EBOOK

TRANSFORMING A CRISIS INTO AN OPPORTUNITY

Introduction

Transforming a Crisis Into an Opportunity

The world is battling a crippling crisis today. The global economy is in peril and businesses have taken radical measures to mitigate the adverse impacts of economic decline. Companies have had to leverage the technology at their disposal to allow their employees to work remotely. Although technology has made remote work feasible, the unexpected magnitude of the situation has caught most small and midsize businesses off guard.

One of the challenges most companies face right now is ensuring business continuity with minimal loss of productivity of their remote workforce. While this unprecedented crisis has certainly transformed the way businesses around the world operate, it has also provided companies with an opportunity to reinforce their IT infrastructure to efficiently deal with the current situation and similar situations in the future.

Having a Business Continuity Plan Is Critical

As much as we would like to believe otherwise, no business is immune to disaster. Regardless of their size, companies need to be well prepared to ensure seamless continuity of critical operations in the face of unforeseen crises. The ultimate goal for businesses should be to minimize downtime. This includes the ability to maintain workforce productivity during an emergency, regardless of whether their employees are working remotely or in the office. It is imperative for businesses to have solid business continuity plans (BCPs) in place.

Not having a BCP as a part of your crisis management plan can be detrimental to your business. With a robust BCP in place, business leaders can respond swiftly and effectively to any contingency without negatively impacting customer confidence, profitability or brand reputation. Regardless of the size and nature of your business, a BCP can help prevent financial losses and maintain the stability of your business during tough times.

What Does a Business Continuity Plan Typically Include?

A BCP offers a set of guidelines that should be followed in order to maintain all critical functions of the business, should an unexpected crisis hit. BCPs focus not only on technical operations (hardware/software issues) but also take into account personnel when considering business continuity.

Designing an effective BCP consists of five stages:

Determining the potential risks:

The first step towards developing an effective BCP is defining the potential risks and threats that could disrupt your business operations. You need to consider all types of risks ranging from natural disasters, to human and even technical threats.

Defining the effect of those threats:

Once you have determined the potential risks, you need to identify the ones that are likely to have the most damaging effects on your business.

Developing your BCP:

This is the stage at which you need to draft the actual business continuity plan, complete with ways to mitigate disruptions caused by a crisis, recover from a disaster and identify the resources that will be required to protect your business (including your staff and assets) from further compromise.

Executing your BCP:

Once you have finalized your business continuity plan, you must share it with all your employees and key stakeholders and get their feedback on the guidelines included in the plan.

Review periodically:

It is essential to review your BCP periodically and make sure that it remains up to date and relevant. You can update the plan as and when necessary.

Components of a BCP

Team — The first and one of the most important components of creating a BCP is organizing a continuity team. Your BCP will be effective only if it is well-designed and if there is a dedicated team to execute it at a moment's notice. The continuity team will not only carry out the BCP in the event of a crisis but will also ensure that your other employees are also well aware of the plan.

Objectives — A critical aspect of a BCP is identifying potential threats to your business and then determining the objectives of having a BCP in place. In other words, you must outline the purpose of your BCP and how it can help you sustain your business when hit by a crisis.

BIA — You should run a Business Impact Analysis (BIA) in order to determine how losing various business units, processes and functions during a disaster is likely to impact your business. BIA helps in determining the individual financial impacts of different business operations and identifying the most critical functions that you need to protect and restore.

BDR — Have a solid backup and disaster recovery plan (BDR) as a part of your business continuity planning. We will discuss more on this below.

Testing Plan — Another critical aspect of a BCP is testing to ensure that you have identified any weaknesses in the plan before it is put to use in an actual crisis. The best way to discover any flaws or gaps is to test the plan in hypothetical crisis scenarios. Testing the BCP also involves determining how well the business continuity team is able to manage various disaster situations. You can correct weaknesses before the BCP is used in a real disaster. Along with frequent testing, it's also important to keep the BCP up to date with new developments in your business.

Information Checklist — Your BCP should have an information checklist that specifies how your employees can interact with one another during a crisis. The checklist should include a list of resources the business continuity team might need, details of the location where the backup data is stored and the emergency contact details of the management team.

In a nutshell, a solid BCP must have contingency plans in place to deal with all the different aspects of running a business that might take a hit during a crisis.

Backup and Disaster Recovery Plan

When hit by a crisis, the last thing you should be worrying about are your backup systems. Your backup systems should provide reliable, enterprise-class business continuity and disaster recovery (BCDR). Focus on reducing downtime with instant recovery, ransomware detection and automated disaster recovery testing.

Many organizations are now using a number of different Software as a Service (SaaS) applications, such as Microsoft Office 365, Google G Suite and Salesforce, to enable a more mobile and distributed workforce. With this shift to SaaS applications comes the need to have a backup solution that will protect all of your SaaS app data. A loss of this data could really slow down your business at a time when efficiency and productivity are more critical than ever. As such, it is imperative to back up your SaaS data to keep it protected against malicious attacks during a crisis.

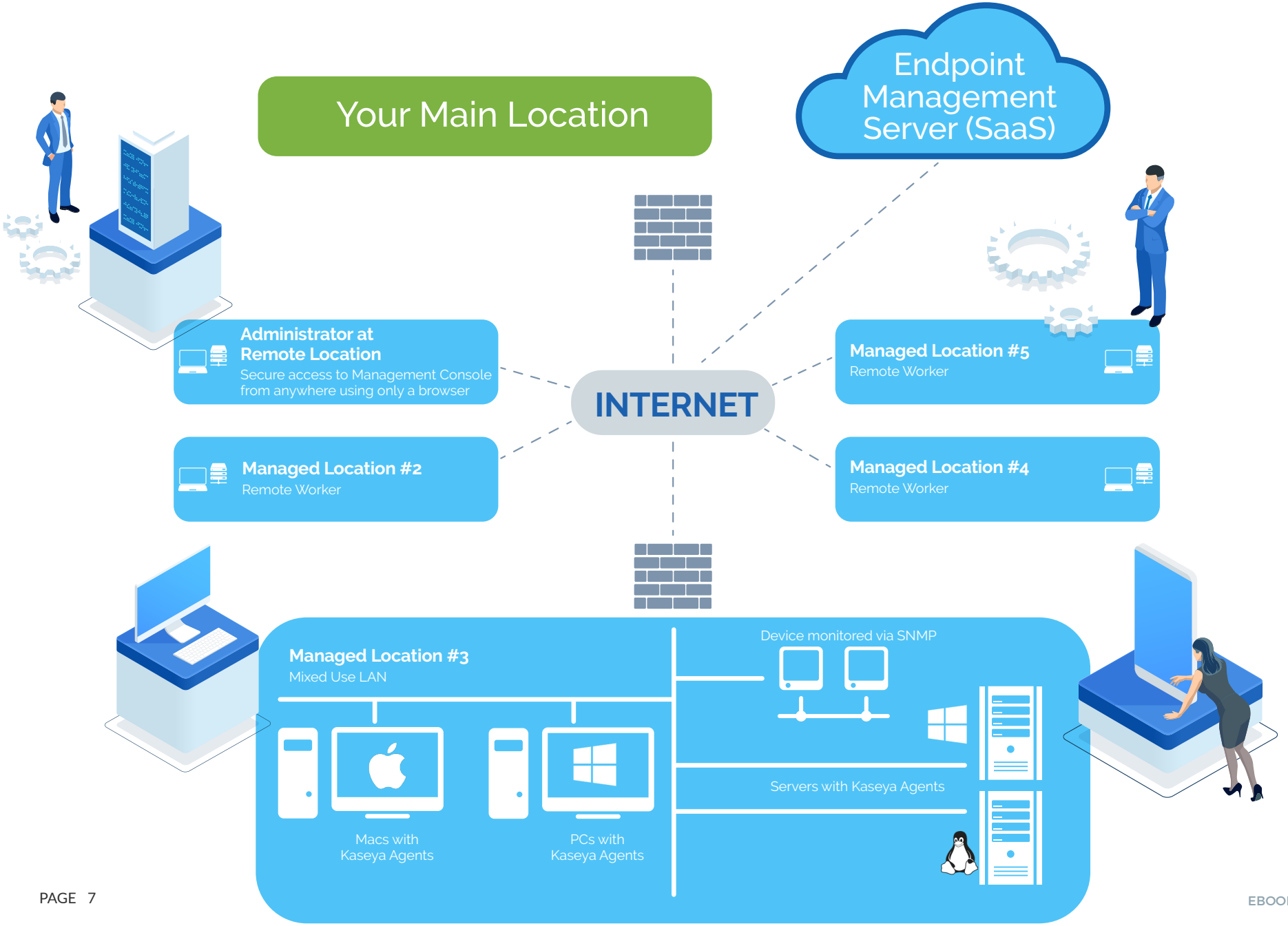
An appliance-based DRaaS solution can be integrated into your endpoint management tool, allowing you to manage backups from the same console. Meet the backup demands of the business with a backup solution that will ensure your business data remains safe from any unexpected incidents of data loss or downtime.

Built into Kaseya VSA, a powerful endpoint management solution, Kaseya Unified Backup offers you reliable backup services for your business that you can manage from a single pane of glass. This appliance-based solution enables instant recovery of your backed-up data and minimizes downtime so that you can quickly get back on your feet after a crisis.

Managing Remote Worker IT Environments

What we learned from the current pandemic is that we must be prepared to institute remote work policies on short notice. A robust BCP should include an IT management solution that ensures smooth operations in case employees have to abruptly switch to remote work. The right remote management and monitoring (RMM) solution will help you efficiently manage the remote devices of your users that are working from home.

Your endpoint management solution should provide remote monitoring and remote control of remote and off-network endpoints. This way, your IT team can easily and efficiently access any of these endpoints to troubleshoot issues and maintain system uptime for your employees and, in the case of MSPs, your clients.


Your Main Location
Endpoint Management Server (SaaS)
Administrator at Remote Location
Secure access to Management Console from anywhere using only a browser
INTERNET
Managed Location #5
Remote Worker
Managed Location #2
Remote Worker
Managed Location #4
Remote Worker
Managed Location #3
Mixed Use LAN
Device monitored via SNMP
Servers with Kaseya Agents
Macs with Kaseya Agents
PCs with Kaseya Agents

Endpoint management tools can provide access to these devices without interrupting the user so that the IT technicians can work behind the scenes. This keeps employee productivity high while allowing the IT team to resolve issues quickly.

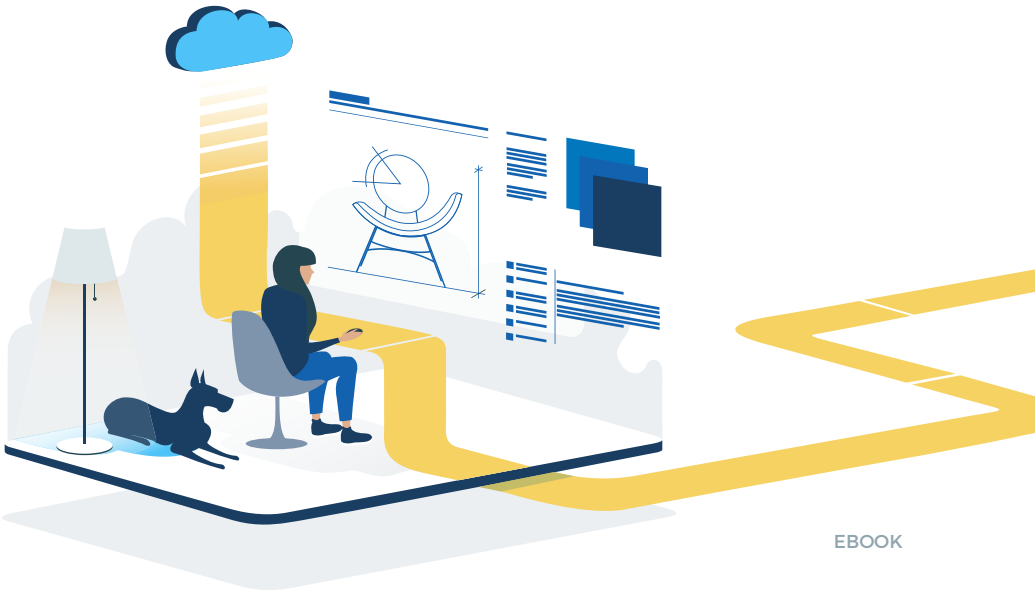
The remote access feature can also be used to allow remote workers to securely access their office-based computers from their home office, especially in cases where some computers may not be allowed to go offsite.

Remote access is a powerful feature that allows employees to access their work computers and continue to work productively if they need to abruptly transition to remote work. This means that even if your entire team suddenly needs to start working from home, your business operations can continue uninterrupted during an unexpected crisis.

Ensuring Security of Remote Workers

During any crisis, such as the current pandemic, cybercriminals work overtime to exploit vulnerabilities that can expose your business to potential cyberattacks. With the lines between working from the office and working from home blurring, prioritizing the security assessment of your systems and networks should be your main focus. Implement Dark Web monitoring to know when employee login credentials have been compromised.

In addition to this, it's important to provide extensive security training to your workforce to ensure that they follow the best practices required to keep your systems protected against cyberattacks. This will help in reducing the risks of ransomware and other cyberattacks that can be extremely costly for small and midsize businesses. Also, consider using Single Sign-on (SSO) and 2-Factor Authentication (2FA) as a general practice to ensure that logins are more secure, regardless of whether employees are working from the office or their homes.



Kaseya VSA — An Intelligent Solution to Better Manage Your Business During a Crisis

Kaseya VSA is a Remote Monitoring and Management (RMM) solution that is designed to support smooth business operations even in the event of an unforeseen crisis. Whether you are looking to provide your internal IT team with complete visibility and control of end-user devices, or you want to ensure top-notch IT service delivery for your MSP clients, Kaseya VSA streamlines your routine IT operations and minimizes disruptions for your remote workforce during a crisis.

It provides access to the powerful capabilities of remote endpoint monitoring and management, backup management, IT documentation and AV/AM solutions from a single pane of glass. It allows you to remotely access and troubleshoot end-user devices, enhance security and ensure greater technician efficiency. Kaseya VSA is a solution that will keep you well prepared should a crisis, such as the current pandemic, hit again in the future.

Some of the key defining features of Kaseya VSA that are extremely useful for managing a remote workforce during a crisis include:

- *Remote endpoint management with Kaseya Live Connect and Kaseya Remote Control*
- *Patch management of remote, off-network devices and deployment of AV/AM clients*
- *Employee activity monitoring*
- *Remote worker secure access to office-based computers*

VSA™ by Kaseya

SCHEDULE A DEMO

Learn how to ensure business continuity when faced with another crisis in the future. Schedule a demo of Kaseya VSA now!

Schedule a demo to learn how to ensure business continuity when faced with another crisis in the future.

About Kaseya

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

05262020