BlackBerry

Whitepaper

Seven Strategies to Securely Enable Remote Workers

macOS

Laying the ground-work to securely enable a remote workforce could make or break a company's ability to sustain business operations should a crisis require large populations to remain at home.

Is your organization ready to securely support a wide range of remote workers in the wake of a global pandemic? Given the uncertainty a widespread health crisis can bring, infectious disease specialists at the CDC and elsewhere have advised organizations to prepare for the possibility of social distancing and extended period quarantines as part of their business continuity and disaster recovery planning.

For businesses and other organizations, this preparedness should include leveraging a Zero Trust security architecture and the right tools to ensure workers can securely access company systems, data, and productivity suites with minimal disruption to workflows. Zero Trust strategies assure that effective security controls are in place to govern every single user, device, application and system interacting with an organization's IT environment.

Maintaining a seamless workflow for remote workers impacted by a pandemic or other wide-scale event will require IT and cybersecurity teams to implement Zero Trust strategies to securely support the collaboration and productivity tools that assure continuity for critical business operations.

Laying the groundwork to securely enable a remote workforce could make or break a company's ability to sustain business operations should a crisis require large populations to remain at home. This whitepaper provides insights on key areas of focus and advice for organizations when considering the best solution options to support a secure remote-only workforce.

Removing the VPN Speedbump

Many of today's traditional remote work security solutions depend upon VPN (virtual private network) technology that can not only impede productivity due to poor performance, but also may not effectively safeguard an organizations' networks and workflows against sophisticated threats, and in some cases may even introduce security vulnerabilities.

As far as performance goes, VPN users or those considering them to support remote workers need to understand that there are limitations to speed and functionality. VPNs can only perform as well as the speed that the Internet connection provides, and for consumer-grade ISPs that can mean connection speeds that are significantly lower than a user may be accustomed to when working within their corporate network environment.

Furthermore, the fact that the VPN has to encrypt and decrypt every packet during a session means users will likely experience decreased performance by the very nature of how VPNs are designed to work. This is especially true if the workflows involve large files, images, video content or computational processes.

Large enterprises need a faster, more secure channel of connection that adheres to Zero Trust security principles to allow remote workers access to their files and productivity software in order to enable work from home. This will be key in a potential pathogen outbreak that results in a situation where many employees who traditionally work from the office will be forced to work remotely for extended periods.

A viable solution should offer secure access from anywhere to any application, desktop tool or file on a corporate network while allowing employees, contractors and partners to use their personal devices to access behind-the-firewall content without sacrificing the performance they enjoy when working in a traditional corporate-owned and managed environment.

A solution should also offer secure and auditable aggregation of enterprise assets in a single virtual desktop environment that provides access to all enterprise apps, tools and files even when working offline in the case of intermittent connectivity, and provide turnkey access management to quickly onboard or offboard users and provision endpoints easily.

VPN Limitations:

- Costly licenses
- High implementation costs
- Increased Network Requirements
- Complex to set up
- Speed and functionality limitations
- No offline capabilities in the case of intermittent connectivity

Device-Agnostic Capabilities are a Must

The productivity apps that a great solution should provide access to:

- Email, calendar and contacts
- Documents
- Microsoft® Office 365® apps
- Intranet sites
- Cloud-based business apps (e.g., Salesforce or Workday®)

Users today have high expectations about how they are able to conduct business, and a secure remote work solution needs to support the most common workplace applications, including Microsoft® Word, Excel® and PowerPoint®, as well as the ability to share documents with colleagues anytime, anywhere. IT teams should be seeking out solutions that allow users the ability to conduct business no matter where or when from which device on the most common operating systems, including Windows®, macOS® and Linux®.

Ideally, the solution should provide secure browser functionality to run common web as well as legacy applications, and also provide access to intranet resources users are accustomed to when working in the office. A browser-based solution also allows users to connect seamlessly to email, calendar, contacts and more without the need for IT to actively manage individual devices or cumbersome VPN systems that may not offer the same level of performance.

A secure browser-based platform as part of a Zero Trust architecture eliminates the need to manage a fleet of devices - managing the secure browser is all it takes - and it also eliminates device-specific and operating system obstacles.

Anticipate Mobility Challenges at Scale

There are several alternative document, spreadsheet, and slide creation software platforms out there in this SaaS era that never quite cut it in an enterprise environment. Most workers are used to Word, Excel, and PowerPoint, so IT teams will need to provide seamless access to Microsoft® Office to maintain their productivity levels when working from home.

In the face of circumstances that will require a majority of the workforce to go remote, organizations will need solutions that can mobilize all their core business applications including collaboration, ISV and custom-developed tools. However, the conflicting needs of IT, developers and business owners often present significant barriers to mobile-only initiatives. Organizations should look for solutions that offer a common application platform to speed mobilization process by enabling each stakeholder to accomplish their business-critical responsibilities with little to no interruption.

In a crisis situation where a workforce accustomed to conducting business in-office needs to shift to a remote-only mode of operation, enterprises will need to be able to accelerate mobilization and increase IT agility while ensuring critical business functions are not disrupted. In some cases, this may mean in-house developers will need to quickly build custom applications to support workflows using their preferred development tools and methodologies to maximize efficient code reuse while conforming to organizational security policies. A good enterprise mobility solution should allow business unit leaders the flexibility to adopt or develop a wide range of applications without requiring significant IT investments with long procurement cycles.

A rapid shift to mobility also means the addition of new endpoint applications to the network along with business demands that will emerge on an almost daily basis. IT teams will be challenged to enable services to meet these ever-changing requirements and will need to rely on solutions that can quickly scale to enable the assimilation of new applications and devices. A good solution should simplify management by way of a single platform for scenarios that include business-to-employee, business-to-partner, business-to-customer and business-to-supplier needs even in cases where IT does not control the device(s) employed.

Enable Productivity Regardless of Internet Connectivity

In the event that a wide swath of workers will need to swiftly socially distance themselves from the general public to stay safe during a widespread pathogen event, it's likely that some of them will run into periodic connectivity issues in certain instances. This means that the remote work platform an organization chooses needs to have a robust offline mode to provide access to a range of assets even when the Internet is not accessible.

A viable solution must allow users to securely create, edit and format documents, spreadsheets, PDFs and presentations from any mobile device with the minimum disruption to normal workflows. Most office productivity tools are designed to function optimally with connectivity, so IT teams should ensure options are in place so a remote workforce can maintain access to productivity tools in a crisis even during periods where they have to work offline.

Send mass notifications and collaborate in times of crisis

- Rapidly alert recipients - via SMS, mobile app, and secure email
- Target notification recipients - by location or groups
- Account for employees - stay apprised of employee status, take steps to prevent the spread of illness and avoid loss of productivity

Reliable, Company-Wide Crisis Communications Emergency Notifications

A mobile workforce that may be subject to periods with no Internet connectivity presents another critical challenge: maintaining company-wide critical communications and the ability to monitor employee wellbeing. Organizations should consider the benefits of communications tools designed specifically for collaboration in times of crisis. An emergency notification system can be an indispensable mitigation tool when normal business operations are interrupted due to an emergency, and the solution should enable real-time visibility into the safety status of your personnel for more effective crisis response and assured business continuity.

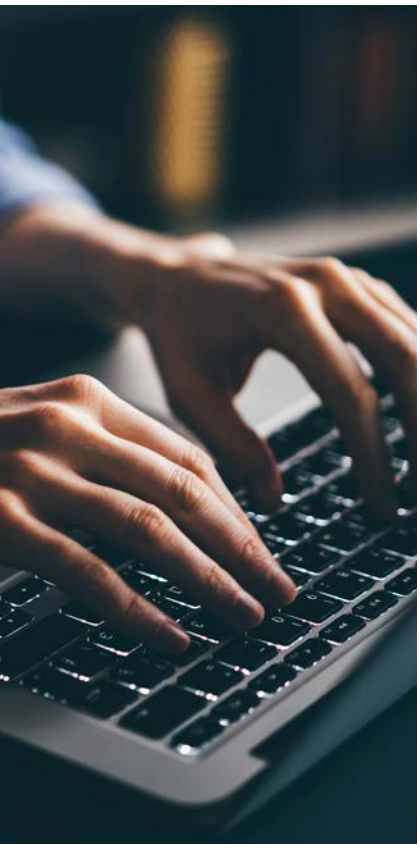
These tools can enable your response teams and leadership to maintain better situational awareness during an incident, provide better visibility into the status of key business units, and allow teams to collaborate securely and efficiently with internal resources and external third-party services. A viable solution should unify all communication modalities to alert everyone with a single click so emergency managers can reliably provide rapid communication across the entire enterprise.

The most advanced endpoint security options for mobile devices leverage Artificial Intelligence (AI) and have the ability to prevent advanced threats pre-execution, including fileless attacks, zero-day attacks, and external device-based attacks.

Reinforce Cyber Hygiene Best Practices

Organizations responding to a crisis by mandating remote work should also consider efforts to refresh their employees on basic security best practices, including the potential risks posed by connecting to public Internet when working from places like cafes or libraries.

All devices used for work should be updated with the latest versions of firmware, operating systems, and software, and organizations should consider the security benefits of whole disk encryption software that can prevent unauthorized access to sensitive data should a mobile device be lost or stolen.



Devices used for work, whether company issued or owned by the employee, should also have approved endpoint protection software installed. The most advanced endpoint security options for mobile devices leverage Artificial Intelligence (AI) and have the ability to prevent advanced threats pre-execution, including fileless attacks, zero-day attacks, and external device-based attacks. Solutions should also offer features like script control and memory defense, and should have the ability to detect and block attacks without the need for human intervention and should not be dependent on cloud-lookups, signatures, heuristics, or sandboxes, as well as the ability to protect devices while working offline as well.

It All Needs to be Secure and Easy

Even as organizations smooth the path to easy access for remote workers during a crisis situation, they'll need to assure mobility solutions offer the highest level of security where authentication and user access is concerned. Organizations should consider the benefits of a platform that adheres to Zero Trust principles and can provide continuous authentication so only authorized users are granted access to the documents and systems they require for their job duties.

Zero Trust solutions that employ machine learning and predictive AI to dynamically adapt security policies enforcement based on criteria like user location, device handling and other behavioral factors not only provide effective security controls, they can also protect against human error and well-intentioned security workarounds. Continuous authentication can also improve the user experience by minimizing disruptions and the need to reauthenticate across multiple devices and applications unless warranted.

Continuous authentication leverages passive biometrics and other usage-based patterns to perpetually verify a users' identity in an unobtrusive fashion while assuring that an unauthorized user is swiftly and automatically blocked from access. This enhances the security posture of the organization and at the same time improves the end-user experience. Continuous authentication solutions learn in order to apply security intelligently based on understanding of the user and user behaviors, relaxing security policies when a user is in a trusted location and dynamically adjusting when they are in a higher-risk location.

Finally, the whole process should be manageable for IT administrators. With a potential flood of new remote users that may be imminent from a pandemic or other crisis situation, IT will need a platform that can simply onboard and offboard users, devices and applications.

Conclusion

Most enterprise IT leaders today already recognize that offering remote work opportunities to the workforce is no longer a “nice-to-have” perk for a select few workers in limited situations; enterprises are increasingly finding that remote work is a “must-have” job requirement.

Zero Trust strategies are essential to assuring effective security controls are in place to manage every user, device, application and system that touches an organization’s IT environment. Maintaining a seamless workflow for remote workers will require IT and cybersecurity teams to implement Zero Trust strategies to securely support the collaboration and productivity tools that assure continuity for critical business operations.

The recent COVID-19 or Coronavirus outbreak highlights the necessity for organizations to build-out a remote infrastructure based on Zero Trust strategies to securely support a large mobile workforce and maintain business continuity in a crisis.

For more information visit

www.blackberry.com

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.