Crowe

Q&A

Security Risks of Rapidly Going Remote

Frequently Asked Questions

Smart decisions. Lasting value.™

Q: What are the best options for a business to implement remote access?

This is a tough question to provide a one-size-fits-all answer to, since every organization faces different constraints, such as number of users, cost, licensing, bandwidth restrictions, devices available, and technology already in use. If you need to design a remote access solution from the ground up, there are a couple of primary options.

Option 1: VPN

First, you can deploy hardened, Microsoft Windows™ Active Directory-joined laptops to all your employees. The devices would be deployed with a preconfigured, always-on, split-tunnel virtual private network (VPN) with multifactor authentication (MFA) enabled. Joining a laptop to the domain allows IT to enforce its policies via Group Policy, which can automatically and programmatically bring devices into compliance with companywide IT policies and security baselines.

As for the VPN, a split-tunnel VPN pushes only traffic intended for the internal network through the VPN tunnel and allows normal internet traffic to be routed through the home network as normal. This method can help reduce the load of traffic going through the internal network.

Most organizations have a VPN-capable firewall and an Active Directory infrastructure. If you don't already have one set up, it might take a couple of days to properly configure the VPN and verify that all laptops have the correct software installed.

Option 2: VDI

The virtual desktop infrastructure (VDI) option might be better than a VPN if inadequate licenses, bandwidth, or laptops or a VPN firewall are present.

Depending on the computing requirements of your users, a VDI could be set up to provide access to specific on-premise applications with sensitive information so that data isn't directly routed over the internet to a user's home network. There are a multitude of ways to use VDIs, so if bandwidth through the internal corporate network were an issue, cloud-based VDIs could be used to provide quick access to virtual desktops that would only need connectivity from the cloud to internal resources, therefore reducing the stress on internal networking equipment.

This option requires a VDI infrastructure to be put into place, which can be expensive and time-intensive to set up if not already present.

Q: What are the top mistakes an organization might make in deploying remote access?

Some common missteps include (in no particular order):

- Allowing internal servers to become directly accessible from the internet (such as remote desktop protocol (RDP) servers) without any additional hardening, monitoring, or access restrictions
- Not enabling MFA for VPN and other remote access
- Allowing unsecured employee endpoints access to the internal network without any security baseline or additional monitoring
- Not hardening corporate devices
- Trusting employee home networks
- Not testing remote infrastructure at scale
- Not defining a data classification and data management strategy, which should encompass company data in all forms in an employee home environment, including data on paper

Q: Employees are using personal devices. How can organizations establish secure access to company data?

When considering the use of bring-your-own-device (BYOD) systems – in other words, employee personal devices – there are many risks to an organization. The device could be unpatched and be susceptible to malware such as ransomware or it could allow attackers to use remote code execution to gain control of the device remotely.

A popular option when using employee devices is to provide access to internal resources via VDI rather than direct VPN access. Although this method would have the advantage of not directly storing sensitive data on the device, there are still ways an unsecured machine could allow for data compromise.

For example, malware that can capture screenshots and log keystrokes could be installed on devices, which could be enough to steal credentials and use them for nefarious purposes, even if those devices are simply being used to access a VDI environment. This same risk applies when running remote access software such as TeamViewer or LogMeIn.

Administrators should not allow remote access of any type from BYOD systems without first setting standards for security controls on those systems, including but not be limited to patch levels, OS version, AV status, AV last scan, password settings, and firewall configuration. Some remote access software such as VPNs can enforce compliance with these minimum standards, but even if they cannot be programmatically or technically enforced, these data security standards should be clearly communicated as part of a companywide technology policy.

Companies should also specify what types of data will be allowed on personally owned machines. For example, checking email might be permissible from a personal device, but storage of company design documents or financial information might be prohibited.

Q: Is there anything we should be doing to secure corporate assets on home networks? How can home networks be better secured?

Corporate assets should be managed by a mobile device management (MDM) solution. This means that there should be some sort of managing agent on the device or a centralized server that can monitor the device, check compliance with company device policies, monitor and trigger patches or updates, and generally track the device. If possible, an agent should capture log data and forward that to security information and event management (SIEM) software or another security solution for security monitoring. These devices should have their host-based firewalls enabled to only communicate with explicitly allowed or required services and block all others.

Employee home networks should be viewed as potentially hostile and certainly untrusted. Many employees use consumer routers and do not 1) change the default administrator credentials, 2) update their device regularly, or 3) use strong Wi-Fi passwords. These easy steps are critical to securing a home network.

Other threats to home networks include other devices that might be compromised or infected by malware or unsecured IoT devices. Both scenarios could allow attackers the ability to communicate with the employee device in question; therefore, devices should be hardened against those threats. Employee devices can have their host-based firewall enabled to prevent communication with untrusted devices. For more savvy users, segmentation can be used to place the employee device on a portion of the home network that the other devices cannot talk to (such as a guest network).

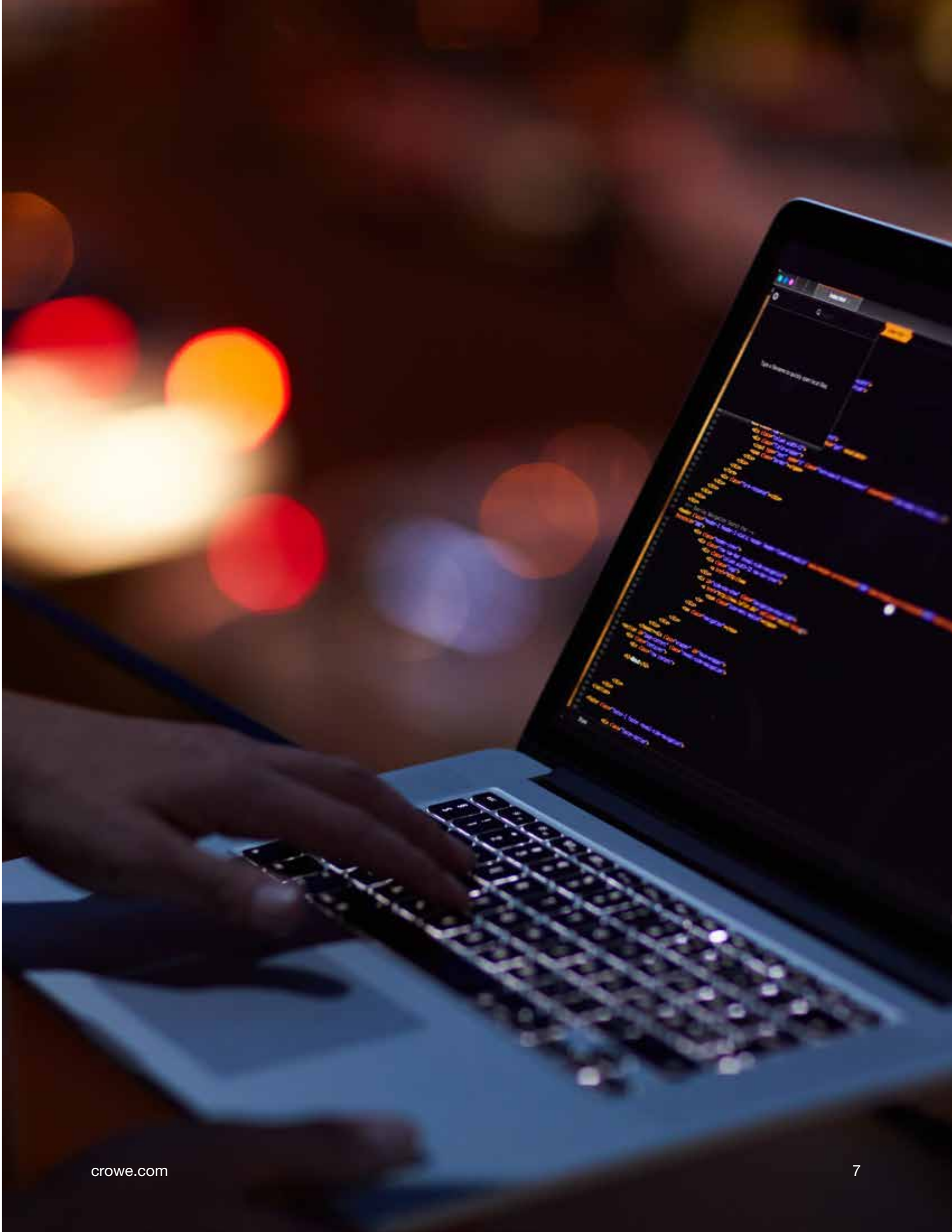
Q: Where do LogMeIn, TeamViewer, and Google Chrome Remote Desktop sit in the spectrum of remote access solutions? How do they compare to a VPN?

VPN technology has been in corporate environments for a long time. It often comes bundled as a configuration option within purchased equipment and software. TeamViewer, LogMeIn, and others are third-party software applications. Therefore, companies should have patching and support plans in place to make sure the software is appropriately updated and supported.

Beyond software updates, companies should learn how the technology works. The software could be transferring sensitive information in the form of keystrokes or video to servers operated by these third parties all over the world. Questions to consider when examining these products include:

- Do the third-party software providers have access to that data?
- Is there end-to-end encryption? If so, who holds the encryption keys?
- Where is the data going?
- What is the authentication requirement? Because this is an external service, MFA should be a consideration.

In summary, VPNs are a vetted technology that uses known protocols and encryption schemes, while third-party remote access software might function in unexpected ways and transfer data via different methods. VPN technology joins the machine to the corporate network, whereas remote access solutions such as TeamViewer and LogMeIn can provide remote interactivity without placing a device directly into an internal network. These solutions should not be disregarded altogether, but rather understood and considered depending on the type of information being transferred.



Q: What should companies communicate to their employees as they get used to the new normal of remote access? Additionally, what should companies do about the end-user risk, and what are some of the scams employees should be looking out for?

These days, most of us are out of our element, and nothing seems normal, which places additional stress on each of us. All this makes it easy to lose focus and make mistakes we wouldn't make in our normal environments. During this time, employees should be reminded to:

- Understand that others might attempt to take advantage of the company or its employees
- Be aware that phishing attempts are on the rise
  - If you are not expecting something or you don't recognize the sender, slow down and analyze the situation.
  - When in doubt, pause and ask someone for a second opinion – or more importantly, contact your IT department.
  - If anything seems urgent, be on heightened alert.
- Accept official communication ONLY from identified sources
  - These can be organizational email inboxes or individual email inboxes.
  - The CEO sending messages from a Gmail account is likely not legitimate and has been a tactic employed by attackers to fool employees.
  - As policies change and companies shift, attackers might attempt to take advantage of the turmoil to inject their own messages.

Many employees are used to receiving instructions in person. This means it might be easier for attackers to take advantage as people are no longer relying on face-to-face validation of requests and could therefore follow unverified instruction via technology-based channels.

There are some fairly accessible technologies that allow people to impersonate audio and even video of people (a method known as a "deepfake"). We expect to see some cases of cyberattacks involving deepfakes if this remote work situation persists for months.

When it comes to phishing, threat actors are as busy as the rest of us, only they are working on new social engineering schemes. Many are the same techniques we've seen in the past, just with a new twist, as explained by a recent KnowBe4 alert[1]:

- **Emails that appear to be from organizations such as the Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO).** Scammers have crafted emails that appear to come from these sources, but they contain malicious phishing links or dangerous attachments. For example, a malicious website pretending to be the live map for COVID-19 global cases by Johns Hopkins University is circulating on the internet.
- **Emails that ask for charity donations for studies, doctors, or victims that have been affected by COVID-19.** Scammers often create fake charity emails after globally reported phenomena such as natural disasters or health scares such as COVID-19.
- **Emails that claim to have a "new" or "updated" list of cases of COVID-19 in your area.** These emails could contain dangerous links and information designed to scare you into clicking on the link.

There should be no shame in double- and triple-checking any request that seems unusual, unexpected, or urgent, and especially critical decisions of financial transfers, data transfers, and data access. If we slow down and stay focused, we can recognize the signs of threat actors.

Q: How can organizations deal with security monitoring from a remote perspective? What about remote incident response (IR)?

One of the first requests to make when assisting in IR is "Show us your logs." The reality is that if an organization didn't capture what happened as an ultimate source of truth, it's extremely difficult to understand what occurred in the environment, let alone help eradicate the threat. This becomes more important for remote devices on employee home networks, where there are likely no additional network logs to assist in the process.

Therefore, it is critical that logs are captured and stored from remote workstations, and if possible, those logs should be ingested and analyzed in real time by an SIEM solution or managed service provider that can monitor for anomalies and malicious activity even when the device is not directly connected to the corporate network. The reality is that you can't stop what you don't even know about, so gaining visibility is the first step in evaluating security and detecting incidents.

When it comes to dealing with an incident, containment is priority number one. The fundamentals don't change:

- Response teams comprised of individuals within the organization should assist with:
  - Technical support
  - Legal and regulatory compliance
  - Executive decisions
  - Communications
  - Third-party interactions
- Technical teams should focus on containment, eradication, and business continuity.
  - While containment is a primary focus, organizations should also understand how they can maintain uptime and recover quickly.
  - In some cases, organizations will rush to contain at the risk of maintaining chain of custody. Maintaining chain of custody can be important to the process of eradication and recovery, but it is a delicate balance when time is not on your side.
- Legal teams should be involved from the onset to understand and manage interactions with law enforcement, comply with state and federal regulations (including privacy regulations), and certainly to manage any ransomware demands.

- Executive leadership is important as well, as key business decisions often need to align with customer and third-party relationships.
- The communications team and communications plan should be a top priority, as the only way to overcome a crisis is efficient and effective communication from the top down. The communications team is as important in managing a crisis as any other.

Right now, crisis management people are already overloaded with one crisis. A cybersecurity incident will require them to split their time three ways: day-to-day, the COVID-19 crisis, and a cybersecurity crisis. If possible, it might be prudent for organizations to have some sort of check-in to determine if they need to rethink their original IR plans. While it seems like one more distraction, it can be very beneficial to have proactively thought through this process.

Q: Should organizations be worried about insider risks? As companies widen the threat landscape through mobile workforce deployment, could the sale of systems access and confidential data by insiders become more likely?

The kinds of resources and marketplaces available to those looking to make a quick buck through cybersabotage or sale of internal access have certainly grown. Online marketplaces such as Torum as well as other clones of the now-dead AlphaBay, Hansa, and infamous Silk Road dark websites seem to be everywhere. These sites, combined with modern tools such as cryptocurrency, seem to make criminals virtually anonymous, all pointing to an easier commoditization of insider access.

The convenience of committing a crime like that may be enticing. However, in this climate, it appears employees might be more concerned with keeping a steady paycheck. Therefore, it would come down to incentivization. If an employee were to be terminated remotely, that incentivization might finally be there. That former employee would have the technology, remote access to the network, and a motivation to make some money at the organization's expense.

To prevent such a problem, any termination scenarios should be heavily coordinated between human resources and IT, and the remote management technologies in use, such as an MDM solution, should be used to prevent an individual from maintaining any access to the organization's environment or company data post-employment.

Learn more

Glen Combs
Partner
+1 859 264 3168
glen.combs@crowe.com

Troy La Huis
Digital Security Sevices Leader
+1 616 233 5571
troy.lahuis@crowe.com

Please reach out if you have additional questions. To stay up-to-date on cybersecurity issues, follow our blog at crowe.com/cybersecurity-watch.

---

[1] Stu Sjouwerman, "Extreme Measures: The Epidemic of COVID-19 Phishing Emails Rages On," KnowBe4, March 16, 2020, https://blog.knowbe4.com/extreme-measures-the-epidemic-of-covid-19-phishing-emails-rages-on

crowe.com

CC2062-025D