TANIUM™

Business Continuity Lessons From 2020

How Technology Leaders Maintained Visibility and Control When Their IT Networks Transformed Overnight

Table of Contents

3 Your New Mandate: Prepare for the Unpredictable

4 Why You Must Prepare for the Unpredictable

5 Lessons Learned From 2020

7 Five Steps to Better Business Continuity

10 How Tanium Can Help Prepare You for Anything

11 Be Ready for Whatever Comes Next

Your New Mandate: Prepare for the Unpredictable

2020 was the largest business continuity test in history. The world experienced a pandemic of unprecedented scope. Organizations were forced to send the majority of their workforce home.

And technology leaders guided their organizations through digital transformations that were much bigger and faster than they ever could have planned for.

Some organizations passed this test, and thrived during these events. Other organizations failed, and continue to struggle to this day.

But both groups learned the same hard lesson: Unpredictable events can occur and change everything overnight.

This eBook will help you better prepare your business to be agile and adaptable.

It extracts insights from those who struggled and those who thrived during the events of 2020 — and will teach you how to be **ready for whatever comes next.**

It will explore:

- How it is possible to prepare for the unpredictable, and why it's worth doing
- What steps you must take to prepare for the next big, unpredictable crisis
- How Tanium gives you the tools you need to be ready for whatever comes next

Why You Must Prepare for the Unpredictable

It sounds like an impossible task — to prepare for an unpredictable event. But 2020 proved that it's possible.

Some organizations and technology leaders were prepared despite the fact they never built a pandemic or lockdown into their business continuity planning.

"If you had asked me a year ago, I would have said there's absolutely no way something like this could happen," said Charles Ross, Chief Customer Officer at Tanium. "I would have considered the idea a far-fetched, made-for-a-movie event that is probably never going to happen in our lifetimes."

As the events proceeded, every organization and leader scrambled to respond.

"Every hour we'd be getting a new update," explained Ross. "One hour a business was up and running, and the next hour they were completely shutting down — everyone is going home, their systems are now moving with them — and this was happening every hour, around the clock."

Every one of these organizations knew that digital transformation and work-from-home (WFH) were the future. But no one thought it would happen so fast.

"You had a lot of people talking about migrating to the Cloud, but you see they have two, four, six-year plans to get there," explained Stephanie Aceves, Director of Technical Account Management at Tanium. "COVID-19 told them — very quickly — that is not viable."

Everyone had to move themselves and their clients through much bigger transformations than almost anyone had expected or built the infrastructure for.

"Many organizations I talked to had work-from-home policies and infrastructure to provide remote access," explained Jon Oltsik, Senior Principal Analyst and Fellow at the Enterprise Strategy Group. "The problem was, they had it for 40% to 50% of the workforce, not 80% to 90% of the workforce."

But not everyone had the same experience moving to distributed environments. Even though no one predicted these events, some were better prepared than others, and experienced a relatively easy time adapting to the demands of the moment.

"Those who were prepared knew how to predict what was coming next," explained Ross. "They were managing their businesses comfortably — even under very new sets of conditions."

But unprepared organizations were flying blind. They lost visibility into their endpoints. They lost the ability to perform basic security controls like patching. They lost the ability to use many of the legacy tools they depended on in the office.

> *"Many organizations had policies and infrastructure for supporting remote access. But they only had it for half their workforce, not 90 percent of their employees."*
>
> Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

"There are a lot of companies that are completely in the dark about how they are doing business," explained Ross. "They put on a tough face and say they've got this, but behind the scenes they are scared."

They don't know their risks. They don't know if they've been compromised. They don't even know if they're about to lose their business to malicious actors.

They paid the price for being unprepared for the unpredictable events of 2020 — and many of them continue to pay that price to this day. They haven't yet re-established fundamental visibility and control over their environments and remain at risk.

You don't want to be in this position. You don't want to pay this price. You must find a way to prepare for the unpredictable before the next big event happens. Here's how.

Lessons Learned From 2020

To produce this eBook, we spoke with multiple technology leaders who were prepared for the events of 2020 without predicting those events — and all of them shared a few traits that made them ready to respond to the moment.

First, they all had well-developed and well-tested business continuity plans.

Some of their plans included pandemics. Some of their plans included regional lockdown scenarios. But none of their plans included the breadth of 2020's crises.

"This kind of event happening is once in a lifetime," said Scott Lowe, Managing Director and Founder at EndpointX. "You can do as many DR tests as you'd like, but I bet none of them were 'Get 100% of your staff to work from home in five days.'"

But even though none of these leaders foresaw the scope of these events and their requirements, all of them had taken business continuity seriously pre-pandemic.

"I don't think any organization was truly and completely prepared for essentially all of their remote workforce to be working remotely," said Chris Hodson, Tanium. "But there are different ends of the spectrum for maturity for business continuity and technology architecture."

Those who were prepared had more mature plans than other organizations and — crucially — they had actually tested those plans. They had performed tabletop exercises and live drills of their continuity capabilities prior to the pandemic and knew they would hold up to the demands of the moment.

Second, they had already developed distributed endpoint capabilities.

When workers went home they brought their endpoints with them. They dissolved their on-premises environment, and created a new distributed world.

Unprepared organizations scrambled to adapt to these new distributed environments. But prepared organizations had already established the ability to maintain visibility and control over distributed environments — before they needed to.

"The foundational things that allowed us to work from home and support our employees through COVID were really in place beforehand," explained Mitch Teichman, Senior Manager of Client Engineering at VITAS Health. "The beauty of that was, when COVID happened and a lot of other companies were looking at various solutions, we didn't have to do anything different."

Teichman — and other prepared leaders — did not have to think about how they would operate and secure their new environments.

"Having that peace of mind — to not have to worry about visibility and control when we were scrambling and had to worry about so many other things — was tremendous for my team and the IT organization," Teichman elaborated.

Instead of worrying about the fundamentals, prepared technology leaders were able to focus all of their time and attention on the larger challenges of those early days.

"I can't imagine what it must have been like for organizations to not only struggle with 'How are we going to get everyone to work from home?' but, in addition, something as basic as 'How are we going to patch a distributed workforce?'" said Teichman.

Many unprepared leaders continue to struggle with these same basic tasks. But prepared leaders have maintained visibility and control over their new environments this entire time — all because they developed the capability to do so before they needed it.

Third, they leveraged the right technology tools

The prepared leaders we spoke to used different tools than the unprepared leaders.

Unprepared leaders leveraged legacy tools that were built for on-premises environments. These tools struggled to operate in the new distributed environment.

A lot of organizations have worked with N-tier systems architecture, and hub-and-spoke connectivity models, all of which are aligned with a working-in-an-office, connecting-in-an-office scenario," said Hodson. These tools were fragmented and narrowly focused, creating further problems.

"Many companies struggled with siloed, disparate solutions during the pandemic, '' explained Hodson. "From a security perspective, they had a different tool to handle each of their threats. When the pandemic struck, this created technology problems, cost problems, and people management problems as each tool had its own remote team managing it, exacerbating the issues inherent in working remotely."

> *"Many companies... had a different tool to handle each of their threats. When the pandemic struck, this created technology problems, cost problems, and people management problems."*
>
> Chris Hodson, Global CISO, Tanium

By contrast, prepared leaders used modern tools built for distributed environments.

"Having an effective endpoint management solution was really key," explained Ralph Loura, Chief Information Officer at Lumentum. "If you have thousands, or tens of thousands, of devices, you can't afford to have your team manually addressing each of these issues. You need a well-instrumented platform that you can use to run data collection and run execution and action on a wide range of devices across the globe."

Prepared leaders depended on these tools in 2020. These tools continued to work when their staff went home. These tools maintained visibility and control over their new environments.

These tools acted as the glue that held their business continuity plans together. In short, for prepared leaders, having the right tools made all of the difference.

Five Steps to Better Business Continuity

These lessons tell a simple story. You need to develop mature business continuity plans. At the same time, it is critical to establish comprehensive endpoint device management capabilities before you need them. Finally, make sure you use tools that can adapt as today's dynamic business networks evolve.

To help you bring these lessons to your organization, we have developed them into a simple five-step process you can follow to build better business continuity.

If you follow this process, you'll address any lingering continuity issues from the past year, and set your organization up to respond better to whatever comes next.

These five steps to better business continuity are:

Step One: Assess your business continuity gaps.

Step Two: Revisit — and test — your business continuity plans

Step Three: Re-establish visibility and control over your endpoints.

Step Four: Embrace distributed operating and security models.

Step Five: Re-evaluate your endpoint management and security tools

Step One: Assess your business continuity gaps.

Ask yourself a few questions to determine where your own business continuity plans didn't stand up to the events of 2020, and what might require adjustment:

- ✓ Did we experience significant downtime during our move to remote work?
- ✓ Did we have to compromise security to make our move happen?
- ✓ Did we maintain visibility and control over our endpoints?
- ✓ Did we scramble to replace our legacy tools with new remote solutions?
- ✓ Have we restored the capabilities we lost during our move?
- ✓ Would things be different if a new big, unpredictable event happened this year — or would we be in the same position as we were when 2020's events happened?

Step Two: Revisit your business continuity plans and test them.

Take your answers from step one. Use them to make a list of the gaps in your business continuity plan.

For each gap you identify, ask yourself:

- Why did we experience this gap?
- What capabilities must we develop to fill this gap?
- Once we develop those capabilities how can we test them to ensure we have solved this problem — before another big, unpredictable event occurs?

Step Three: Re-establish visibility and control over your endpoints.

Make re-establishing control over your endpoints your number one priority.

Even if you didn't fully lose visibility and control over your endpoints, take a moment to ensure you have developed these capabilities to a mature degree.

Ralph Loura — CIO of Lumentum — provides a practical guideline for how mature your endpoint visibility and control must be to maintain meaningful business continuity. To deploy mature endpoint visibility, you must meet these criteria.

"Having good endpoint edge intelligence is the key to everything else," explained Loura. "I need intelligence coming off every device, all the time — what's occurring on it, what may or may not have been deployed, and what activity is normal or abnormal that's occurring on the device — so I have the information I can use to make better decisions about how to proceed."

To deploy mature endpoint control, you must meet these criteria.

"I need to be able to touch every device on a moment's notice when I need to," explained Loura. "Being able to rapidly respond, isolate, and recover are key capabilities to prevent a minor issue from becoming a major issue — and ultimately potentially becoming a real significant issue in your environments."

If your endpoint visibility and control does not meet or exceed these criteria, determine what you must do to upgrade your capabilities — and do it.

Step Four: Embrace distributed operating and security models.

2020 made it clear: On-premises operating and security models break during crises, while distributed models can adapt in real-time to rapidly changing conditions.

"Those organizations that were more of an internet-first model — who were using distributed computing for a distributed workforce — had a head start, and had significantly less impact from a technology perspective," said Chris Hodson, CIO of Tanium.

With that in mind, look at your business continuity plans. Look at your plans to upgrade your endpoint visibility and control capabilities.

Ask yourself:

"Will I be able to execute these plans and perform these capabilities in fully distributed environments, or do they still assume some connection to an office and network?"

Make sure you can execute every element of your plan — and every facet of your visibility and control capabilities — no matter where your endpoints might live.

Step Five: Re-evaluate your endpoint management and security tools.

Finally, determine which tools to keep and which to replace.

To do so, follow this simple approach suggested by Charles Ross of Tanium.

"Take a step back. Take a hard look at the investments you've made. And make decisions, 'Are those giving me the value that I need to operate as an organization going forward?' Any tool that isn't providing value now is unlikely to do so in the future and now is the time to rationalize your environment."

> *Take a step back and make decisions about the IT and security investments you've made. Any tool that isn't providing good value now is unlikely to do so in the future. Plan accordingly.*
>
> Charles Ross, Chief Customer Officer, Tanium

To bring this approach to life, just make two lists. On the first list, put every tool that maintained its functionality. On the second list, put every tool that broke when your environment changed last year.

No need to complicate this exercise. Once you're done look at your two lists. Keep the tools that maintained their functionality, and plan to replace those that broke.

And if you need to replace any of your endpoint tools, consider Tanium.

How Tanium Can Help Prepare You for Anything

At Tanium, we didn't predict the events of 2020. But we did design our platform to prepare organizations for any event.

And over the course of the past year, a diverse range of organizations and technology leaders used Tanium to maintain business continuity at every step of their journey.

Here are a few examples:

- **Scott Lowe of EndpointX** used Tanium to move his large financial institution clients through their transformations. He was even in the middle of deploying Tanium for a large organization in the Nordics when they sent all of their staff home with two hours notice. Despite these challenges, Lowe and his teams used Tanium to help their clients transform in a fast, efficient manner.
- **Ralph Loura of Lumentum** upgraded his legacy on-premises tools with Tanium and other modern, distributed solutions a year before the pandemic struck. In 2020 he used Tanium to transition thousands of Lumentum staff — spread across 22 countries — to distributed operations without losing business continuity.
- **Stephanie Aceves of Tanium** directly helped many of our customers undergo the rapid transition to primarily WFH environments. Her customers used Tanium to quickly re-establish a baseline of visibility and control over their new environments. Having Tanium gave these organizations a head start and kept them ahead of the curve.

There are a few reasons why Tanium helped these leaders — and many more — maintain business continuity for themselves and their clients.

Tanium:

- Automatically scales and adapts to changes in endpoint environments without additional infrastructure, which enabled technology leaders to maintain visibility and control over their environments as they transformed overnight.
- Leverages distributed architecture that doesn't require significant bandwidth to operate, which enabled technology leaders to perform their endpoint management and security tasks without overloading the VPN.
- Can deploy new endpoint management and security capabilities in hours or days — not weeks or months — which enabled technology leaders to quickly spin up any new capabilities they needed at a moment's notice.
- Provides a unified platform for core endpoint management and security capabilities, which enabled technology leaders to do their jobs without worrying about unnecessary complexity, costs, or team management challenges.

While technology leaders used a wide range of Tanium's capabilities to maintain business continuity throughout the events of the past year, Tanium offers key platform services that provide a unified view and comprehensive control of your endpoint devices.

Asset Discovery and Inventory
Know what endpoints and applications are in the environment, even as the environment rapidly changes.

Patch and Software Management
Apply large-scale patches and software installations and updates to distributed endpoints in minutes or hours.

Vulnerability and Configuration Management
Find open vulnerabilities, breaks in compliance, and policy misconfigurations and remediate issues.

Incident Response
Leverage a comprehensive suite of unified capabilities to rapidly detect, investigate, and remediate incidents.

Be Ready for Whatever Comes Next

2020 has passed. But you aren't out of the woods yet. You must find a way to maintain continuity, all without knowing:

- When the current crises will end
- What the world will look like afterwards
- When the next big, unpredictable event might happen

We can't tell you the answer to these questions. But we can help you fill any gaps in continuity you opened in 2020, manage today's ongoing uncertainty, and — most important of all — **be ready for whatever comes next**.

To learn if Tanium can help you prepare for the unpredictable, reach out today. Take the appropriate next step to see if Tanium is the right platform to drive your ongoing business continuity requirements.

Schedule a free consultation and demo of Tanium.

Schedule Now

Let Tanium perform a thorough gap assessment of your current capabilities.

Get Gap Assessment

Launch Tanium with our cloud-based offering, Tanium as a Service.

Try Now

TANIUM.

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.