SOLUTION BRIEF

Secure Remote Access for Your Workforce at Scale

Executive Summary

Organizations face a number of different potential emergency situations, such as illness, flood, hurricanes, and power outages. Implementing a business continuity plan is essential to ensuring that the organization is capable of maintaining operations in the face of adversity and preparing for potential disasters.

An important consideration for organizations developing a business continuity plan is that the organization may not be capable of sustaining normal operations onsite. The ability to support employees working remotely is essential to ensuring both business continuity and security. Fortinet solutions offer an integrated solution to support telework. FortiGate next-generation firewalls (NGFWs) have built-in support for IPsec virtual private networks (VPNs), enabling remote workers to connect securely to the company network. With endpoint protection, provided by FortiClient, and multi-factor authentication (MFA) with FortiAuthenticator, organizations can securely support remote work and maintain business continuity.

The ability to securely support a remote workforce is an essential component of any organization's business continuity and disaster recovery plan. An organization may be incapable of sustaining normal operations onsite, due to a power outage or similar event, or illness or flooding may make it unsafe for employees to travel onsite.

In these scenarios, an organization must be capable of supporting secure, remote connectivity to the corporate network. For over 400,000 Fortinet customers, their existing technology deployment already contains this functionality. FortiGate NGFWs have integrated support for IPsec VPNs, enabling secure connectivity for employees working from alternate work sites.

Remote work decreases employee unproductive time by an average of 27%.

Remote employees work an average of 16.8 more days per year than onsite employees.

85% of employees claim that they reach maximum productivity when working remotely.[3]

Allowing remote work increased employee retention in 95% of organizations.[4]

Securing the Remote Workforce with FortiGate NGFWs

The IPsec and SSL VPNs integrated into every FortiGate NGFW offer an extremely flexible deployment model. Remote workers can either take advantage of a clientless experience or gain access to additional features through a thick client built into the FortiClient endpoint security solution. Power users and super users would benefit from deploying a FortiAP or a FortiGate NGFW for additional capabilities.

Fortinet solutions are designed to be easy to use from initial purchase through end of life. FortiGate NGFWs and FortiAP wireless access points include zero-touch deployment functionality. Appliances deployed at remote sites can be pre-configured before they ship, allowing for automatic set up onsite, which ensures business continuity and support for telework.

The Fortinet Security Fabric takes advantage of a common Fortinet operating system and an open application programming interface (API) environment to create a broad, integrated, and automated security architecture. With the Fortinet Security Fabric, all of an organization's devices, including those deployed remotely to support telework, can be monitored and managed from a single pane of glass. From a FortiGate NGFW or a FortiManager centralized management platform deployed at the headquarters environment, the security team can achieve full visibility into all connected devices, regardless of their deployment situation.

In the event of a natural disaster or other event that disrupts normal business operations, an organization must be capable of rapidly transitioning to a fully remote workforce.

Beyond offering encryption of data in transit, via a VPN, Fortinet solutions offer a number of other **features that can help an organization to**

secure its remote workforce. These features include:

- **Multifactor authentication.** FortiToken and FortiAuthenticator enable dual factor authentication of remote employees.
- **Data loss prevention (DLP).** FortiGate and FortiWiFi provide DLP functionality for remote workers, which is essential for teleworking executives with frequent access to sensitive company data.
- **Advanced threat protection.** FortiSandbox offers analysis of malware and other suspicious content within a sandboxed environment before it reaches its destination.
- **Wireless connectivity.** FortiAPs provide secure wireless access at remote work locations with full integration and configuration management in a single pane of glass.

A Secure Foundation Ensures Business Continuity

Preparing for business continuity and disaster recovery is vital for any organization. **An important component of this is the ability to support a mostly or fully remote workforce with little or no notice.**

When developing business continuity plans, it is essential to ensure that the organization has the resources in place to secure this remote workforce. Fortinet solutions are easily deployable and configurable and enable an organization to maintain full security, visibility, and control regardless of their deployment environment.

Learn how Montra Solutions enables Secure Remote Work:

Click to Contact Montra

montra.io/contact-us/