謀
RESEARCH
Influence and insight
through social media

May 2021

Are You Ready for the Risks and Security Threats of the

HYBRID WORKPLACE?

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: HYBRID WORKING IS NOW PERMANENT

No one would argue that the COVID-19 pandemic changed a lot of things in our lives. We shop, learn and even entertain ourselves differently. Without a doubt, the most profound impact has been the change in the way we work. According to the ZK Research 2020 Work-from-Anywhere Study, prior to the pandemic, 22% of all workers were remote employees. That number peaked at 72% but is expected to settle at 42% for the foreseeable future—almost a doubling of the number of remote employees in less than two years.

This dramatic shift in workstyle has had a profound impact on the IT organization. The massive wave of people working from home created an equally large swell of cyber activity, as employees are no longer protected by traditional corporate security technologies such as perimeter firewalls, intrusion detection and prevention, and network forensics. A 2020 study by Atlas VPN found that Google registered more than two million new phishing websites in 2020, an increase of almost 20% from 2019. The trend shows no signs of abating any time soon; in fact, the problem has gotten worse.

A recent study from OpenText found that phishing has increased by a whopping 510% from January to February of 2021 alone, with the top five targets being eBay, Apple, Microsoft, Facebook and Google. The study also found that more than half of phishing sites use HTTPS, which hides the "bad" traffic from traditional security tools. Phishing has increased because it enables threat actors to target workers directly. If a user's computer becomes infected, that infection can create a backdoor into the company network of their employer.

Looking into the future, many business leaders interviewed by ZK Research confirmed that they expect workers to return to the office in the near future, but they also expect most people to continue to work from home at least one or two days a week. Given that the work-from-home phase is now permanent, IT needs to change its focus from being connectivity oriented (that is, how to connect people) to being security minded with an emphasis on keeping workers safe while sustaining the hybrid work model.

SECTION II: UNDERSTANDING THE RISKS OF HYBRID WORKING

Protecting the hybrid workplace requires a good understanding of the risk created by having data scattered across workers' computers in remote locations. It's easy to think that having VPN software connected to the company network might be sufficient; however, it's anything but. The majority of attacks target individual users instead of a company firewall. This creates an unprecedented level of risk, as the enterprise security solutions that companies spend millions of dollars on are completely bypassed.

Also, the pandemic accelerated the adoption of cloud-based applications. For example, 54% of respondents to the ZK Research 2020 Work-from-Anywhere Study stated that they increased spending on software-as-a-service (SaaS)–based collaboration tools as part of their remote worker tool kit—but cloud apps are a double-edged sword. Many businesses consider SaaS offerings to be

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

The shifting dynamic of work and security requires a new approach to IT.

more secure than traditional apps because the cloud provider takes care of all the security measures. However, employees download content from the cloud and then share it in other applications, and one infected file can spread malware very quickly throughout an organization. Most businesses do not have the ability to monitor and secure traffic once it leaves the corporate network, so the cloud effectively creates one massive blind spot.

The shifting dynamic of work and security requires a new approach to IT. Historically, infrastructure management and cybersecurity were handled independently, as the needs of the IT teams were different. The hybrid workplace requires these two disciplines to be combined.

SECTION III: THE IMPORTANCE OF COMBINING INFRASTRUCTURE AND CYBERSECURITY

The convergence of infrastructure and cybersecurity offers best-in-class protection across the company because the same data that is used to ensure endpoints are running correctly can also be used to detect threats. IT management software ensures that the software in use company-wide is current and patched, while security tools can detect active or even potential threats by monitoring anomalous traffic. Generally, most users conduct the same activities day after day. When something changes even slightly, that indicates the user's computer may have been breached. The combination of IT and security is powerful, as security systems can detect what happened and IT management can determine why, which leads to faster remediation.

Another benefit of combining these two domains is that doing so improves an organization's ability to proactively assess risk. This is relevant not only for IT; it benefits the entire C-level of a company. The data from a unified solution provides visibility into where the biggest risks are so IT and business leaders can determine where to focus their near- and long-term efforts. For example, the data might show that a few thousand devices are running older software that is susceptible to a certain type of malware. Many of these devices might be older systems that contain no critical company information and are segmented into a secure zone where a breach would pose no risk. The company could de-prioritize these and focus on ones that contain sensitive information.

SECTION IV: TANIUM PROVIDES A COMPLETE IT AND SECURITY SOLUTION

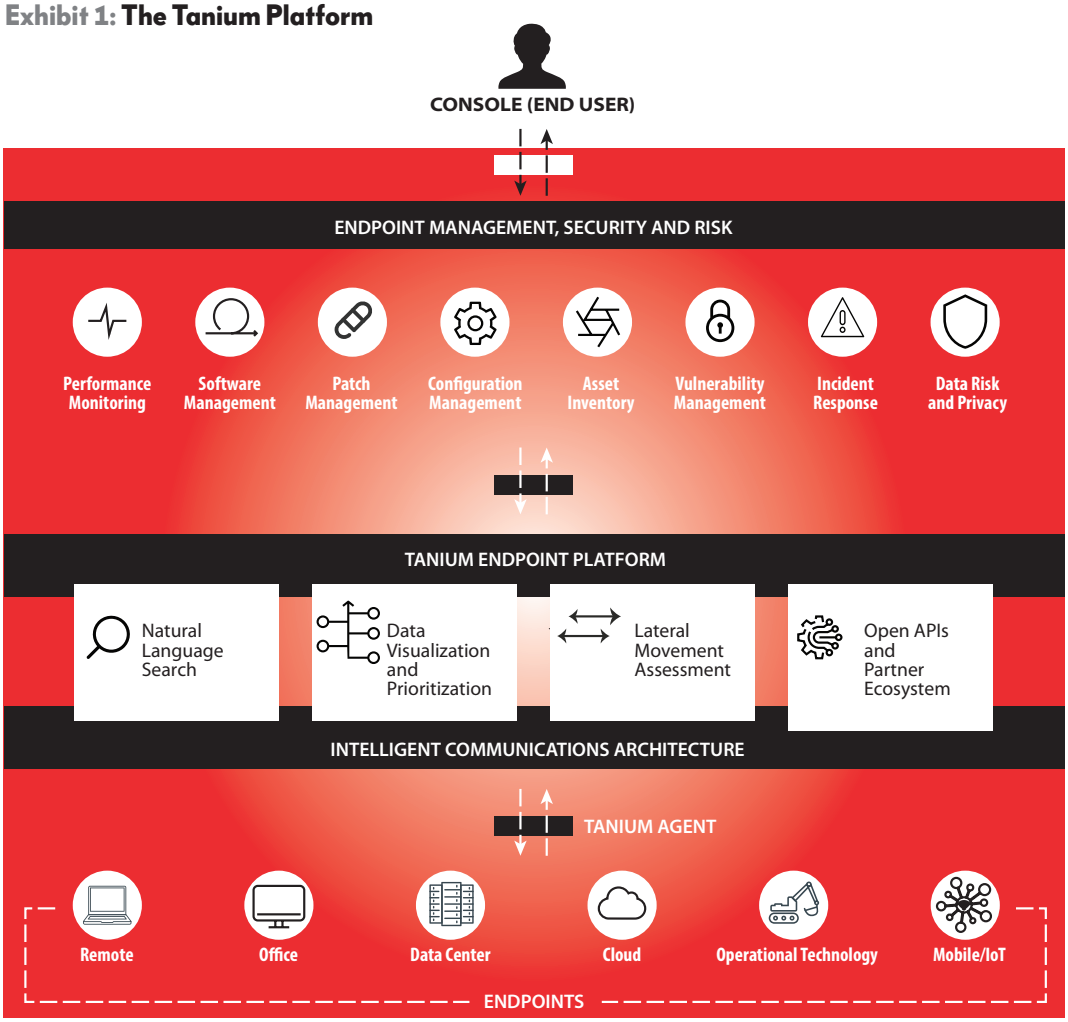
Tanium, an IT and security vendor, offers a holistic endpoint management and security platform that ensures businesses are ready for the hybrid work era. ZK Research considers Tanium to be the premium vendor in infrastructure and security management—based on both customer feedback and the fact that 50% of the Fortune 100 relies on Tanium, as do multiple branches of the U.S. Armed Forces. In 2020, Tanium was also ranked #12 on the *Forbes* Cloud 100 list of the top 100 private companies in cloud computing.

The company's flagship product, the Tanium Platform, provides real-time visibility with combined control, enabling a much faster response to remediating threats compared to processing and analyz-

ing data manually. Tanium uses a lightweight agent that runs on the endpoint, which provides a high-fidelity view of all the activity on the device. Many vendors try to accomplish this through network analytics; and while it's true that one can infer a fair amount from network analytics, IT pros will still be blind to the activities on the device itself. Tanium's platform is highly robust and can easily scale up to millions of endpoints, serving the needs of even the largest organizations. Another benefit of Tanium's agent approach is the speed of analytics. With traditional solutions, data must be gathered from several silos in order to locate anomalous activity. This can take months to do and can put the company at risk. The agent-based approach, combined with machine learning–based analytics, can perform the same tasks in just a few hours.

Exhibit 1 shows the breadth of the Tanium Platform. The solution is ideally suited for the era of hybrid work, as the agents can run on a worker's endpoint regardless of where they are located. Tanium provides a complete solution with capabilities such as automated inventory discovery,

Exhibit 1: The Tanium Platform



Tanium and ZK Research, 2021

incident response and patch management. In addition, the platform is a single tool that gives IT and security a common view, enabling them to work with a single source of truth.

Companies that deploy Tanium will realize the following benefits:

Rapid resolution: Tanium users can ask a question in plain English to inquire about the state of endpoints, analyze results and take action.

Extensible solution: Tanium's data can be connected to external or third-party systems, improving the effectiveness of those tools.

Accurate decision making: Tanium provides rich and comprehensive data. The solution constantly measures and reports on key security and operations metrics, enabling decisions to be made based on real data.

Improved security: Tanium connects to most identity providers to strengthen zero-trust initiatives.

Minimized risk of lateral movement: Tanium's real-time data visualization reduces the ability for threats to move laterally. Overly permissive admin rights or backdoors into systems will be exposed in the dashboard.

Deployment flexibility: Customers can choose to deploy Tanium as an on-premises solution or as a SaaS-based offering.

SECTION V: CONCLUSION

The world has changed, and it continues to change faster than ever before. IT and security pros need to be ready for the new era of hybrid work. It's unrealistic to expect tools designed for a rapidly vanishing era to work in this "new normal." The key to protecting a business and minimizing risk is to bring together IT and security data with a platform like Tanium's. Businesses that do so will be able to adapt regardless of what the future holds, while those that don't will find it increasingly harder to manage and secure their environment—and will eventually reach a point where the task is untenable.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314