




**TOP
FIVE**

Top 5 Must-Haves to Ensure Remote Worker Security

The global shift from working securely in an office to working at home has increased the number of devices, physical sites, and network traffic and opened enterprises to unprecedented levels of cyber risk – some of which is created unknowingly by remote workers as they strive to maintain productivity from home.

Percentage of Increase in Cyber Threats/Alerts	GLOBAL	APJC	AMERICA	EUROPE
0% – 24%	31%	25%	31%	47%
25% – 50%	33%	35%	36%	23%
51% – 75%	23%	27%	24%	11%
76% – 100%	5%	6%	3%	2%
Don't know	8%	6%	5%	17%

 25% or more threats
% of Increase in Cyber Threats or Alerts

SOURCE: <https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html>

Already stretched thin trying to support the sudden shift to remote work – and the thousands of devices workers are using to access the network – IT teams are asking themselves:

- Can we verify user identity remotely?
- How do we allow secure access to company applications?
- Can we safeguard our network against probable danger?
- Can we strengthen our posture within budget?
- Can we do it all uniformly with as few vendors as possible?

The risks include:

- A lack of internal policies and procedures that allow remote access to company data
- Use of unauthorized SaaS-based applications
- Bypassing the VPN to obtain corporate access
- Low – or no – awareness of public Wi-Fi perils

While securing a corporate network can be formidable, the following 5 Must-Haves will provide CIOs/CTOs with peace of mind by safeguarding remote work.





Must-Have 1: Multi-Factor Authentication (MFA)

MFA technology verifies users' identities before giving them admission to a company-approved application. It also improves IT's visibility into all devices trying to gain access to the corporate network. When considering MFA, pay attention to not only security, but also ease-of-use, including self-enrollment on demand; uncomplicated, layered security; options based on user need; and shadow IT minimization.

Must-Have 2: Robust VPN

To ensure workers have secure remote access to your network on any device from any location, a VPN must move beyond traditional capabilities to give IT departments visibility and control over the "who" and "what" of remote access. This includes built-in web security and proactive malware protection; sustained data encryption; and burst capacity support.

Must-Have 3: Cloud-Based Security

Safely accessing corporate data and applications via a secure VPN connection is only half the security battle. With so many SaaS applications in use from outside the safe confines of the

corporate network, it's important to protect remote workers' devices from passing along an infection. Cloud-based security can help IT departments protect against DNS changer malware, monitor DNS requests, and prevent threats dynamically.

Must-Have 4: Cloud-Based Analytics

Malware evolves rapidly and IT departments scramble to keep up. How do you protect your enterprise from a new and powerful infection that enters, invades, and paralyzes your network from a secure remote device? By taking advantage of cloud-based analytics to proactively and continuously search for, detect, deter, and defeat the most advanced threats — before they wreak havoc.

Must-Have 5: Help from an Expert

Providing remote worker security is complicated, particularly when it comes to juggling new software. An experienced vendor — one that specializes in core capabilities — can help your IT department provide this high level of protection via one interface and products that work together to fortify security posture.

Looking Ahead

As vaccines become more widely available, CIOs/CTOs must begin to define what business resiliency means to their enterprises. The goal is to move beyond business continuity and create a strategy that helps your business take full advantage of opportunities created by a new, more dynamic work environment.

Next step - Hybrid work returning to the workplace

Business leaders are already recognizing that worker productivity is sustainable, if not improved, in a fully remote or hybrid work environment. In the not-too-distant future, office space will be

available on an as-needed basis. Employees will demand greater flexibility and businesses will begin shedding footprint and reducing operating costs dramatically.

Final Step - Redesigning the workplace

Post-COVID-19, an enterprise's reimaged workplace secures, connects, and enables the distributed workforce with anytime, anywhere access through any device. IT departments will be at the forefront of optimizing each worker's experience for performance, cost, and security.

Why Choose Black Box?

Our dedicated team of Edge Networking solution architects and deployment engineers have deep technical expertise combined with a consultative approach to craft the right solution for every client, every time. As your trusted partner, we can help you design, deploy, and manage an optimized network for secure remote work and a return to a transformative workplace.

