Securing Remote Work:
Protecting Your Endpoints the Right Way

Brave New World

The abrupt shift towards supporting remote work, creates a series of security challenges to many organizations. All of a sudden companies are now operating across workers' various endpoints from corporate laptops to personal and mobile devices, on Wi-Fi networks and public clouds at a greater scale. We've gone from environments where most were confined in our office building, to a brave new world with workers needing access to corporate resources from all sorts of devices, on networks we don't control. How do we know if our laptops have malware, or if the Wi-Fi we're using at the coffee shop is a backdoor waiting to be exploited? This is our new reality and so, the question to IT and Security teams then becomes, "How can you empower employees to do their best work securely, regardless of where they are and what devices they are using?"

Endpoint Security Is a MUST
In Securing Your Remote Workforce

With 70% of breaches originating on endpoints, there is no question that endpoints are a top target of attacks. In light of the recent pandemic, bad actors seize the moment by stepping up pandemic-themed malware and phishing campaigns. Malware like LokiBot, FormBook and NanoCore targeting endpoints including devices being used for remote work are on the rise. Fraudulent websites flourish such as the fake John Hopkins Infection Map infected by Azorult malware. While organizations involved in pandemic related work are especially targeted by attackers who are preying on remote users who may have let their guards down clicking more readily on pandemic related links or attachments unknowingly opening up the backdoor for malware to wreak havoc.

The proliferation of these threats along with the flood of new and unrestricted devices now accessing company data remotely and increased use of cloud-based collaboration platforms or unsanctioned SaaS apps place additional pressure on IT and endpoint security teams to keep remote workers productive and secure.

Verify, Access and Defend

Here are three ways to enable remote work productivity without compromising security.

1 First, you need to **VERIFY** the identity of your users before granting access to corporate applications. One way to do this is using multi-factor authentication (MFA). MFA secures your applications by using a second source of validating your users' identity, like a phone or a token.

2 Second, you want to provide secure **ACCESS**, while empowering employees to work from anywhere on any device. You can do this by leveraging Virtual Private Network (VPN) technology, which establishes secure connections to the network for your remote users.

3 Third, you want to **DEFEND** your data from threats as attackers target your remote work environment. Do this by establishing a first line and last line of defense to block, detect and respond to attacks before compromise by using both DNS and endpoint security.

ıllıılı
CISCO Secure

Cisco Secure Endpoint:
The industry's first solution that unifies user and endpoint protection

‣ **Powerful Protection:** Machine learning, fileless and ransomware protection, next gen AV and more

‣ **Advanced EDR:** Hundreds of predefined queries, endpoint snapshot, threat hunting and endpoint isolation

‣ **Breach Defense:** First line and last line of defense against advanced threats

‣ **Secure Access:** Integrated multi-factor authentication and VPN

‣ **Securing Remote Work:** Verify, enable secure access and defend remote workers

‣ **Powered by Talos:** Sees more threats than any vendor on the planet

‣ **Simplified Security:** Built-in platform for better visibility and automation beyond the endpoints with SecureX
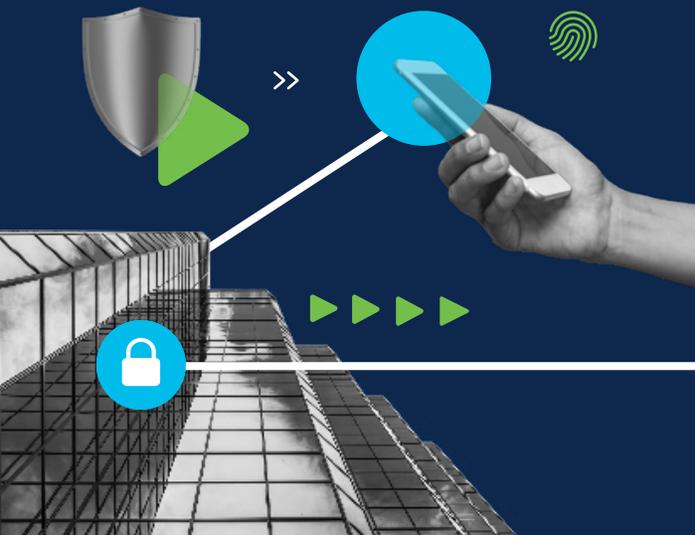
Stop the Threat to Remote Work … at the Endpoint

Protecting all devices your employees use to remotely access company resources is critical. When users and devices are off-network, antivirus and other preventative measures alone are no match for today's advanced threats, including zero-day exploits. You need to see an attack coming, not wait to respond to it after it reaches your endpoints. With a built-in platform approach to endpoint security you can:

• Protect your remote workers' devices, including their home computers and mobile phones. With multiple protection techniques at your disposal you can automatically block known threats using next-gen antivirus. You can defend the applications remote users use frequently including online collaboration tools like Zoom, Slack, Webex, Microsoft Teams and others from Zero day exploits, fileless remote code execution and other malware attacks. You can stop ransomware before it can cause damage. And you can employ machine learning to analyze behavior such as command and control activity, data exfiltration and more.

• Gain unified visibility and control of all devices being used for remote work, allowing you to see every threat to the endpoints — where it came from, where it's been and what it's doing. You can run playbooks that help you speed time to detection and response by automating critical tasks like performing live queries and proactively hunt for threats, and taking actions to automatically block known threats by isolating compromised endpoints and employing other attack surface reduction mechanisms.

Simple, Effective and Integrated Secure Remote Worker Solution from Cisco

Cisco's Endpoint Security solution defends your remote workforce by blocking attacks at the endpoint before compromise, while helping you respond to threats quickly and completely. It is an integral part of the Cisco Secure Remote Worker solution, helping accelerate business success with security that works together by combining the power of Cisco:

‣ **Duo** verifies the identity of all users before granting access to corporate applications.

‣ **AnyConnect** enables secure access to the enterprise network for any user, from any device, at any time, in any location.

‣ **Umbrella** provides the first line of defense against threats on the internet wherever users go.

‣ **AMP for Endpoints** provides the last line of defense, enabling protection, detection and response on the endpoint against known and unknown threats.

‣ **SecureX** protects remote work with a cloud-native built-in platform that automates actions and enables faster decisions.

Contact your Cisco account manager to get started with Cisco's Endpoint Security solution or sign up for a trial to test-drive our all-in-one Secure Remote Worker that is part of Cisco SecureX platform built for the security needs of remote workers.