Let's Keep Things Moving: Business Continuity With BlueFort and RSA.

BlueFort Security | RSA

The big picture

If there's one thing that is abundantly clear for businesses, it's the need to be able to quickly adapt in order to let staff be productive from remote working environments.

Remote working isn't a new concept. In fact, it's been a growing trend for the last decade. So, when considering business continuity, endeavor to make longer term solution investments that will provide future ROI.

Here are a few considerations on how your business might implement a robust remote working set up.

Key considerations

1. Have a plan and make sure that everyone knows what to expect. Clear communications with staff letting them know what they should and shouldn't expect are key.
2. Prioritise. Make sure that business critical apps are available to the most important users with the minimum delay. Ancillary applications can be restored later.
3. What about legacy applications? Do you need to deploy a remote desktop solution for them?
4. Is your remote access solution resilient enough to deal with a spike in users?
5. It is easy to onboard new users? How will you let them know what to do?
6. Is it secure enough? Are the protections for users, data and applications still robust?
7. Could you scale up or down to meet demand or will you need additional bandwidth or licenses to do so?
8. Do users require other equipment such as monitors, printers or other peripheral devices at home

BlueFort Security | RSA

Focus on secure, convenient and reliable remote working

What is remote working?

Ultimately, remote working allows staff to carry out their roles away from the office and allows them to access the key tools that they require to do so. These tools could range from things like devices, data and applications, telephony and communications systems.

There are three key objectives for any remote working solution, these are:

Secure access

Convenient access

Reliable access

In today's computing environment, with applications and data typically provided by a mix of on-promise and cloud resources, the concept of remote access has changed. For many cloud-based applications, the key components should already be in place and battle tested by 'business as usual' operations.

For on-premise applications the situation is usually more nuanced. Typically, an organisation will have some on-premise applications that are already served by a VPN for regular remote working. In a Business Continuity scenario this needs to scale at speed – taking in new use cases, new user communities and new applications.

The good news is that there are many virtual appliance VPN's available. These can be rapidly deployed to reliably scale access and securely to your users.

BlueFort Security | RSA

Seamless to the user

When working remotely users expect to carry out their roles as usual, with minimum disruption or inconvenience. Ideally, access to apps, files and systems stay consistent.

A hotspot for this is authentication. Most applications come with a basic two factor authentication (2FA) option as standard. For office-based users, they probably only ever use a standard username and password. But, for remote access, this is simply not secure enough.

Best practice authentication solution takes into account factors above and beyond ‘do they have the right credentials?’ Modern MFA solutions consider a whole host of variable factors; how you log on, where from, what you are accessing, time, device used… and so on. This is much more difficult for hackers to imitate in order to gain access to your network and is also less intrusive to the user.

Once the user has been authenticated it’s then possible to quickly sign them onto the other applications with no further action from the user themselves. This Single Sign-On works across cloud, hybrid and VPN access to on-premise access. Not only does it simplify the user experience, it means less calls to the helpdesk and vastly improved security too.

BlueFort Security | RSA

IT friendly deployment

In the event that a user requires remote access, IT would typically onboard an individual on to the remote access system manually. These processes are rarely scalable during a business disruption.

When large numbers of users are asked to work remotely, IT staff – who themselves may not be able to make it into the office – must scramble to support these users. Essentially creating a ‘crisis within a crisis’.

We advise that you scrutinise the practicalities of a deployment and of a business continuity scale up. Would your situation rely on hardware? Is significant admin involved? Will you receive technical external support? All important questions to consider.

BlueFort Security | RSA

Avoid unnecessary costs

One of the limitations of scaling remote access solutions is that they are typically licence based or have capped user allowance.

Check to see if your remote access solution has a business continuity plan, reasonable use policy or add-on which would allow you to temporarily flex user count to accommodate a spike.

BlueFort Security | RSA

Solution spotlight:

One solution that's proven to be very popular with our client base is the Business Continuity Add-on for RSA SecurID users.

Benefits include:

Flexible licences that can be activated 6 times for 60 days – valid for 3 years

Rapid deployment; you just need email address and phone number of the new users

Familiar; Management from the same place that you would manage existing SecurID user accounts

Self-isolation friendly; No hardware is required, and no software needs to be installed on the user's mobile phone device or PC

An investment; these licenses can be used for any future unprecedented disruptions or if you have natural user spikes in your business. Many businesses have times when they rely on remote or temporary workforce – and these tokens can be used then (rather than activating a full license of SecurID for those individuals).

Find out more here.

BlueFort Security | RSA

Accelerate deployment:

Rollouts and scale ups of remote access solutions are often time critical. If you don't have the time or inhouse expertise to focus on the rollout then outsourcing is a great way of achieving rapid deployment.

If you choose to outsource, be sure that they are familiar with and accredited to work on the chosen technology solution.

If you're in need of a quick, effective solution to scale up your remote access authentication, network bandwidth or security management, please get in touch. We'd be delighted to discuss how we could be of help.

Contact us:

Phone: **01252 917000**

Email: **enquiries@bluefort.com**

Website: **bluefort.com**

Connect Follow us

BlueFort Security | RSA