ActZero

THREAT INSIGHT

Holistic Attacks

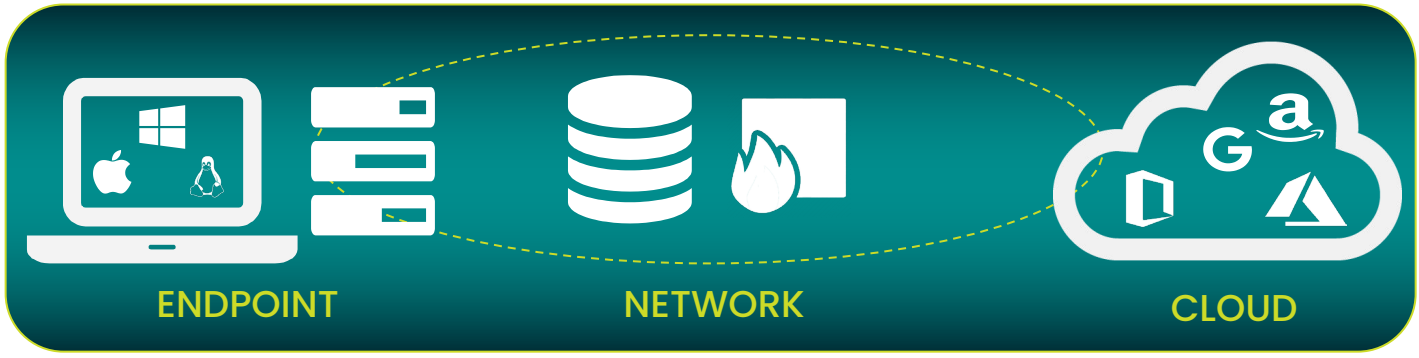
Why threats that jump around can leave you in a house of pain

As the amount of data stored in systems has increased, so has the frequency and sophistication of cyber attacks. The days of simply relying on a firewall and antivirus software to protect a business' network and data are over. The technology landscape has shifted dramatically in the past decade. and businesses are being impacted by attacks that not only shut down and compromise devices, but affect the network and cloud as well.

Catch me, if you can

Threat adversaries search for "open doors and windows" on your network that can be exploited, then execute attacks against them. With **holistic attacks**, the attack can originate anywhere a vulnerability exists whether that be the cloud, a server, a workstation endpoint, or a mobile device. From there, the attack can spread like wildfire, jumping across vulnerabilities and platforms until many endpoints and cloud systems are compromised.

Take for example ransomware attacks, which come in three extortion tactics. One that locks files and demands money, one that demands money over threat of releasing details, and one that expands the problem to your business partners and clients. When an employee unknowingly clicks on a phishing email, the ransomware jumps into the endpoint. From there, it jumps across the network into the cloud, maybe even your Salesforce environment. Once in the cloud, they start grabbing and bundling data, then exfiltrate it. Often,m you simply focuse on getting files unlocked on the device. They lurk within the unprotected gaps



How do you prepare against holistic attacks?

Gather Cross-Platform Insight

There are many point source solutions in the market, and even some that are multimode (meaning they'll gather information from multiple sources). These can all be purchased and managed by and organization, or by a managed services provider. The challenge in doing so is that while they can gather telemetry from different points, that telemetry is often filtered, and the tools fail to make the connections between data, or see the patterns across the platforms that will provide a holistic view of the threat. You need a solution that can do just that. Better yet, find a solution that uses artificial intelligence (AI) and machine learning (ML) to intelligently pinpoint threats that have evaded defenses by correlating the indicators of attack directly with threat intelligence, proactively blocking malicious activity.

Employ Holistic Threat Hunting

Now that you've detected some anomalous behaviour or potential threats, you need well-guided threat hunters that can handle the investigations. The threat hunting team needs to filter through alerts, and advise you where to take actions. But, without good AI and ML modelling that can filter out false positives using user behavioural analysis and time-proven models, they'll waste efforts investigating needless alerts.

Get SOC Support

And what happens with the alerts once they do get to you? You also need a well-equipped SOC to deal with it. A SOC can't be efficient if its trying to manage disconnected alerts from point source or multimode solutions. It's like playing a game of whack-a-mole in a 4D game.

Combat sophisticated attacks with ActZero's holistic MDR approach

ActZero's ai-enabled Managed Detection and Response (MDR) solution looks at the entirety of attacks across your endpoints, network and cloud. We collect raw, unfiltered data from endpoints, network, and cloud, and bring them into our data lake. We process this data using our highly-trained and constantly-tuned ML models to detect incidents that might have evaded other prevention measures. This helps us unravel an entire attack, and develop models to more quickly and more precisely detect these threats, wherever they may appear.

To learn more about how ActZero MDR's capabilities can safeguard your organization against holistic attacks, contact us now.

Email: info@actzero.ai
Phone: +1.855.917.4981