Cyber Talk

Coronavirus Outbreak
Secure Remote Access Guide

Coronavirus Outbreak

Secure Remote Access Guide

The COVID-19 virus outbreak, also known as the coronavirus, has caused major supply-chain disruptions for a wide range of industries around the world. Aerospace companies Airbus and Boeing, and automakers Tesla and G.M. have both closed production facilities while Apple is experiencing disruptions that have delayed iPhone production in China.

COVID-19 has also resulted in global employers, including technology companies, requiring their employees and third-party contractors to work from home.

Today, 43% of all U.S. employees work off-site at least part time, according to Gallup's State of the American Workplace report.[1] Research also shows that employees believe working remotely is not a productivity hinderance and the majority of Americans feel that remote workers are just as productive as those who work in an on-site office.[2]

With companies now adopting remote work en masse due to the coronavirus threat, online security has become a critical issue.

1 https://www.gallup.com/workplace/263510/manage-remote-employees.aspx

2 https://news.gallup.com/poll/184649/telecommuting-work-climbs.aspx

Business Continuity, Disaster Recovery and the Coronavirus

In response to crises such as the coronavirus, organizations should have IT disaster recovery plans in place that have been developed in tandem with business continuity plans. These plans should include business priorities and recovery time objectives for IT resources along with a business impact analysis. Technology recovery strategies should also be developed to restore hardware, applications and data in time to meet the needs of the business in the event of an outage.

Secure remote access also plays a critical role when considering disaster recovery and business continuity, as organizations must be flexible enough to enable remote work for a majority or all of their employees while still achieving normal workforce productivity despite external disruptions.

The coronavirus has forced organizations to shift their employees and IT resources so that they can function with work at home scenarios or in secure locations.

Guide to Implementing Secure Remote Access

Many organizations let their employees, contractors, business partners, and vendors use enterprise remote access technologies to perform work remotely, leveraging organization-owned and bring your own device (BYOD) client devices that must be secured against data breaches and theft. Security concerns include the lack of physical security controls, the use of unsecured networks, connection of infected devices to internal networks, and the availability of internal resources to external hosts.

In addition, security policies and agreements with third-parties regarding device security cannot always be enforced, potentially leaving unsecured, malware-infected, and compromised devices connected to sensitive organizational resources.

Therefore, to secure organizations using remote access technologies to mitigate BYOD and third-party-controlled access risks to network resources, the National Institute of Standards and Technology (NIST) recommends that organizations implement the following controls:[3]

Plan remote work-related security policies and controls based on the assumption that external environments contain hostile threats.

- Organizations must assume that client devices used at external locations by employees and third-parties are susceptible to loss or theft and could be used by malicious actors to access data or gain organizational network access.

- Mitigating client device loss or theft includes encrypting device storage and sensitive data stored, and not storing sensitive data on client devices altogether. For mitigating device reuse threats, use strong and multi-factor authentication.

Develop a remote work security policy that defines telework, remote access, and BYOD requirements.

- Remote work security policies should define remote access types, devices, and the type and access policies for remote workers.

- The policies should also cover how remote access servers are administered and how their policies are updated. Organization should make risk-based decisions about what levels of remote access should be permitted from which types of client devices.

3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Ensure that remote access servers are secured effectively and are configured to enforce remote work security policies.

- The security of remote access servers is particularly important because they provide a way for external hosts to gain access to internal resources, as well as a secured, isolated telework environment for organization-issued, third-party-controlled, and BYOD client devices.

- In addition to permitting unauthorized access to enterprise resources and telework client devices, a compromised server could be used to eavesdrop on communications and manipulate them, or to provide a "jumping off" point for attacking other hosts within the organization.

Secure organization-controlled remote work client devices against common threats and maintain their security regularly.

- Remote work client devices should include all local security controls used in an organization's secure configuration baseline for its non-telework client devices.

If external device use (e.g., BYOD, third-party controlled) is permitted within the organization's facilities, strongly consider establishing a separate, external, dedicated network for this use with remote access policies.

- Allowing BYOD and third-party-controlled client devices to be directly connected to internal enterprise networks adds risk, as these devices do not have the same security safeguards as the organization's own devices.

NIST also recommends placing remote access servers at the network perimeter and defines four types of remote access methods:

- Tunneling servers provide administrators control over the internal resources for remote worker access at the network perimeter.

- Portal servers that run the application client software on the servers themselves. Placing them at the network perimeter because the remote access user is only running applications on the portal server, not on servers inside the network.

- Remote desktop access does not involve remote access servers, so there is no issue with the placement of the remote access server.

- Direct application access servers run the application server software on the servers themselves. Placing them at the network perimeter has a similar effect as the remote access user is only running applications on the direct application access server, not on servers inside the network.[4]

4 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Vendor-based Corporate Access

Vendor-based Corporate Access enables organizations to meet NIST remote access security standards and more while easily managing least privilege access to internal resources with real-time, intelligent trust decisions based on defined policies and contextual data. The solution's zero trust architecture also restricts user access to authorized resources so that the right people have access to the right resources at the right time, without the need for a VPN.

With granular access control over and within each resource, based on the dynamic and contextual assessment of user attributes and device state, Vendor-based Corporate Access provides a rich set of rules that can be enforced across all users, servers and enterprise data stores, including user commands and database queries.

The security of remote access servers, such as gateways and portal servers, is also important as they let external hosts access internal resources, as well as provide a secure, isolated remote work environment for organization-issued, third-party-controlled, and BYOD client devices.

Vendors, like Check Point, provide several secure remote access options for remote workers, including VPN Replacement, Third-party Access, Developer Access and Privileged Access Management (PAM) as well as application. database and remote desktop access that meets or exceeds NIST security controls.

Additional benefits of Vendor-based Corporate Access include:

- Agentless architecture for deployment in under three minutes with optional security certificates.
- Granular access controls over and within each resource based on the dynamic and contextual assessment of user attributes and device state. Policies can be enforced for all users, servers and enterprise data stores, including user commands and database queries.
- Control over third-party access to and within any application, server, database or environment with monitoring, logging and alerting functions.
- SSO for SSH keys are maintained in a central and secure location, eliminating manual management of static credentials and reducing the risk of lost or compromised keys.
- Management and monitoring of database access with granular control over permissions.
- Audit trails of user activity including server access executed commands and queried data, as well as fully recorded sessions.

Part of Check Point SASE

Check Point Corporate Access is part of CloudGuard Connect, which is redefining **SASE** by making it **easy** to secure access to **corporate applications, SaaS and the internet** for any user or branch, from any device, without compromising on security.

To learn more, **contact us for a demo** or visit us at **checkpoint.com.**

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com