EINPRESSWIRE

CRA Survey: Endpoint Security Goal – Save Users from Themselves

The most common endpoint strategy among respondents is based on the belief that employees can't be trusted to safeguard their own credentials and access.

NEW YORK, NY, UNITED STATES, September 14, 2023 /EINPresswire.com/ -- On the surface, endpoint security might resemble a game of Whac-A-Mole: For every couple of loose devices that get patched on time, another vulnerability rears its head demanding immediate attention. But an August 2023 Cybersecurity Buyer Intelligence survey of 200 security and IT leaders and executives, practitioners, administrators, and compliance professionals tells a more nuanced story.

On the one hand, respondents prioritize securing what they see as a defining feature common to most endpoints: email access and communication. At least 3 in 4 use a secure email gateway server to monitor and manage all emails being sent and received from devices connected to the corporate network, which in theory should reduce the likelihood of email compromise from malware and phishing attacks. On the other hand, the most common endpoint security methods are those that operate off the notion that employees can't be trusted to safeguard their own credentials and access. Multifactor authentication and strong password enforcement top the list, requiring users to submit extra proof that they are who they say they are to weed out imposters.

"As we move toward more and more data being stored in cloud platforms, it becomes increasingly important to restrict access by unmanaged (BYOD) devices," said one respondent. "Remote work is certainly a challenge. Even though I would say we've trained the employees properly, there's always a little risk there since you don't always know what employees are doing while working in their remote locations."

Key takeaways from the report:

• Three out of five respondents admitted to one or more compromised endpoints in the last year. That's a lot of compromise, considering 63% reported having 1,000 or more endpoints on their network. Desktops, mobile devices (like laptops and tablets), and servers were the most common targets of these attacks.

• Not all endpoints are observed equally. Just 59% of respondents are confident that at least 75%

of their endpoints receive monitoring around the clock. That means a huge proportion of devices are essentially being left...to their own devices – either operating off the grid or receiving only periodic attention.

• Endpoint security prioritizes securing end users from their own behaviors. MFA, strong password enforcement, and security awareness training are the most common tactics used for endpoint security. Many respondents employ an EDR or EPP tool in their endpoint security strategy, but more than a third plan to incorporate an AI or machine learning-based approach to their strategy in 2024.

• ... And yet, employee negligence and user carelessness is still considered the top challenge to securing endpoints. Half of all respondents are concerned that users will fall prey to schemes – like phishing emails or social engineering attacks – that give bad guys a foothold into the network. As one respondent said, all it takes is "one rogue click to compromise the entire organization."

For more detailed findings and analysis, download the full report.

About CyberRisk Alliance
CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and LaunchTech Communications. Click here to learn more.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
press@cyberriskalliance.com

This press release can be viewed online at: https://www.einpresswire.com/article/655635212