3RT NETWORKS

POWERED BY LYNXX NETWORKS

WORK ANYWHERE:
6 WAYS TO PROMOTE SECURE EMPLOYEE PRODUCTIVITY

The future of workplaces is in the midst of a transition, with a variety of organizations experimenting with fully remote teams, bringing workers back to offices full-time or taking a mixed approach. No matter where your employees end up working from, you want to ensure they have the tools they need to be productive, yet you don't want to create cybersecurity gaps for hackers to exploit. Fortunately, focusing on productivity and security does not have to be an either/or dilemma.

You can implement strategies and solutions that help employees get their work done efficiently, wherever they're located, without sacrificing security.
Five ways to do so include:

1. Implement Endpoint Protection

Whether employees use their own devices from home or use company-owned devices in your main office, you need to protect the increasing number of devices that access your corporate network and data. For example, network security tools like antivirus software or firewalls might not work if a remote employee uses an off-network device.

As such, companies need to improve endpoint security with tools like Cisco Advanced Malware Protection (AMP) for Endpoints. This cloud-based solution uses machine learning and powerful investigation to automatically block known attacks and continuously discover new threat vectors as they arise. It also enables immediate endpoint isolation, should a device become infected, to stop potential spread to the network.

When exploring endpoint protection solutions, make sure they integrate with your existing security measures, so you don't end up sacrificing one aspect of security to make room for another. AMP for Endpoints, for example, is the only solution with an integrated approach that shares threat intelligence to and from all other parts of a security infrastructure.

2. Ensure Employees Use Trustworthy Devices

As employees work from anywhere, they might be more likely to use their own devices to access sensitive information. While you want employees to have this flexibility to get their work done, you don't want them to increase risk, such as if an employee loses their personal smartphone, which then exposes company data.

Tools like Duo Security, part of Cisco, can be used to help ensure the security of employees' devices, without being overly intrusive. For example, Duo can assess whether personal devices have proper security protections like passcodes on smartphones. Depending on whether they have these protections, IT teams can then adapt their access policies to corporate data and systems accordingly.

Duo also simplifies protections while letting employees work anywhere, such as by providing push notifications to an employee's smartphone when logging in from home to verify their identity.

3. Control Cloud Access

Using cloud-based tools can provide the flexibility needed to work from anywhere and stay productive, but you want to make sure that your employees use secure cloud systems and that they don’t accidentally create backdoors into your network.

Cisco Umbrella is a cloud-based solution that protects both on- and off-network devices, including company-owned and personal ones. By blocking cyberthreats at the DNS and IP levels, rather than just, say, scanning files that an employee downloads while working on-site, you can better prevent threats from reaching your network in the first place. Meanwhile, employees can still work as usual, without having to jump through overly restrictive hoops.

Beyond providing DNS-level security, tools like Cisco Umbrella can also be used to protect against cloud security threats with its Cloud Access Security Broker feature. This feature can help identify issues such as suspicious logins based on User and Entity Behavior Analytics, as well as providing visibility into the cloud apps that connect to your network.

4. Leverage Secure Collaboration Tools

Modern collaboration tools for activities like videoconferencing can make remote work just as productive as on-site work, but not every collaboration tool provides the same level of security. If you're discussing sensitive information during a video call, for instance, you wouldn't want an unauthorized user to be able to listen in.

Using tools like Cisco Webex Meetings and Teams can be a great way for employees to stay productive remotely, while still having a high level of security. In addition to being used for webinars and remote training purposes, Webex Meetings can be great for teams that want to have video calls for online meetings from essentially any device. It integrates with Webex Teams to allow users to message each other seamlessly, either during meetings, in the office or on-the-go.

5. Partner With a Consultant

Cybersecurity developments move quickly, and if you're not up to date on all fronts, those vulnerabilities will become prime targets for attackers. Instead of investing internal teams in the full-time job of researching attack vectors and shoring up security, many businesses leverage third-party security experts to take on the heavy lifting while keeping their IT teams focused on business initiatives. Managed service providers have the resources to keep their teams consistently updated on emerging threats and defense strategies, and they can help you apply them in a way that makes sense for your organization.

Consider creating a list of security priorities, and check providers against your list. Make sure they have extensive experience in network security, endpoint protection, collaboration tool security, data backups and other items you identified as important to your organization. Further, make sure they have experience securing companies with remote or disparate workforces, so you can be sure your company is protected from every angle.

6. Maintain an Up-to-Date Data Backup:

With employees potentially working from a combination of locations that can change from day to day, you want to ensure they can access the data they need remotely, while still maintaining a secure, up-to-date version of your data in case anything goes wrong.

Many organizations don't realize the backup and continuity power of some of the applications they're already using. Microsoft 365, for example, comes with resiliency and recoverability capabilities that go far beyond simple backups. Further, some companies supplement their existing solutions with more complete solutions, like Veeam's cloud backup, for a more complete and reliable data recovery model.

The most complete coverage option when it comes to data recovery is usually to partner with a managed provider. 3RT Networks, for example, offers offsite data protection as a service (DPaaS), which includes a data protection plan built and tailored specifically for your company's unique setup. With DPaaS, companies can rely on continuous monitoring and optimization, and they have a go-to partner they can call, should disaster strike.

Be Ready to Work Anywhere

While the future of work might not be clear at this moment, implementing these types of solutions can provide your organization with the flexibility to stay productive and secure, no matter where employees work from.

To learn more about how your organization can implement the technology and oversight you need for any environment, get in touch with our team of experts, who can design and implement agile solutions to help you improve productivity and profitability.