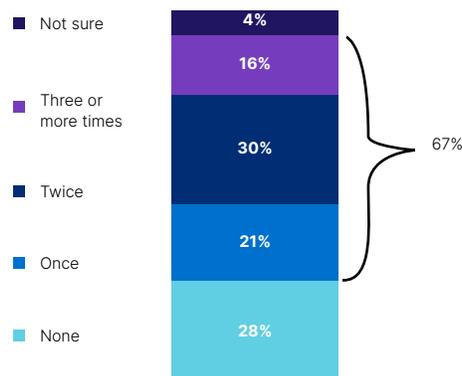
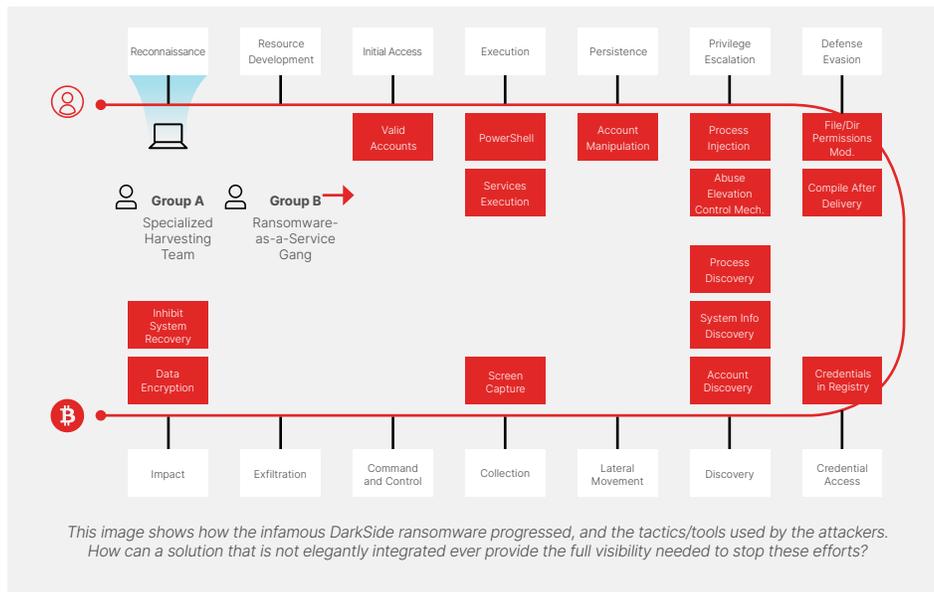


Figure 1: Responses to "How many times have you been a target of a ransomware attack?"

MITRE ATT&CK®—DarkSide Ransomware



2. Secure web gateways are cited as essential technology

One of the most common attack vectors for ransomware is via the web. While the ability to identify and block connections, communications, and downloads to malicious sites is essential, the technologies used for these tasks are increasingly available as part of a modern next-generation firewall (NGFW) (cloud-delivered or on-premises). A secure web gateway plays a vital role in protecting your remote workers and offices. But traditional networks (campuses, data centers, branch offices) require an NGFW solution. What an NGFW adds—that is not found in a secure web gateway—is more broadly applicable coverage (beyond port 80 and port 443) and additional protections to address top access methods identified by respondents—open ports (49%), Remote Desktop Protocol exploits (49%), and unpatched vulnerabilities (40%).

And while speaking of methods of entry, phishing is reported as the most common method of entry. So, it was surprising to see how few organizations selected secure email gateway products as essential to stopping ransomware. Email is still the most common attack vector for ransomware. And while the end-user training that nearly all respondents reported investing in is vital, organizations will significantly reduce their exposure with strong technology designed to filter out as many email-borne threats as possible. Frankly, the native controls from email infrastructure vendors are not enough if you truly want to reduce your email security risk.

Essential To Secure Against Ransomware

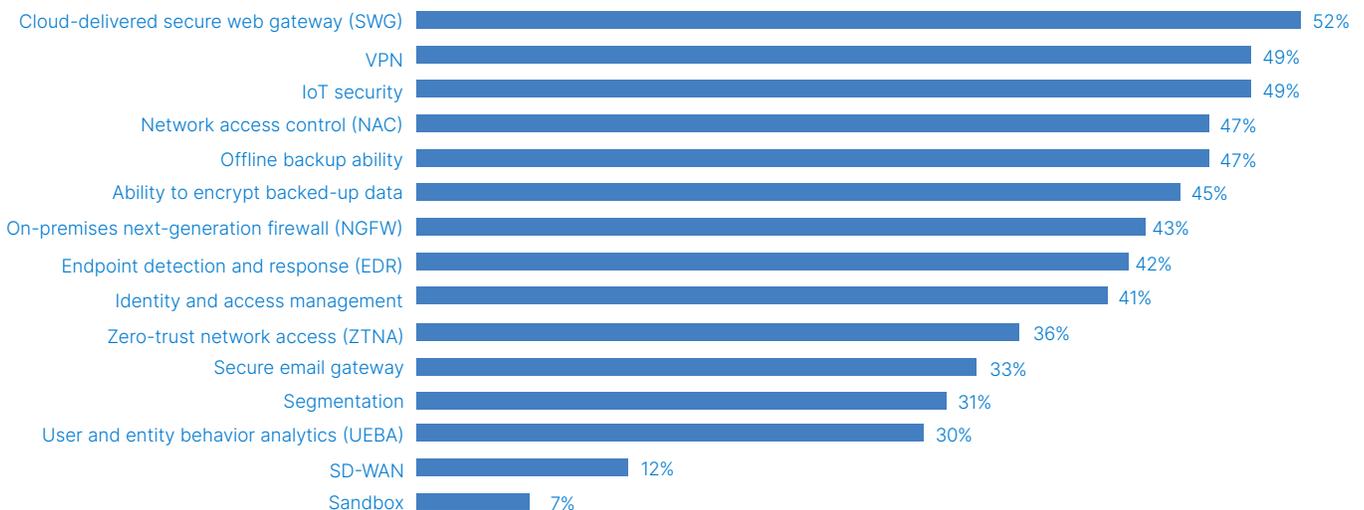


Figure 2: Responses to “What products/solutions do you believe are essential to secure against ransomware?”



3. An integrated approach to stopping ransomware is required

While there is a wide range of security technologies available to reduce the risk and impact of ransomware, including some of the critical components discussed above, it was interesting that most (81%) respondents view integrated components that work together as extremely or very important. Regardless of their features, individual point products will never provide the level of prevention, detection, and response that a fully integrated system can provide. So, in addition to evaluating the effectiveness of email, web, and endpoint controls individually, it is essential to look at how they can work together to provide stronger, faster, and more manageable protection from ransomware.

Important Aspects of Cybersecurity Solutions

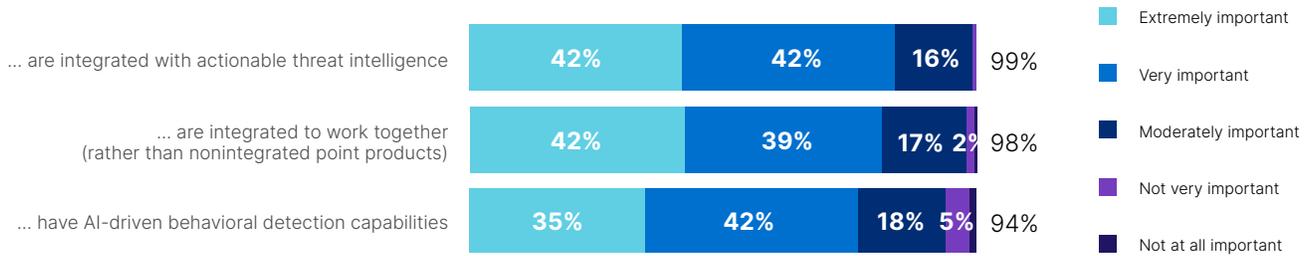


Figure 3: How important is it that a ransomware strategy consists of cybersecurity solutions that ...?