Malwarebytes

EXECUTIVE SUMMARY

3 Simple Steps to a Secure Remote Workplace

Devices are 12x more vulnerable when outside your office

Executives are 6x more likely to be targeted by cybercriminals

3,600+ malicious coronavirus-themed domains were created in 4 days

Malwarebytes Chief Information Officer Greg Higham recently sat down for a 30-minute webinar on securing a remote workforce. The insights drew from his own experience moving from the hypothetical to reality, as the COVID-19 pandemic forced the immediate execution of Malwarebytes' already-created remote workforce plan—a plan that looked good on paper but had yet to be tested in a real-world environment. Here are highlights of his three-step process for securing a remote workplace.

1 STEP ONE

Increase your device security in uncontrolled environments. This includes immediately patching everything, even if costs you downtime. Your VPN vulnerabilities and other exploits are being targeted and need to be immediately secured. You must also discover and secure all personal devices employees are using for work. Finally, you'll need to ensure remote workers are always protected from threats—even when not connected.

2 STEP TWO

Effectively operationalize security for remote work. This ranges from executing at least a daily scan schedule for verifiable security (and hopefully more), to establishing a prioritization scheme for high-value individuals (executives) and departments (such as finance) to ensure they have increased security, monitoring, and remediation. Ultimately, this also entails ensuring operations can be automated across groups of machines or batched across your entire device pool.

3 STEP THREE

Recover quickly from attacks that have been triggered. It's critical to act quickly to isolate and recover from a compromised endpoint before it begins to sprawl. This includes ensuring remote remediation is thorough and effective. You'll also need to leverage expert incident responders to recover remote endpoints after a successful cyberattack.

Although not an official "step", Greg emphasized the importance of human connection. The pandemic created fear and uncertainty among employees, and this led to the company increasing the frequency (while decreasing the length) of voluntary all-hands meetings. Further, Greg initiated brief (15 minutes) daily video chats across his department to ensure they felt "connected" and engaged.

Throughout the discussion Greg explained how **Malwarebytes Endpoint Detection and Response** and other Malwarebytes solutions provide the technology to keep your workers protected—whether they're working remotely or on-premises. The meetings gave people a chance to listen, ask questions, and gain understanding. **Greg concluded by summarizing key tips on protecting your remote workforce and ended with perhaps the best advice of all, "Remember to wash your hands."**

Securing your remote worker

Increase device security specifically for an uncontrolled environment

Effectively operationalize security for remote work

Optimize remote device recovery

Most of all, don't forget the human connection!

WATCH WEBINAR

Watch the 20 min Webinar recording addressing today's realities, and strategies organizations can deploy to secure remote workers.

https://bit.ly/3dYil6u

Greg Higham is Chief Information Officer & Executive Vice President at Malwarebytes. He has a long history of helping teams create a technology vision, global operations management, and scalable business growth.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.