Malwarebytes

eBOOK

5 steps to secure your remote workforce: a practical guide

The urgent need to secure remote workers

Even before COVID-19, IT and security professionals knew that working remotely was becoming more popular, giving companies access to the best talent and enabling these valued workers to either stay in the places they call home or have the freedom to be digital nomads. According to a 2018 study, 70 percent of global employees were already working remotely at least once per week.[1] However, with the pandemic compelling people to work from home (WFH), IT leaders are now dealing with a ballooning remote workforce and all the security issues posed by their diverse work conditions.

The need to keep remote teams productive and protected has never been more urgent.

1. CNBC. 70 percent of people globally work remotely at least once a week, study says. May 2018.

As companies shift to enabling employees to work safely from any device, any network, anywhere, “the perimeter” is rapidly becoming an outdated term. This means you must reassess how to best protect your endpoints and your teams’ personal devices so that people can work safely and efficiently. What can you do? Here are the five crucial steps you must take to set your teams up for security success.

1. **Understand the challenges.**
2. **Regain control of your security posture.**
3. **Operationalize security for remote work.**
4. **Accelerate the recovery of compromised remote devices.**
5. **Engage employees on the importance of cybersecurity.**

Ready to get down to business?

1

Understand the challenges

The first step is understanding the main challenges of this new reality. Let’s dive in.

Understand the challenges

1

Challenge 1: Zero Trust is great—but not everyone has the resources.

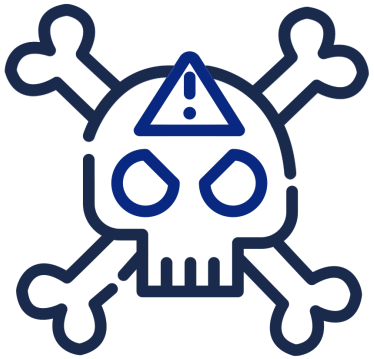
We're big proponents of the Zero Trust approach. With Zero Trust, everything and everyone is considered suspect until you can be sure they're safe.

It's an ideal security approach, particularly for executives—but it can get complicated and time-consuming when dealing with more users and different kinds of devices. To be realistic, not everyone may have the resources for Zero Trust.

Challenge 2: Cybercrime is a growing threat.

According to the 2020 State of Malware Report, business threat detections surged from 8.5 million in 2018 to 9.6 million in 2019, an increase of 13 percent. Hacking, evasion, and stealth techniques also advanced in 2019, becoming more sophisticated and diverse.[2]

In addition, cybercriminals are working overtime to feed on our present concerns. Thousands of scam and malware COVID-19 sites are being created daily, promising vital information and instead delivering malware.[3] And with remote workers using their own home networks, it becomes harder to track the threats targeting businesses, making businesses even more vulnerable.



According to one security researcher, more than 3,600 new malicious domains containing the term "coronavirus" were created between March 14–18 alone.[3]

2. Malwarebytes. 2020 State of Malware Report. February 2020.
3. ZDNet. Thousands of COVID-19 scam and malware sites are being created on a daily basis. March 2020.

Challenge 3: Users aren't vigilant about their cyberhygiene.

Cyberhygiene has always been an issue. For example, 46 percent of staff members admit to moving files between work and personal computers while working from home. A further 13 percent admit to sending work emails via personal email addresses because they can't connect to an office network.[4] This behavior can't be expected to improve as more devices move beyond the eyes of security professionals.

So how do you overcome these challenges? While no one has all the answers, experience provides a well-lit path. Our next three steps come from the deep experience of our own CIO, Greg Higham, and are in fact the very steps he took in securing Malwarebytes' remote teams when California's governor issued its "shelter in place" order.

4. Indusface. How to maintain security with remote workers? June 2017.

Regain control of your security posture

In an expansive WFH environment, we are no longer building a fence to protect networks within a specific domain but instead aiming to protect free-range devices across the world. Therefore, you need to immediately increase device security across the board. Here is our CIO's advice and how he did it.

2

Regain control of your security posture

2

Action 1: Bolster your infrastructure by eliminating your patch backlog.

You need to make sure that you've installed the latest security patches on everything. When you wait to install updates, you're leaving a door open for cybercriminals. VPN exploits are a hot target for the bad guys and VPN usage just went through the roof, yet this infrastructure is often not patched due to its 24x7 availability requirements. Simply put, it's better to take an availability hit than be breached.

> ***Our CIO did it by...*taking our critical servers offline to make sure we were patched as soon as possible, removing known threat paths.**

Action 2: Discover all the devices that employees are using for work, including personal and offline devices.

Your users' mobile and home devices are being added to your company network, so securing those devices is imperative. But first, you need to discover them by using a reliable discovery tool.

> ***Our CIO did it by...*running the Malwarebytes Endpoint Discovery tool, which enables you to easily see what's attached to your network.**

Regain control of your security posture

2

Action 3: Ensure that all devices have the right role-level security applied.

Now that you gained visibility into the devices on your network, you need to make sure they have the proper level of security for their role. You may want to use a personal security portal that manages security deployment and licenses for personal devices.

> ***Our CIO did it by...*implementing the network access control policy that uses Malwarebytes agentless remediation to bring a device into compliance before it allows VPN access. He also leveraged the Malwarebytes Personal Security Portal.**

What's the Malwarebytes Personal Security Portal?
It installs Malwarebytes personal protection and remediation on personal devices, enabling you to manage deployment and licenses without needing to manage these devices' security policies.

3

Operationalize security for remote work

Everyone has gone remote—including your IT ops and security teams. That means efficiency and process have never been more important. Here are our CIO's tips on how to effectively operationalize security in these times.

Operationalize security for remote work

3

Action 1: Implement a security routine.

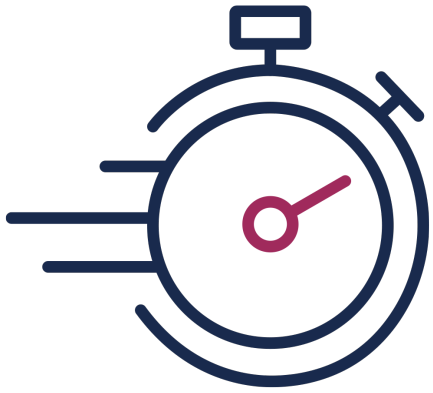
The longer devices are out of the office, the less secure they become, so have your team schedule automated scans at least once a day. It's best to use an efficient cloud-based solution, as this minimizes risk while maintaining performance.

> ***Our CIO did it by...*implementing a cloud remediation scan schedule. All devices are scanned daily, while those belonging to key departments and individuals are scanned two or more times a day.**

Action 2: Enable a quick response by building a security prioritization scheme.

If you're attacked, you need to be able to both assess the situation and respond—on the double. With a tool like Malwarebytes Nebula, our cloud-hosted security platform that maximizes limited resources and simplifies endpoint protection, you can use predefined group security levels to rapidly assess the severity of the attack and immediately respond.

> ***Our CIO did it by...*prioritizing security levels based on roles, which included defining group security policies based on their access rights and risk profile.**



82 percent of cloud users have experienced security events due to confusion over Shared Responsibility Security Models.[5]

5. IDG Connect in association with Malwarebytes. Lattes, lunch, and VPNs: securing remote workers the right way. 2019.

Action 3: Use automation to assist your overworked security team.

Given the current strain on security teams, now is certainly the time to take advantage of automation. By ensuring that operations can be automated across groups of machines or batched across the entire device pool, you not only minimize the risk of manual errors, you also help your team handle their increased workload.

> *Our CIO did it by...*not needing to do much! Malwarebytes integration with leading IT systems management tools allows for the automation of routine tasks.

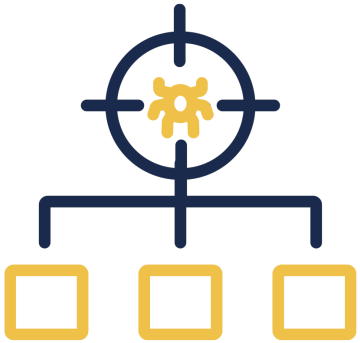
Accelerate the recovery of compromised remote devices

When an attack hits, don't treat remote devices any differently than you'd treat the ones that reside inside your firewall. It's all about rapid isolation and effective remediation.

4

Accelerate the recovery of compromised remote devices

4



Action 1: Isolate impacted groups before sprawl occurs—then ensure proper remote remediation.

You need to quickly isolate infected endpoints, as otherwise an infection can sprawl out of control. With rapid and effective isolation, you give your security team the time they need for proper remediation.

> *Our CIO did it by...*using Malwarebytes Endpoint Detection and Response. With this solution, his team can evaluate the attack vector and isolate those impacted within seconds. The team also ensures that remote remediation flags even innocuous-seeming potentially unwanted programs that later trigger with other malware.

Accelerate the recovery of compromised remote devices

4

Action 2: Plan ahead for widespread malware incidents such as Emotet.

Every company should make sure they can leverage expert responders when they need them. Otherwise, you may not get access to the experts you need during an incident such as Emotet.

> ***Our CIO did it by...*identifying a team of expert incident responders who can efficiently recover remote endpoints after a successful cyberattack.**

In 2019, TrickBot and Emotet surfaced in the top five threats for nearly every region of the globe, and in top threat detections for the services, retail, and education industries.[6]

6. Malwarebytes. 2020 State of Malware Report. February 2020.

5

Engage employees on the importance of cybersecurity

Thought you were done? Nope. You may lead the way down the cybersecurity path, but whether or not your remote workers follow you is crucial. That's why we included this final step. You need to help your workers understand the cyberthreats they face and how they can protect themselves. Here are some key things you can provide guidance on:

- Password management/system access
- Physical security
- Separating work and personal devices
- The importance of secure connections, including precautions about unsecured WiFi
- Cybersecurity best practices, including advice to be wary of phishing emails
- Avoiding Zoombombing

Check out our WFH security blog post for more specific tips.

Your 5-step plan to secure remote workers

Remote workers need assurances for protection and performance—right now.
Ready to get started? Here's your checklist.

- ☐ **1. Understand the main challenges of this new reality.**
  - ☐ Recognize that not everyone has the resources for Zero Trust.
  - ☐ Know that cybercrime is a growing threat.
  - ☐ Be aware that users aren't vigilant about their cyberhygiene.
- ☐ **2. Regain control of your security posture.**
  - ☐ Bolster your infrastructure by eliminating your patch backlog.
  - ☐ Discover all the devices that employees are using for work, including personal and offline devices.
  - ☐ Ensure that all devices have the right role-level security applied.

- ☐ **3. Operationalize security for remote work.**
  - ☐ Implement a security routine.
  - ☐ Enable a quick response by building a security prioritization scheme.
  - ☐ Use automation to assist your overworked security team.
- ☐ **4. Accelerate the recovery of compromised remote devices.**
  - ☐ Isolate impacted groups before sprawl occurs—then ensure proper remote remediation.
  - ☐ Plan ahead for widespread malware incidents such as Emotet.
- ☐ **5. Engage employees on the importance of cybersecurity.**
  - ☐ Provide guidance that helps your workforce understand the cyberthreats they face and how they can protect themselves.

Take the next step toward a secure workforce

See for yourself how Malwarebytes helps protect endpoints and personal devices. To start your free trial today, visit: malwarebytes.com/business/