FROM CHAOS TO CLARITY TO CONTROL

Achieving Resilience in Your Distributed Workforce Environment During the COVID-19 Pandemic and Beyond

How organizations in the most demanding and complex environments are leveraging Tanium to build resilience, maintain business continuity, and manage their long-term risk for today, tomorrow, and the new normal.

TANIUM

Contents

Executive Summary

The COVID-19 pandemic has rapidly, and radically, transformed the way organizations work, necessitating a new approach to endpoint security and management.

Organizations in every industry have been forced to transition the majority of their workforce to remote Work From Home (WFH) arrangements. To accommodate this transformation, organizations have upended their traditional IT infrastructure and adopted decentralized networks, cloud-based services, and widespread usage of employees' personal devices.

Unfortunately, working within this new environment has revealed a hard truth: many organizations experience critical visibility gaps and operate from a lower maturity level in their endpoint security and response capabilities than they initially anticipated.

Taming the Distributed Workforce Environment

Lack of visibility and control has created significant challenges for many organizations. The sudden explosion of unprotected endpoints and an increase in conventional and pandemic-specific external cyber threats has meant that the workforce now has greater access to sensitive data, which is likely to result in fallible user error due to stressful conditions.

These are significant challenges which, if left unaddressed, can lead to organizations suffering serious security events, data breaches, and broken compliance with regulations such as GDPR and CCPA.

However, these challenges can be overcome. From our work supporting customers through these unprecedented times, we've helped to operationalize a practical, effective, and process-driven framework for addressing the significant challenges created by the pandemic.

This framework addresses challenges at multiple stages of crisis – in this case, pandemic response – and identifies how organizations can rapidly move through levels of operational maturity with speed and confidence:

Level 1—Develop Resilience
Immediate steps to stabilize the new operational environment.

Level 2—Recover Operations
Mid-term steps to achieve and maintain business continuity.

Level 3—Plan for the New Normal
Long-term steps to prepare for operations after the pandemic passes.

Within just a few weeks of the massive shift to a predominantly distributed workforce, Tanium helped dozens of customers quickly and efficiently progress through these three maturity levels and gain control of their environment.

Tanium Was Built for This

This paper was developed to crystalize the challenges you currently face, to provide a robust and practical framework for overcoming these challenges, and to outline the ways that Tanium has helped organizations like yours develop effective endpoint security and management practices during these troubled times.

Read on to find a detailed exploration of the specific Tanium capabilities that support our customers' efforts, as well as real-world case studies, that illustrate how quickly and completely organizations like yours can return to stable, secure work.

Our goal is to help you better understand how you can overcome the challenges being placed on you in times of crisis and change.

For immediate support, contact Tanium now to request a discovery session, to see Tanium live in a scheduled demo, or to launch an immediate deployment of our platform to your operating environment.

Endpoint Management and Security in the Age of COVID-19

Everything has changed.

The COVID-19 pandemic has disrupted day-to-day life, triggered global stay-at-home orders, and led to a series of restrictive recommendations from global health organizations, federal governments, and local municipalities.

In response, many organizations have been forced to temporarily close their offices and rapidly transition their operations into a work-from-home (WFH) or distributed workforce environment. This can put significant pressure on critical IT infrastructure and support teams, as few IT organizations are designed to support every employee working remotely.

For most organizations, this transition has upended their traditional IT networks and necessitated the rapid adoption of decentralized networks and cloud-based services. While this transformation has given organizations the tools to continue their operations, it has in turn, created significant new operational and security gaps.

As the world collectively takes on COVID-19, many organizations have enacted company-wide WFH policies to help slow the spread of the virus. For many organizations the sudden requirement to support a fully-remote workforce has amplified an uncomfortable reality: critical visibility gaps are everywhere, and they can seriously escalate cybersecurity risk.

Cybercriminals and advanced persistent threat (APT) groups were among the first to react to the spread of the pandemic, using classic social engineering techniques to spread business email compromise (BEC), ransomware, and traditional phishing scams. New Tanium research reveals that enterprises are now entering a new wave of home working threats driven by:

- An explosion in unprotected endpoints
- Stressors such as user error and shadow IT that expose assets to elevated cyber risk
- Compliance challenges

> “Running corporate applications in the uncontrolled and widely variable environment of end-user home networks presents unique challenges to I&O due to a lack of visibility and control over the environment.
>
> **Gartner**
> **"Use DEM to Understand and Enhance Your Employees' Work-From-Home Experience"**
> *Josh Chessman, et al, 22 April 2020*

Exacerbating these challenges today are:

More Endpoint Vulnerabilities

Remote workers often access cloud-based workflows and decentralized networks from unknown computing devices.

Even known devices are often operating with open vulnerabilities due to the effort or bandwidth required to connect them to a centralized patch management solution.

This lack of visibility into unprotected endpoints exposes organizations to many threats. It creates unknown vulnerabilities, makes risk assessments harder to perform, and increases the chances of remote employees suffering breaches.

More Sensitive Data Proliferation

Remote employees now have to store, shuttle, and work with a greater volume of sensitive data from their devices. This has created an increased risk of data spillage, where the wrong data ends up in the wrong location – either from personal devices spilling into the corporate network, or simply from spillage within the corporate network itself. At the same time, this proliferation of sensitive data has increased the chance of any compromised endpoint creating a significant compliance breach.

Both the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) allow regulators to levy major fines on organizations that are found to be substandard in how they process and secure personal information.

Global CIOs claim to have spent over $70 million on compliance over the past 12 months and an additional $185 million on cyber liability insurance in response.[1] Yet, visibility gaps continue to undermine such efforts. Over a third (37 percent) claim that a lack of endpoint visibility and control is the biggest barrier to maintaining compliance.[2]

> "More than 70 percent of IT leaders are finding unknown computing devices every day or week. It's impossible to protect what you can't see.
>
> Tanium Visibility Gap Study

More Employees Leveraging Personal Devices For Corporate Usage

The raft of personal devices that employees are now using to do their jobs from home is one of the biggest vulnerabilities in a company's network. While corporations

[1, 2, 3] Tanium Visibility Gap Study conducted by market research specialist Vanson Bourne

quickly shifted to accommodate remote work, few have incorporated employees' laptops, tablets, and mobile devices into their patch management programs, which could leave corporate data exposed.

Even the least sophisticated attack can take advantage of these unsecured endpoints and the apps that they run. For businesses to operate safely, they need clear oversight of all devices connected to their networks. However, many businesses still struggle with full visibility of corporate computing devices. Our latest research shows that more than 70 percent of IT leaders are finding unknown computing devices every day or week.[3] And it's impossible to protect what you can't see.

More External Threats and Attack Vectors

Finally, we have seen an increase in attacks and exploits from opportunistic malicious actors. The cybercrime economy is estimated to be worth $1.5 trillion annually[4], with the number of new security threats soaring at an alarming rate. In some cases, cybercriminals are deploying new, highly-targeted exploits to take advantage of specific applications, such as Zoom, that have been rapidly adopted during the recent rush to WFH operations. In many cases, these malicious actors are simply deploying standard threats, like phishing, in an increased volume to take advantage of the current chaos and lowered vigilance. Such threats are designed to deliver everything from ransomware to credential-harvesting and business email compromise.

According to Tanium data, the majority (53 percent) of IT leaders say that endpoint blind spots can leave them exposed to cyberattacks.[5]

While most organizations are aware of these threats, and are taking every internal action possible to address them, they find themselves challenged to adequately take control amidst the current chaos.

[3,5] Tanium Visibility Gap Study conducted by market research specialist Vanson Bourne

[4] Information Age

re·sil·ience
/rə'zilyəns/

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

National Institute of Standards and Technology

Why Internal Endpoint Management and Security Has Become Near-Impossible

Few organizations were prepared to adopt enterprise-wide WFH operations.

They had to make the transition at high speed, and have done their best to spin up new remote infrastructure, applications, and capabilities in a very short period of time. For the most part, organizations have been successful at doing so, and must be commended for the radical transformation they realized in a very short window.

Yet, this transition came at a cost.

The current requirements to accommodate a highly distributed workforce have placed tremendous strain on remote connectivity infrastructure and IT support staff.

The result? Organizations are contending with a range of challenges that prevent them from making endpoint management and security an internal priority.

Under these conditions, it is clear why front-line staff and management have lacked the resources and capacity to deliver effective endpoint management and security: they are overburdened simply attempting to maintain a normal working cadence.

A new approach is needed.

Priorities Competing With Endpoint Management and Security

Overwhelmed Staff

Internal IT and security staff are stressed, stretched thin, and some may get sick themselves.

Lack of Capacity

Many organizations are operating legacy VPNs that lack the licenses, updates, and features to support mass WFH.

Performance Failures

VPNs are "melting" under the dramatic increase in access volume, and challenged to handle outside-in data flows.

Unknown Risks

Because they lack visibility into their WFH operating environment, most organizations don't know what their risks are, or how to prioritize them.

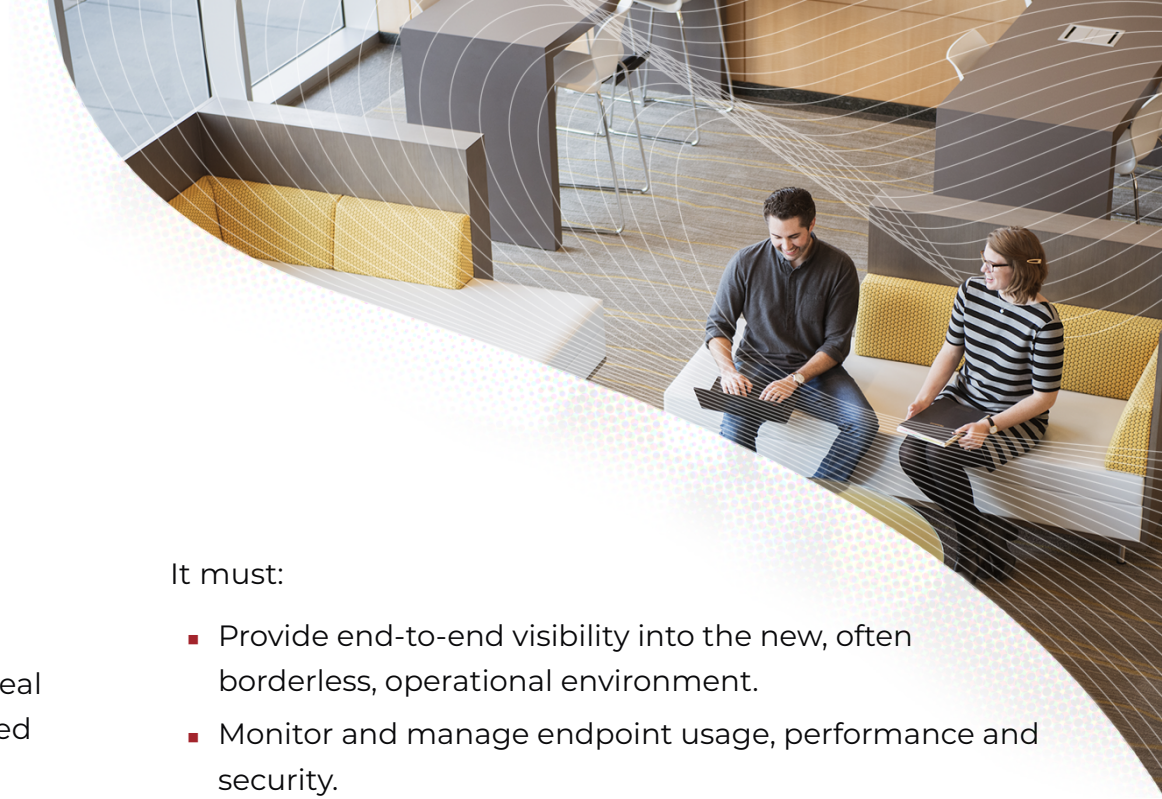
Missing Devices

In some organizations, corporate devices are being taken home without employees following appropriate protocols, or are being outright stolen.

"Open Doors"

Many devices used by WFH employees lack antivirus software, proper configurations, and alignment to risk management frameworks which includes patching.

Solving the Endpoint Management and Security Challenge: A New Framework



The current crisis and demand for a predominantly distributed workforce is a new systemic challenge for organizations. The challenge can't be resolved by piecemeal solutions, by following policies and procedures that worked in the past, or by asking overstretched internal teams to simply do more.

Our current context requires a radical rethinking of how customers manage and secure operational environments. It also necessitates the application of a practical, process-oriented framework that is tailor-made to move their organizations through this crisis, and beyond.

After a few weeks of helping our clients effectively manage this crisis, we've identified the significant problems this framework must address.

It must:

- Provide end-to-end visibility into the new, often borderless, operational environment.
- Monitor and manage endpoint usage, performance and security.
- Monitor and manage distributed workforce infrastructure and software deployments.
- Continue to manage existing centralized infrastructure.
- Help enforce policy and maintain fundamental IT hygiene.

Though this is an evolving project, the three-level framework has delivered meaningful outcomes for our clients as they have sought to gain visibility and control over their new operating environment.

A Framework to Gain Visibility and Control Over the Distributed Workforce Operating Environment

LEVEL 1
Develop Resilience

It is imperative that you stabilize your current situation, and ensure you can withstand the daily pressures and threats created by your new distributed workforce operational environment.

To begin, consider a few questions:

- How can I adapt my existing operations and security processes to deliver outcomes in a distributed workforce environment?
- How can I accelerate my time to detect and respond to a breach of one or more of my endpoints?
- How can I create more effective working relationships between my IT operations and security teams?

LEVEL 2
Recover Operations

Once your environment is stable, you must achieve and maintain business continuity to allow operations to function as normally as possible for the remainder of this crisis.

To begin, consider a few questions:

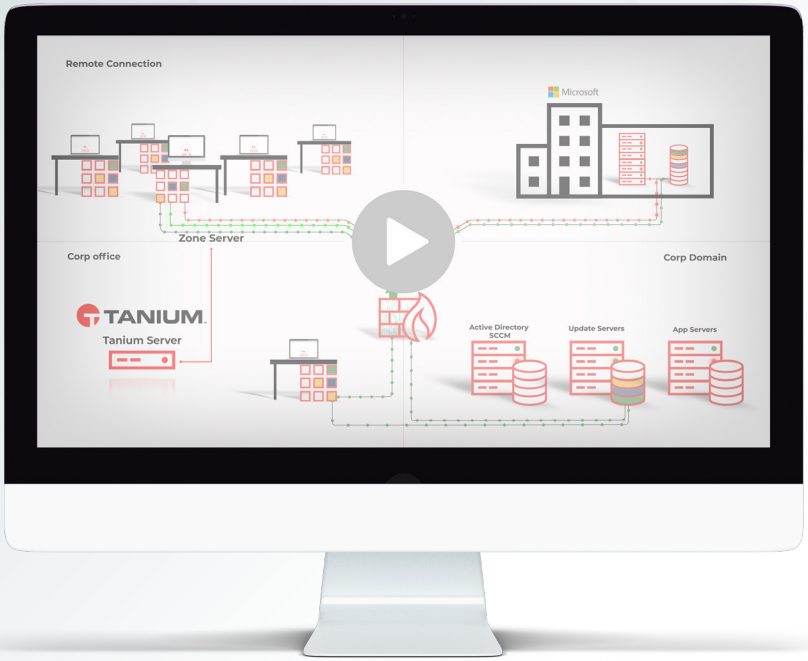
- How can I ensure sufficient network capacity through our VPN to accommodate increased remote working?
- How can I rapidly and securely provide my teams all of the tools they need to collaborate?
- How can I keep all infrastructure and applications routinely updated, patched, and operating effectively without impacting VPN capacity?

LEVEL 3
Plan for the New Normal

Once you are operating as normally as possible, you must look ahead, and begin to plan for and address the challenges to come once the crisis passes.

To begin, consider a few questions:

- How can I ensure my remote employees don't bring back threats when they return to a centralized environment?
- How will my day-to-day operations change? What elements of this distributed workforce environment will we keep?
- What have I learned? How can I create more robust operations that will hold up better to the next crisis?



Learn how Tanium overcomes patching challenges in an unplanned remote workforce.

Tanium: Designed to Deliver on This Framework

While the various impacts of the current pandemic were difficult to predict, such as the rapid transition to a near-complete distributed workforce environment, we have found that the Tanium platform was built to meet the exact needs of this moment.

The power of Tanium was built to harness the intrinsic speed of low-latency LAN traffic, which helps reduce inefficiencies caused by bloated databases, overloaded connections, and heavy traffic across WAN segments. Not only does this architecture make for very fast, scalable, and extensible endpoint visibility and control within corporate networks, but it also works well in highly distributed situations. Through the Tanium Zone Server, remote endpoints can be seamlessly, securely, and scalably managed without needing to tax VPN connections.

Tanium provides resilience, visibility, and control over endpoint-rich environments, and can deliver these outcomes rapidly through streamlined user interfaces and seamless integration into existing operational contexts.

Tanium's Targeted Value in Distributed Workforce Crisis Management

Tanium is primarily deployed by enterprise-scale organizations that operate in complex, demanding environments. Our platform gives IT operations and security teams a set of accurate, current information regarding the state of their endpoints. We provide a unified toolset that develops resilience and restores operations within this escalating crisis, while setting a foundation for secure, effective operations after the crisis passes and the new normal sets in.

Our customers have already deployed Tanium to grapple with this current crisis, and have found the use cases below particularly valuable.

In addition, Tanium includes hundreds of proven runbooks developed for specific use cases – including many that are immediately relevant to distributed workforce environments – to provide fast, comprehensive answers to mission-critical questions.

How Tanium Helps Customers Amidst Crisis - Key Use Cases

Policy Governance

Tanium monitors and enforces internal policies, and helps configure devices and applications according to corporate standards.

Hygiene Maintenance

Tanium performs daily vulnerability and patching scans and helps close all known exploits on devices and applications in a timely manner.

VPN Optimization

Tanium monitors and manages VPN endpoint usage and overall performance, and helps sustain uptime during high usage and spikes.

Software Management

Tanium helps deploy, configure, and update third-party applications through a self-service interface with scalable deployment of secure tools.

Tanium's Out-of-the-Box Endpoint Management and Security Solutions

We leverage our platform to deliver a portfolio of solutions that integrate seamlessly into our customer's existing infrastructure, applications, and processes. Combined, our solutions provide a congruent set of security and management capabilities across end-user, cloud, and server endpoints.

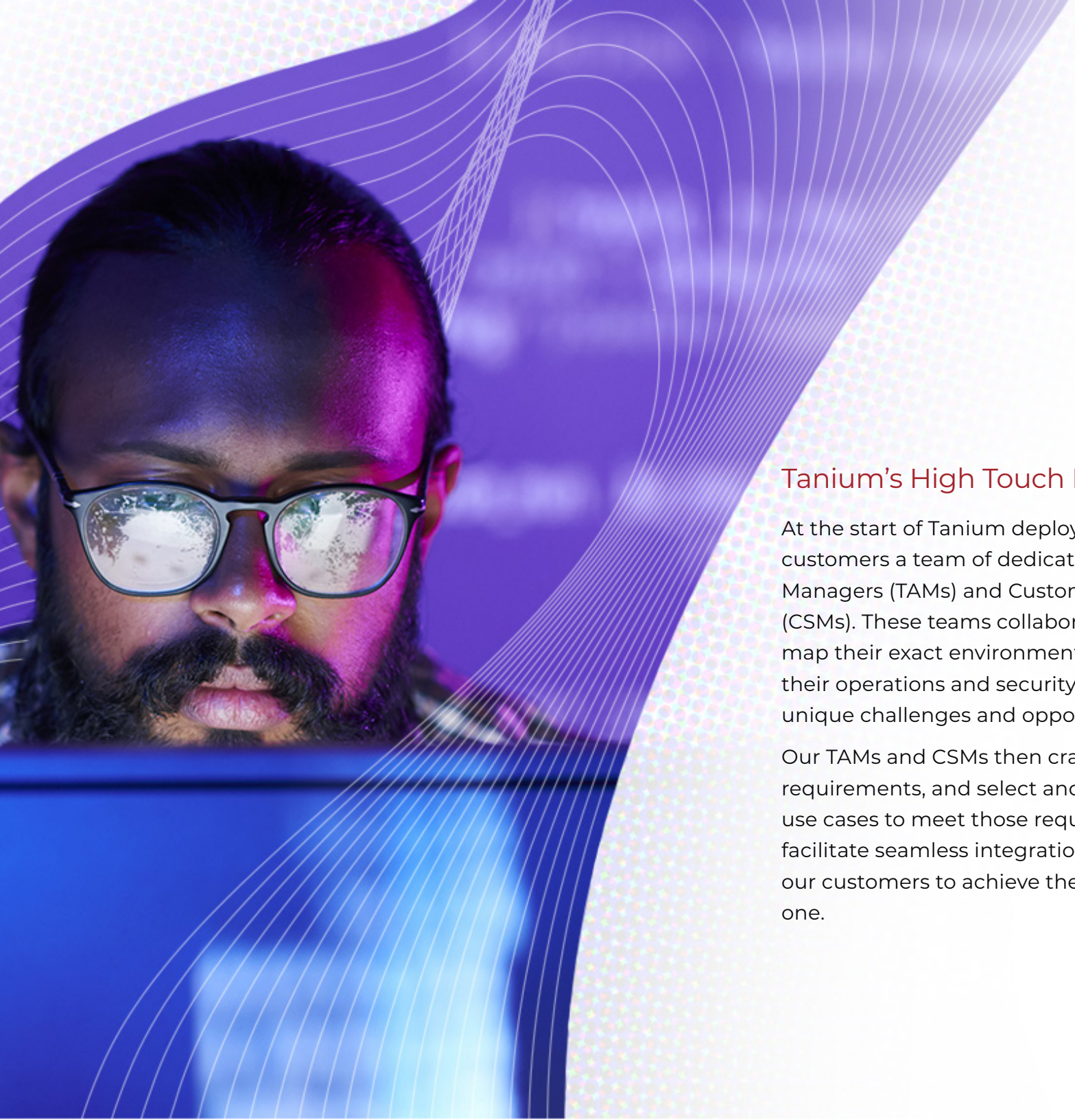
To assist our customers in gaining visibility and control over their distributed workforce environments, we have focused on deploying solutions that are centered on two critical capability sets:

Unified Endpoint Management

Gives teams visibility into the state of the systems across their enterprise, by providing tools to inventory, monitor, contextualize, and remediate endpoint assets.

Unified Endpoint Security

Gives teams end-to-end security for end-user, server, and cloud endpoints including the ability to identify assets, protect systems, detect threats, respond to attacks, and recover quickly.



Tanium's High Touch Deployments

At the start of Tanium deployments, we assign our customers a team of dedicated Technical Account Managers (TAMs) and Customer Success Managers (CSMs). These teams collaborate with our customers to map their exact environment, find the gaps between their operations and security capabilities, and define their unique challenges and opportunities.

Our TAMs and CSMs then craft a detailed set of requirements, and select and adjust the appropriate use cases to meet those requirements in order to help facilitate seamless integration. The goal is to partner with our customers to achieve their desired outcomes from day one.

Tanium's Benefits: What the Tanium Core Platform Delivers

Every Tanium deployment delivers the following fundamental benefits for organizations that seek to gain control over their endpoint-rich WFH environments.

Security Posture Improvement

Integrates fast and complete incident response throughout the distributed workforce network, to help safeguard data against known risk and privacy concerns.

Complexity Reduction

Performs ongoing asset discovery and inventory, to provide visibility and control while reducing operational complexity.

Data-Driven Decision Making

Generates and presents accurate, timely information, to drive simple, targeted answers to the environment's most complex and demanding questions.

IT Operations & Security Team Alignment

Closes the gap between IT operations and security teams to break their silos, align their activities, and remove friction from their working relationship.

Tanium's COVID-19 Endpoint Solutions: Real Cases, Real Results

While the crisis is still new, many of our customers have already experienced – and have successfully overcome – some of the most common challenges created by the COVID-19 pandemic.

Here are just a few examples that illustrate how Tanium endpoint management and security solutions helped customers develop resilience, restore operations, and plan for the next normal.

CUSTOMER	CHALLENGE	SOLUTION	OUTCOME
Multinational Financial Services Company	This customer felt concerned over work-from-home (WFH) employees installing their own personal printers to corporate assets, creating new security vulnerabilities.	Tanium rapidly identified tens of thousands of corporate assets with printers installed and provided this information in a clear report to the company's IT security team.	This customer's security team gained real-time visibility into their corporate assets, quickly diagnosed the evolving situation, and identified problematic assets.
Large Professional Services Firm	This customer had recently completed M&A activity and needed to both migrate assets and map their vast new endpoints – right when the pandemic hit.	Tanium migrated over a thousand new assets before the cutoff deadline, mapped the customer's new endpoints, and provided a complete patch management solution.	This customer can now identify lost and unmanaged assets, deliver patches with minimal impact, and close accountability gaps from loss of shared services.
Global CPG Company	This customer needed to address a security vulnerability in the Zoom messaging platform that was installed in many of their distributed workforce's assets.	Tanium identified impacted assets and remediated the vulnerability with an update package deployed to priority assets within hours.	This customer rapidly and accurately remediated this vulnerability across 50,000+ workstations spread across their global operating environment.
Government Agency	This customer mandated WFH for non-essential employees, and risked losing endpoint visibility, flooding their help desk, and complicating their ability to adopt and update third-party tools.	Tanium worked with the agency to provide end-to-end solutions, helped to properly configure their Zone Server for remote workers, and assisted in their seamless transition to a distributed workforce.	This customer has gained complete visibility and control over endpoints, flattened the curve of help desk calls, and allowed rapid third-party tool adoption.

How Tanium Can Help Transform Your Endpoint Management and Security

Tanium collaborates with customers to drive effective endpoint management and security during these unprecedented times. These times also highlight the type of benefits that can be obtained from Tanium's products.

While every Tanium solution is uniquely tailored to the operational environment in which it's deployed, the majority of our solutions create a transformed operational environment that provides:

- ✓ Simplified hygiene against personal assets
- ✓ Comprehensive visibility into endpoints
- ✓ Reduced burden on internal IT and security staff
- ✓ Remote incident remediation processes and tools
- ✓ Efficient and lowered endpoint management loads
- ✓ Adaptable, scalable endpoint management and security
- ✓ Ability to handle increased VPN access volume and spikes
- ✓ Complete reporting, triaging, notifications, and access control
- ✓ End-to-end management and security from within a single platform

Take the Next Step: Gain Clarity, and Take Control

Each customer is unique. But one thing unites us all: we are all transitioning through uncertain times. No one can say exactly what will happen tomorrow. No one knows when this crisis will pass. No one knows how work will be structured after this crisis does pass. The next new normal sets in.

There is one empirical truth Tanium customers understand: no matter what the new normal looks like, we've got your back. **Tanium was built for this.**

We work hand-in-hand with IT infrastructure teams to help ensure the secure and stable operations of critical WFH infrastructure and application ecosystems throughout this crisis and beyond. We help our customers allow remote employees to maintain efficiency and effectiveness no matter what happens next. We provide visibility into, and control over, the performance of technology services and the security over assets, workflows, and data.

To learn more about how Tanium can offer a helping hand – today and tomorrow – please select the next step that is most appropriate for your unique context.

Discover Your Gaps

Request an IT Gap Assessment to gain visibility into your current IT hygiene, and to measure your current Cyber Risk Score.

LEARN MORE HERE >>

Demo Our Solution

Schedule a demonstration to watch Tanium work live, and visualize exactly how our solution can transform your endpoint management and security.

SEE TANIUM LIVE >>

Deploy Tanium Now

Bring Tanium to your organization as rapidly as possible, and quickly gain visibility and control over your environment.

CONTACT US TODAY >>

Tanium offers a unified endpoint management and security platform that is built for the world's most demanding IT environments. Many of the largest and most sophisticated organizations, including more than half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium ranks 7th on the Forbes list of “Top 100 Private Companies in Cloud Computing” for 2019 and 10th on FORTUNE’s list of the “100 Best Medium Workplaces.” Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

tanium.com

@Tanium

info@tanium.com