ActZero

USE CASE

Protecting Remote Employees with ActZero MDR

As companies of all sizes adjust to the new normal, you need to consider the implications of evolving workplace environments on cybersecurity coverage. Some businesses have shuttered offices entirely, shifting to a fully remote workforce. Others are pursuing a hybrid solution of in-office and working from home (WFH), leveraging office space on demand, or even leaving it to managers' discretion as to how their teams will proceed.

The disparity of approaches, and haste with which they were implemented, has caused challenges for IT teams. Organizations that were well prepared may find their solutions less effective (Security Information and Event Management (SIEM)), less manageable (antivirus (AV)), or even completely inapplicable (Firewall, unless paired with VPN).

WFH Challenges to Consider

Control Over Connected Devices: From the consumer-grade router to the IoT devices connected to it, IT has limited control over vulnerable nodes connected to corporate-owned endpoints while employees operate on home networks.

Monitoring/Privacy Liabilities: Monitoring of employees must change when they are outside your office. You need to balance their privacy with your efforts to mitigate risks of security incidents, and regulatory fines / compliance considerations.

Threat Alerting: Sometimes, the tools a remote employee would need to alert your helpdesk of an infection are the very ones that have been compromised.

Ineffectual Technology

Certain solutions were designed for the office and IT-controlled network environments. With employees working elsewhere, these tools may not work:

Antivirus: Your signature-based detection technologies need to be up to date to be effective. Without the capability to remotely deploy updates to employee endpoints, your AV will not be able to detect the latest threats.

Firewall: When configured and managed correctly, Firewalls filter, intercept, and prevent bad traffic from entering your net-work. With employees working outside of your network, your firewalls won't help unless all your employees leverage a VPN to route traffic behind them.

Web Gateway: Similar to the firewall, your web gateway remains unused when your employees web traffic is routed through their own network/ISP.

SIEM: A SIEM requires information to analyze, so it can use rules to determine whether something malicious has occurred. In the absence of key log sources (eg, Access Points), SIEMs lack the visibility to be effective.

So, how do you overcome these challenges and ensure that your distributed work from home environment doesn't compromise your business?

ActZero MDR helps you uncover, mitigate and manage the threats that you can't see with your existing tools. It protects your employees, endpoints, and network across your fully remote or hybrid remote/ in-office solution, demonstrably reducing your cybersecurity risk.

How We Do It

Endpoint Detection & Response: Our EDR Sensors are deployed to all your endpoints, and are visible and operational from anywhere they are connected to the internet. This enables us to contain and disrupt threats, in real time, on your behalf.

Log Analysis: We collect logs from your existing prevention technology (AV, Firewall), end-points, network, and cloud (o365) to address potential indicators of compromise (IOCs) before they become breaches.

Endpoint Hygiene: We analyze your servers and laptops to understand where (on which specific endpoints) your posture is weak, so you can remedy it.

Vulnerability Scanning: We report a prioritized list of vulnerabilities and patching recommendations to you every month

Threat Hunting: Our experts look for many and various Indicators of compromise (IOCs) across an array of Threat Hunts. One such hunt seeks out malicious outbound connections to a malicious IP address from the endpoint, enabling us to detect exfiltration of data and disrupt it.

Virtual CISO: This optional add-on gives you access to expert CISOs to advise on your privacy / compliance issues, or help with security policy, planning, and awareness initiatives.

CONTACT US

ActZero

These are just some of our advanced capabilities. To learn more about how ActZero's Managed Detection and Response Service protects your corporate assets, and your remote workforce, contact us today.

www.actzero.com • 1 855 917 4981