WILINE ENDPOINT SECURITY

Mobile Endpoint Security is Vital for Your Organization's Security Profile

Mobile devices are among the most useful tools for organizations. They allow workers to quickly respond to meetings, get critical work done in their off time and efficiently communicate with their clients, managers and peers. It's not a stretch to say companies are depending more and more on mobile devices to enhance productivity. This is backed by the fact that mobile devices are now the majority of corporate endpoints. This, combined with the fact that many employees now work remotely or in a hybrid capacity using their own devices, has presented a set of serious security threats for many organizations. As the number of mobile devices has grown, so too have the endpoints that organizations must watch over to protect their sensitive data.

MOBILE ENDPOINT SECURITY EXPLAINED

Mobile endpoints are any mobile device that connects to your organization's network. As mobile devices have become more common in the workplace, especially due to remote and hybrid conditions, nefarious actors have been targeting them as an easy way to access company data or upload malware. The frequency of attacks on mobile devices have been rising as well. Verizon's 2022 Mobile Security Index found that nearly half of the companies they surveyed had been compromised through a mobile device in the past 12 months.

To keep mobile devices secure, organizations must have technologies and procedures in place to keep watch over their mobile endpoints. Strong endpoint security can be achieved through the implementation of zero trust policies, thorough employee training on phishing and app usage, as well as continuous security checks. On top of carrying out those practices, it's recommended for any organization to make use of a robust endpoint protection platform (EPP) to keep watch for any breaches. EPPs constantly monitor your endpoints as well as your organization's files, processes and systems for malicious activity, helping to mitigate the damage that a compromised endpoint can cause.

A strong EPP can take much of the risk out of having your users connect to your network with their own devices. Features an EPP can have include:

Phishing protection which blocks connection to URLs, IPs and domains that are deemed to be suspicious.
Mobile threat detection which gives you visibility into the threats that your network is facing and maps where the attack is happening to help your team quickly fix the issue.
Behavior monitoring that tracks unusual activity from users in your network and quickly flags out-of-the-ordinary events for potential malicious activity.

With the promised rise in mobile devices in the workplace, sticking to strong cybersecurity practices backed by an effective EPP can go a long way in ensuring your network is protected from compromised endpoints.

MOBILE ENDPOINTS ARE IN DANGER AND CREATE RISKS FOR YOUR ORGANIZATION

Threat actors have plenty of fantastic reasons to target mobile devices. Chief among them is that the mediums in which malicious entities can get an employee to interact with their malware or other viruses are far greater than on a traditional laptop. Downloadable apps, push buttons, SMS and traditional vectors of infection like emails and dodgy websites all pose separate threats that companies must watch for. There are a wide variety of distribution methods to mobile devices, each of which can easily catch an employee off guard. The fact that many employees look at their devices after hours when they are more easily distracted, or use them for personal use, also heightens their chances of making a mistake and accidentally uploading malicious software onto their device.

The dangers of mobile devices becoming compromised is high. In CrowdStrike's 2019 Mobile Landscape Threat Report, the company highlighted some of the programs that can be installed on a mobile endpoint. These include:

Remote Access Tools: Also known as RATs, these tools allow malicious actors to monitor and collect data from the device, recording everything from active screens, camera and sound monitoring and collection of messaging data all the way to keylogging. RATs can be used to quietly exfiltrate corporate data without the end-user knowing that anything is happening at all.

Mobile ransomware: Just as computers and networks are vulnerable to ransomware, so too are your mobile endpoints. This follows the traditional pattern of ransomware where access to the device is locked until money has been paid in return for a code.

Perhaps the scariest of the cyber threats that a hacked mobile device can bring for any organization is the fact that compromised mobile devices can be used to access their internal network and either exfiltrate important data, or deliver malware directly into their network. With mobile endpoints being such a risk for any organization, it's paramount that security measures and policies are put into place to mitigate risks.

HOW WILINE HELPS TO PROTECT MOBILE ENDPOINTS

To help protect our customers' mobile endpoints, WiLine has partnered with CrowdStrike to deliver best-in-class endpoint protection. As a leader in the Gartner Magic Quadrant for endpoint security, CrowdStrike's groundbreaking mobile EPP platform is a turnkey solution which detects and helps to remediate threats to your mobile endpoints. This lightweight technology works for both Android and iOS devices and provides advanced threat intelligence and full telemetry on network activity, user activity and operating system events. To learn the benefits of CrowdStrike's EPP, try our 15-day free trial today.

WiLine's managed cybersecurity service can help your organization realize a stronger security posture. For more information on our approach to cybersecurity, click here.

About WiLine

WiLine Networks is a disruptive vendor in both the long-haul and last-mile connectivity markets. WiLine's carrier-grade, software-defined mesh network provides extraordinary reliability and flexibility when compared to legacy network providers. WiLine also offers a full suite of managed services to fast forward growth and boost the productivity of your organization.

Protect your organisation's Enpoint Security with WiLine.

Call **1-888-494-5463** today.

www.wiline.com