The security impact of rapidly enabling remote workers

A practical guide for organizations

By Jason Rader, National Practice Director of Network and Cloud Security

Like many organizations today, you may be facing immediate requirements to change over your workforce from on-site to remote or mobile. This is an opportunity to enable new capabilities for employees while continuing to deliver on commitments to clients and the business' financials.

As security professionals often say, the worst time to figure out how to do something is when you absolutely have to do it now.

When properly planned and prepared for, rolling out the changes needed to support a mobile workforce can be tricky. When rolled out without proper notice and preparation, there are areas where outside assistance can make the difference between success and failure.

Working with an organization that has the technology and staffing capabilities along with the experience that it takes to align the people, processes, and technologies required to rapidly deploy and enable remote workers is a definite way to mitigate risk when getting things right the first time is truly the only option.

Critical considerations

Regardless of the reason, enabling a remote workforce is more than simply giving users remote access to the corporate network, and it involves much more than that from a security perspective.

Identity and access management

How do we…

- Remotely create accounts and administer passwords?
- Handle user provisioning?
- Configure and enable remote access at the endpoint?
- Monitor remote workers and ensure visibility of network activities?
- Audit new capabilities?

Collaboration and information sharing

How do we…

- Ensure collaboration is easy?
- Make file access and sharing both simple and secure?
- Appropriately classify new data?
- Securely store new data?

Hardware and software

How do we…

- Determine if a Bring Your Own Device (BYOD) policy is needed?
- Create or refine a secure BYOD policy?
- Provide new hardware to employees?
- Manage secure updates?

Network

How do we…

- Effectively manage network capacity?
- Ensure the right hardware is in place?
- Best facilitate remote access with enhanced security?

Security standards and compliance

- How does enabling remote workers deviate from defined standards?
- Do new standards need to be defined?
- Have the changes we've made in this crisis made an impact to our ability to prove compliance?
- Do we need to perform an audit?

Communications and policies

- How do we communicate when traditional tools are overloaded or inaccessible?
- What are the alternatives to Webex, Teams, Skype, etc.?
- Is remotely working from home covered in the acceptable use policy?
- Have employees been made aware of any new policies?

How to go forth

Use these considerations as a basis for discussion with all stakeholders in planning for key changes and addressing your overall security program.

When confronted with unplanned needs, it's best not to wing it. Work with professionals who have a proven track record and can support you in addressing immediate needs while enabling current security initiatives and aligning solutions with corporate security governance and compliance requirements.

Insight's security practice is comprised of business consultants and security experts who can help your organization face new and emerging challenges, from strategy through implementation and management.

Ask us for more information — we're here for you.

solutions.insight.com/transforming-together

Insight