TANIUM

EXECUTIVE BRIEF

# From Chaos To Clarity To Control

## Unified Endpoint Management And Security In a Time of Crisis

The COVID-19 pandemic has rapidly transformed the way organizations work, requiring 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 and cloud-based services, whilst allowing widespread use of employees' personal devices.

Working within this new environment has revealed an uncomfortable reality: critical visibility gaps are everywhere, and they could seriously escalate cybersecurity risk. In fact, using classic social engineering techniques, cybercriminals were among the first to react to the spread of the pandemic – deploying attacks like business email compromise, ransomware and traditional phishing scams.

## From Crisis to Chaos

These remote working threats have been driven by an explosion in unprotected endpoints, and stressors such as user error and shadow IT that expose assets to elevated cyber risk. Challenges for these unplanned, highly distributed workforce environments include:

### More endpoint vulnerabilities

Devices are operating with open vulnerabilities due to the effort or bandwidth required to connect them to a centralized patch management solution. This leads to unknown vulnerabilities, making risk assessments harder to perform, and increases the chances of remote employees suffering breaches.

### More sensitive data proliferation

The need to store, shuttle, and work with sensitive data at greater volume from remote devices has created an increase in risk of data spillage. On these occasions, the wrong data ends up in the wrong location – either from personal devices spilling into the corporate network or from within the corporate network itself – while also creating a significant compliance breach.

### More employees using personal devices for work

The rapid shift to accommodating an unplanned distributed workforce may mean employees' laptops, tablets, and mobile devices are not covered by patch management programs, potentially putting corporate data at risk. Even the least sophisticated attack can take advantage of these unsecured endpoints and the apps that they run.

### More external threats and attack vectors

Opportunistic malicious actors are taking advantage of the current chaos and lowered vigilance, as evidenced by the soaring rate of new security threats. Cybercriminals are increasing the volume of standard exploits, like phishing, and are deploying new ones to take advantage of currently popular applications – such as Zoom. These exploits are designed to deliver everything from ransomware to credential harvesting and business email compromise.

The current requirements to accommodate a highly distributed workforce have placed tremendous strain on remote connectivity infrastructure and IT support staff. This includes: overwhelmed internal IT and security staff; lack of capacity (especially when operating legacy VPNs); performance failures due to the "melting" of VPNs; unknown risks; untracked assets and devices as employees take them from office for home use without following protocol; and personal devices lacking proper protection or configuration.

## Achieving Clarity

The current crisis represents a new systemic challenge for organizations. It can't be solved by applying piecemeal solutions, by following policies and procedures that worked in the past, or by asking overstretched internal teams to simply do more.

In order to gain visibility and control over the new operating environment, it has become clear that organizations require the ability to:

- Gain 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.
- Enforce policy and maintain fundamental IT hygiene.

For customers grappling with the current crisis, Tanium customers can realize meaningful outcomes and gain control over their endpoint-rich distributed workforce environments. This includes:

### Policy Governance

By monitoring and enforcing internal policies, and configuring devices and applications according to corporate standards.

### Hygiene Maintenance

By configuring daily vulnerability and patching scans and closing all known exploits promptly on devices and applications.

### VPN Optimization

By managing and monitoring VPN endpoint usage, overall performance, and sustaining uptime during high usage and spikes.

### Software Management

By deploying, configuring, and updating third-party applications through a self-service interface with scalable deployment of security tools.

## Seize Control

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 rapid, 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 made seamlessly secure and managed without needing to tax VPN connections.

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

## The Next New Normal

One thing unites us all: we are transitioning through uncertain times, no matter what the next new normal looks like.

What has become increasingly clear is that Tanium is built for this. We help the largest and most demanding IT environments:

### Improve Security Posture

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

### Reduce Complexity

By performing ongoing asset discovery and inventory, to achieve visibility and control while reducing operational complexity.

### Make Data-Driven Decisions

Through the generation and presentation of accurate, timely information in order to derive simple, targeted answers to the environment's most complex and demanding questions.

### Align IT Operations and Security Teams

By closing gaps between IT operations and security teams, breaking their silos, aligning their activities, and removing friction from their working relationship.

## Next Steps

Contact us to bring Tanium to your organization today and quickly gain visibility and control over your environment.

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

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

## About Us

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.



TANIUM