EXCLUSIVE NETWORKS

BUSINESS CONTINUITY SECURITY E-GUIDE

exabeam F5 FORTINET Infoblox Mellanox NOZOMI NETWORKS

NUTANIX paloalto proofpoint rubrik SentinelOne THALES

EXCLUSIVE NETWORKS

THE 'EXCLUSIVE' WAY FORWARD

Given recent events, there has been an imposed shift to working from home, requiring business across the globe to reassess their readiness with the necessary technology and solutions, not just for the short term but potentially irreversibly changing working habits as we move forward.

This has led to companies offering employees remote access to core business appllications and data, on any device on any site. However, today is more than just having remote access. Organizations are gradually focusing on making the journey from remote functions to the next level of advanced analytics, smart network, resilient security and business longevity all accessible from anywhere at any time.

The increase in remote digital workspaces has brought technological and managerial challenges to the forefront, compelling businesses to establish clear processes and stringent security controls. Even those organizations who have successfully mastered modern remote work regimes, are also constantly in pursuit of advanced solutions to boost productivity and ensure business continuity.

As a global cyber and cloud specialist, Exclusive Networks is primed to facilitate and empower businesses with smart digital solutions, going beyond the phase of just securing remote accesses. Always seeking to disrupt the norm, we offer an end-to-end solutions portfolio to support an organization's complete remote work lifecycle, right from setting up digital workspaces and enabling the workforce to provide advanced data analytical tools to guarantee business stability.

In the E-guide we will take you on a journey from initial setup of your remote access needs, all the way trough the augmentation and enhancements to security and user experience our smart solutions can make. Finally, we look at how smarter infrastructre decisions can complete your journey to Robust Secure and Available Networks.

GEARING UP FOR REMOTE ACCESS

F5 FORTINET NUTANIX paloalto THALES

YOUR'E REMOTE. WHAT'S NEXT

exabeam Infoblox proofpoint rubrik SentinelOne

SMARTER INFRASTRUCTURE CONSIDERATIONS

Mellanox NOZOMI NETWORKS

EXCLUSIVE'S WORK FROM HOME SOLUTION | VIRTUAL LEARNING

SCALING CAPACITY FOR REMOTE ACCESS AND SERVICE AVAILABILITY

To ensure your business continues to run smoothly during this crisis, consider the following solutions that support remote access capacity and service availability.

With so many employees working from home, many customers are struggling with capacity to enable secure remote access capabilities. F5's remote access management solution, F5 BIG-IP Access Policy Manager (APM) enables remote access (SSL VPN) amongst more capabilities, to simplify and secure access to applications.

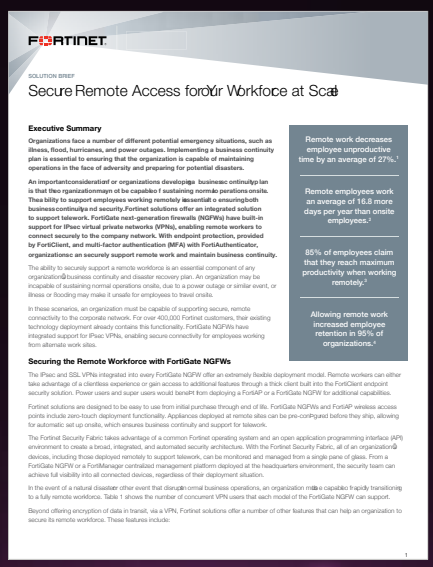
Some organizations are facing significantly higher load on their websites and applications, and are having difficulty operating at scale. To address scalability, F5 has two load balancing solutions: For F5 BIG-IP customers BIG-IP Local Traffic Manager keeps your web sites and apps available and secure; intelligently balancing, delivering, and managing network traffic.

If you don't have a BIG-IP solution, consider NGINX Plus for supported software-based load balancing — a quick and easy way to protect web applications under high load.

SECURE REMOTE ACCESS FOR YOUR WORKFORCE AT SCALE

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.

- Fortinet Teleworker Solutions to securely support remote workforces
- Organizations can leverage their existing FortiGate investments to quickly meet unexpected demand
- Security teams can easily support different categories of access for basic, power and super users


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.

Remote work decreases employee unproductive time by an average of 27%.[1]

Remote employees work an average of 16.8 more days per year than onsite employees.[2]

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

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

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.

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 other event that disrupts normal business operations, an organization must be capable of rapidly transitioning to a fully remote workforce. Table 1 shows the number of concurrent VPN users that each model of the FortiGate NGFW can support.

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:

FACILITATE 'DIGITAL WORKSPACES AS A SERVICE'

NUTANIX
YOUR ENTERPRISE CLOUD

The digital workspace is spearheaded by technology and innovation that enables end-users to access services, tools, and applications from any connected device regardless of their location. Create your digital workspace faster and deliver your end-user's applications and desktop virtualization as a service with more ease and reliability using Nutanix Frame.

paloalto NETWORKS

RAPIDLY SCALE SECURE REMOTE ACCESS

Capacity is key as you plan to onboard large numbers of employees to work remotely with uninterrupted access and a seamless user experience. Palo Alto Networks' award-winning security with multiple deployment options allows you to securely enable your remote workforce at scale. Prisma Access is a Secure Access Service Edge (SASE) solution for securely connecting users anywhere they are, to applications and services everywhere, including the cloud (public and private), SaaS, your data centre and the Internet. Prisma Access is delivered as a cloud service, which is capable of inspecting traffic on all ports and protocols.

THALES

EMPOWER EMPLOYEES TO WORK REMOTELY, SECURELY

Our daily lives have changed considerably in the last decade. The ability to work whenever and wherever employees want, has driven a fundamental change in working practices. Ensuring secure and easy access to corporate resources from remote locations is imperative to achieving this goal.

SafeNet Trusted Access, a strong authentication and access management service from Thales, enables your employees to log into the corporate network and applications easily and securely with minimal disruption to your business.

- THALES Cloud/ On Premises based service means you can get up and running within in a day
- Offer your employees a choice of tokenless authentication methods including Push OTP, SMS, or email
- Ensure secure access to VPNs, remote desktops, virtual environments and cloud-based services such as SFDC and O365

YOUR'E REMOTE. WHAT'S NEXT?

BEHAVIOURAL ANALYTICS IN ACTION

exabeam

What happens after our users connect to VPN? Are their activities within their usual scope? Are we able to identify if someone have their credentials stolen? With Remote Access becoming a business necessity, traditional cyberattacks such as phishing scams risk having a much bigger impact on organizations, especially attacks aiming at stealing credentials.

Today, attackers having a pair of valid credentials have almost guaranteed remote access, and with everyone working remotely, it serves them well to hide among the crowd and go unnoticed.

One of the main goals of Exabeam Advanced Analytics (UEBA) is to understand a user's normal behavior. Using Machine Learning and Data Modeling, any activity unusual to the user's baseline is easily surfaced as an anomaly, and therefore detected at very early stages of the attack kill chain.

In addition, Exabeam's Smart Timelines help give us complete visibility on all activities done by a user, in a form of time based narrative, regardless of where they did the activity (On prem, Remote, Cloud), which optimizes the investigation around abnormal behavior drastically by automating it.

What are you doing today to fight against the risk of compromised credentials?

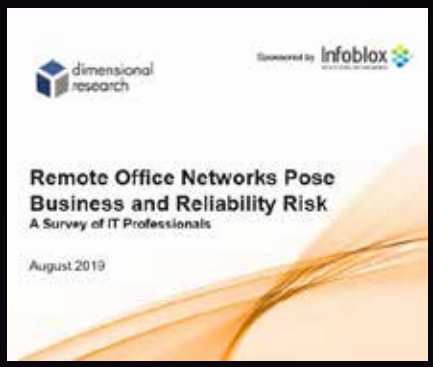
YOUR'E REMOTE. WHAT'S NEXT?

BUILDING RELIABLE REMOTE OFFICE NETWORKS

Infoblox
CONTROL YOUR NETWORK

According to a research report from Dimensional Research, sponsored by Infobox, nearly every company suffers direct business impact from network service interruptions. Three out of four companies surveyed experience network outages several times a year or even more frequently. Nearly half of the companies stated they need three or more hours to resolve an outage. Today more than nine out of ten companies manage their network operations centrally. But network professionals cite the top challenges of distributed network management is lack of on-site personnel and difficulty managing remote locations.

This report reveals that more than 7 out of 10 companies will be utilizing SD-WAN, with broad deployments covering not only remote locations, but corporate offices, and data centers as well as connectivity between them. The move to SD-WAN is driven by the need for increased operational flexibility and efficiencies. It appears that current centralized operational models today are delivering substandard network reliability, but the adoption of SD-WAN will enable new operational models and provide answers to current reliability challenges.



proofpoint.

ENSURING EMAIL CONTINUITY FOR CRITICAL BUSINESS SITUATIONS

Email is essential for business. Traditional approaches to email continuity, designed to ensure high availability with on-premise email deployments, have proven costly and ineffective and left organizations with continued outages. Enterprises are consequently moving to purely cloud based email services — both multi and single-tenant — at a rapid pace. These services offer multiple Service Level Agreements, yet are still subject to costly outages. Proofpoint Enterprise Continuity, addresses the above issues by providing an always-on insurance policy for crucial business communications. This enables users to continue sending and receiving email in the event of an outage without requiring any action from end users or IT.

rubrik

Avoid Ransomware Disasters with a Better Backup and Recovery Strategy

BE PRO ACTIVE, NOT REACTIVE

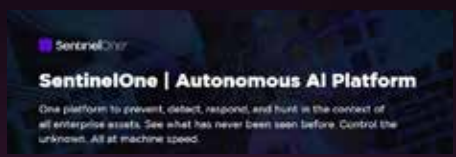
With many organisations believing that their anti-virus software will not block the threats they are facing and Ransomware attacks growing more than 350% annually, Paying a ransom should not be an organisation's only option following a ransomware attack. Recovery is complex and time-consuming, and in many cases, the backups themselves are encrypted or deleted, but with a strong remediation plan, businesses can recover quickly without paying extortionists.

Fortunately, Rubrik provides instant recovery from immutable backups that cannot be compromised. Rubrik also minimises data loss by providing visibility into exactly what was infected.

PROTECT ENDPOINTS FROM ALL THREAT VECTORSE

Pandemics such as COVID-19 provide 'bad actors' with the opportunity to take advantage of the situation; spreading malware, launching phishing and spear-phishing campaigns, and committing fraud through the exploitation of human emotion. With your most sensitive data living on the endpoint and within the cloud, it is vital that you confront the entire threat lifecycle to thwart the impact of attacks on endpoints. The SentinelOne platform delivers the defences you need to prevent, detect, and undo-known and unknown-threats.

SentinelOne™



SMARTER INFRASTRUCTURE CONSIDERATIONS

SMARTER EDGE COMPUTING NEEDS A SMARTER NETWORK

Mellanox TECHNOLOGIES

The most important factor of e-commerce applications is response time, and the best way to get your application speed up is to let the CPU run the application and not manage the network. Mellanox Smart Switches and SmartNICs are the best solution to offload the CPU from transport and communication missions so it can concentrate on running money-making applications.

Mellanox Smart Switches and SmartNICs defeat the deadly deal silent killer. Protect yourself, your data center, and your revenues with our revolutionary offerings – to ensure your compute resources aren't consumed on network tasks and instead stay working on closing deals and increasing revenues.

NOZOMI NETWORKS

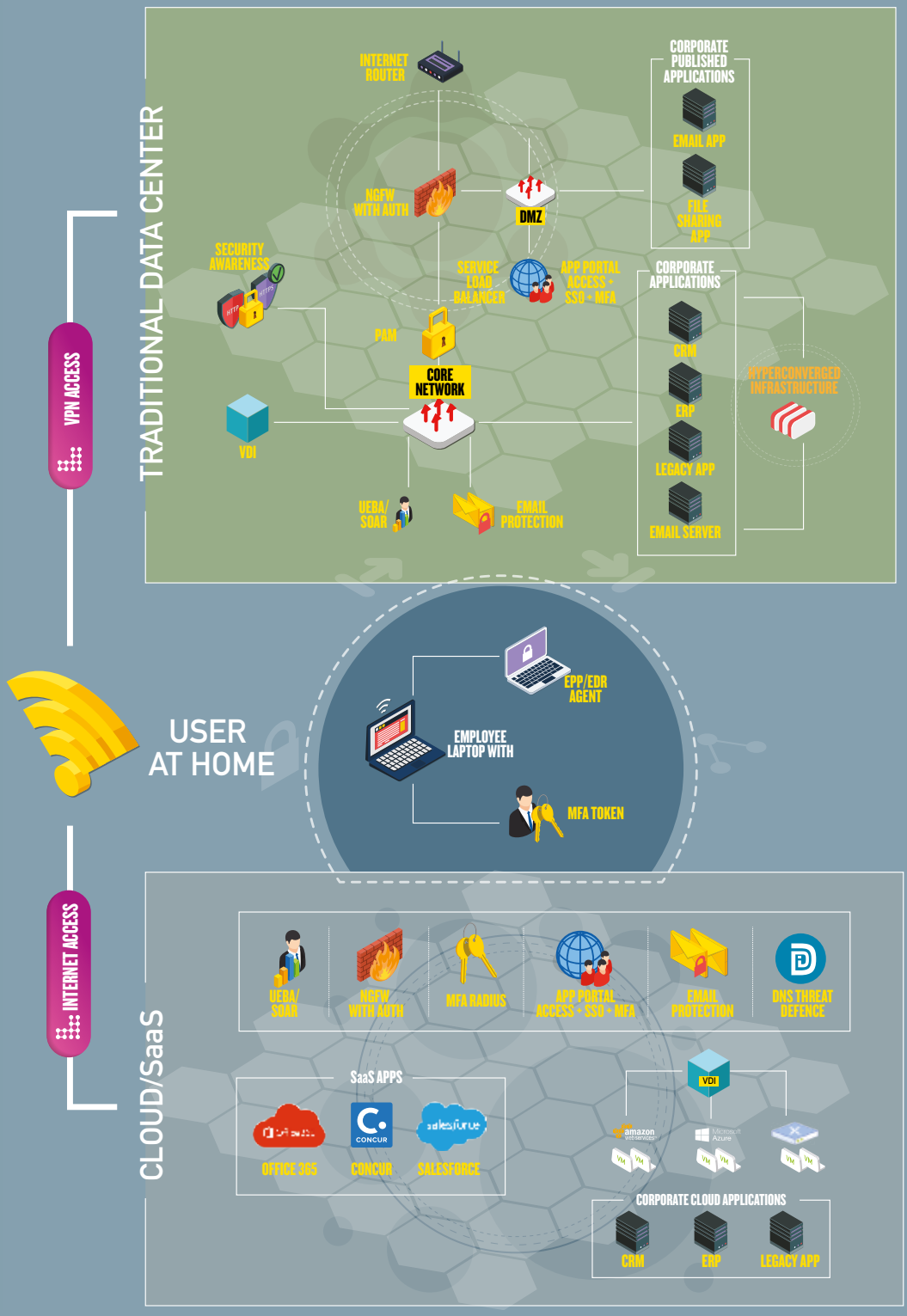
CHOOSE INDUSTRIAL STRENGTH MONITORING & THREAT DETECTION

Whether you're in oil & gas, power, manufacturing, retail, hospitality, transportation, utilities or another industry, creating an accurate asset inventory is key to securing your business and avoiding disruption to you and your customers.

The Nozomi Networks solution provides comprehensive visibility into your industrial network and IOT assets without creating any complexity. It helps you manage and monitor your assets in a highly efficient way, identifying risks to reliability and making it easy to troubleshoot problems. Device visibility is a key foundation for improving cyber security.

Nozomi Networks delivers both cybersecurity and process anomaly detection along with industrial & IOT network visualization and monitoring, asset inventory, and vulnerability assessment. As an organization, you can benefit from enhanced cybersecurity and improved operational reliability with one end-to-end solution.

EXCLUSIVE'S WORK FROM HOME SOLUTIONS



VIRTUAL LEARNING

We've all heard about the growing skills gap in the cybersecurity industry. There is an alarming number of businesses across the Middle East that lack staff with the technical, incident response and governance skills needed to manage their cybersecurity effectively.

And right now, this challenge is exacerbated by the current situation as companies scramble to set up or scale up remote working capabilities.

What is a skills gap?
A skills gap is different to a skills shortage. Rather than a shortfall in the number of skilled individuals working in or applying for cyber roles, a skills gap means that people are filling these roles – but don't have all the skills necessary to keep their business secure.

What can you do about it?
You can never know too much. Training is an invaluable resource that every business should take advantage of if it is available to them. Investing in training can help individuals to make the most of their security solutions and change their businesses for the better. You can start to close the skills gap within your organisation by using any downtime for your staff to get trained up to support existing teams struggling to cope, and to help ensure that going forward, you have a fully qualified workforce ready to quickly implement your business continuity strategy.

FIND OUT MORE about our virtual training sessions by contacting us at marketing@exclusive-networks.com