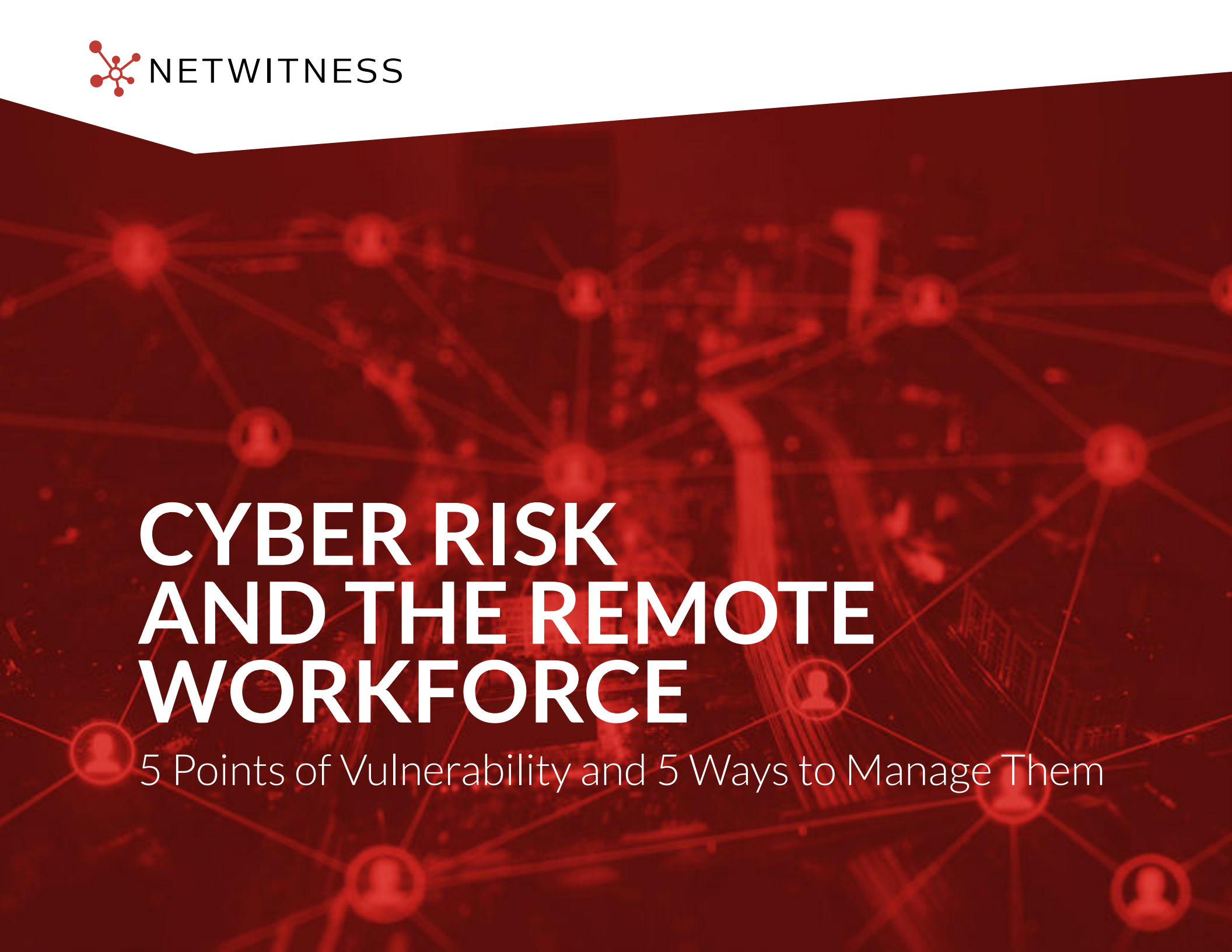
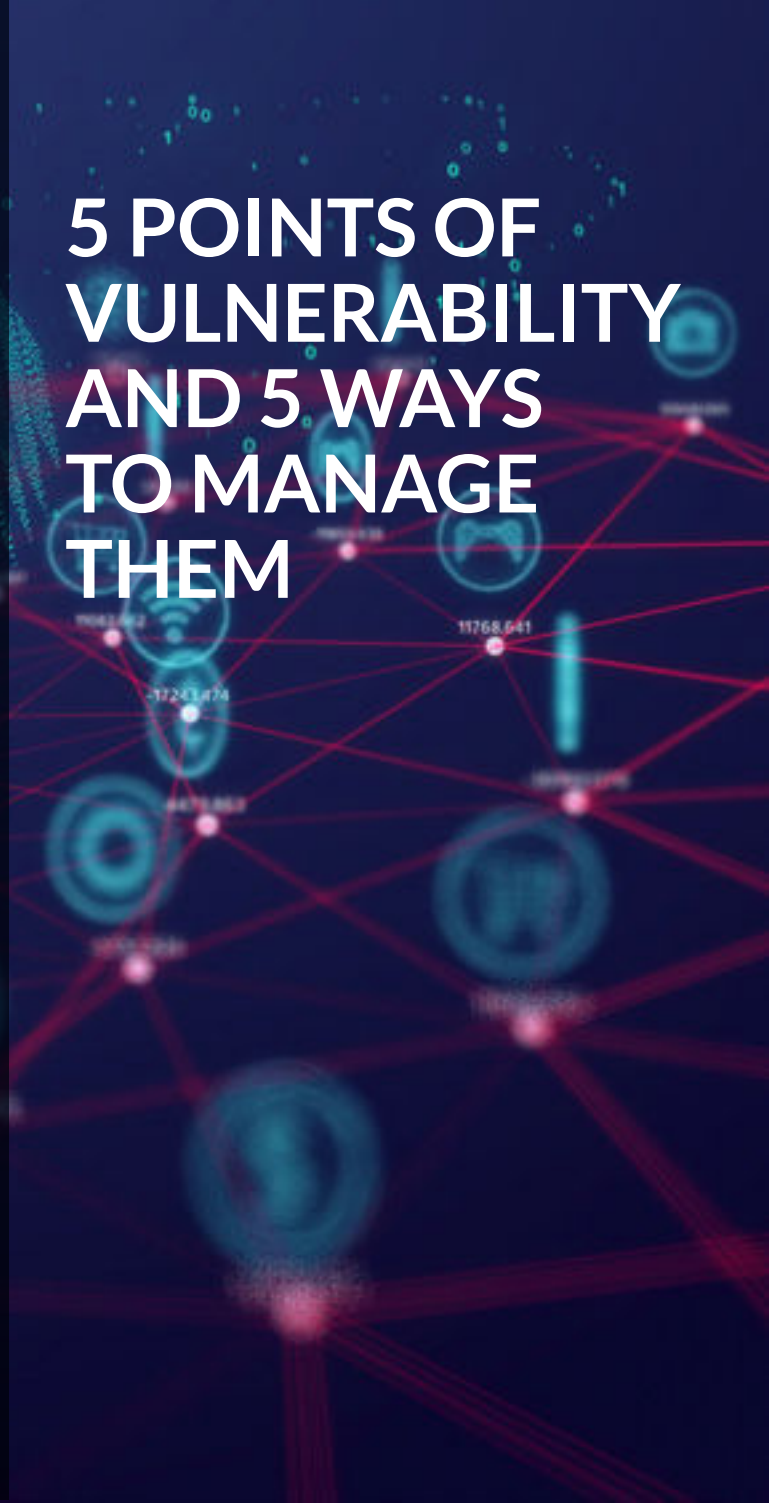
NETWITNESS



CYBER RISK AND THE REMOTE WORKFORCE

5 Points of Vulnerability and 5 Ways to Manage Them

5 POINTS OF VULNERABILITY AND 5 WAYS TO MANAGE THEM



In what seems like no time, many organizations have made a remarkable pivot from perhaps a few people working from home to most or all working from home.

But now that a remote workforce has become one of the greatest assets to your business today, is it also at risk for becoming one of the greatest threats?

The answer is yes—but it doesn't have to be that way.

Read on to learn how extending digital connectivity beyond the workplace increases exposure to cyber attacks and other threats to data security, and what you can do to identify and manage the risk.

WORKING FROM HOME: 5 POINTS OF RISK

NOT A NEW PROBLEM (JUST A BIGGER ONE)

Even before the seismic shift to so many people working from home, organizations around the globe had cyber-attack risk and workforce at the top of their digital risk agendas. According to the RSA Digital Risk Report, these were already the #1 and #2 digital risk management priorities at the end of 2019 for organizations undergoing digital transformation.[1]

When people access work applications and resources from beyond the traditional work perimeter, they lose some of the protections the perimeter provides. This can increase the risk of bad actors getting access to sensitive data. Here are five typical points of vulnerability you'll find in just about any work-at-home environment.

Employees How security-conscious are employees when they're working from home? Do they use work laptops for personal apps? Are they sharing work devices with family members? People may engage in these and other risky behaviors without realizing the danger they may pose.

Endpoints Are laptops and devices in the home office work-issued or personal? Work-issued should be the norm. But remember: While a work laptop has more security controls, those may not be as significant when people connect from outside of work facilities, where new risks can lurk.

Other Devices The laptop may be from work, but if it's connected to a home printer or other device that doesn't have the latest security patches, that's a problem. Home devices can open up a point of entry for a cyber attack, and the security team at work may not even be aware of it.

Home Automation Webcams and smart home components like networked thermostats and doorbells add even more points of entry for cyber attackers looking for vulnerable points of connectivity to exploit.

Wi-Fi Because of the lack of standard configurations for Wi-Fi access technology, connecting to work resources from a home network is inherently riskier than connecting at work.

5 WAYS TO PROTECT THE HOME WORKPLACE

THE PROBLEM WITH PATCHES

Once employees move outside the workplace perimeter, it can be a challenge to enforce the patches and updates that harden devices. Depending on the devices remote employees use, security teams may not have the visibility into their systems needed to ensure employees comply with requests to install updates or take other required actions.

Visibility and insight are essential to identifying vulnerabilities and spotting threats in work-at-home environments. Once a threat is detected, adding context and orchestration is critical to responding swiftly and effectively.

Endpoint visibility An endpoint is often the starting point for threats like phishing and ransomware, so visibility into what's happening on endpoints is crucial to securing at-home work environments.

Network visibility Monitoring network traffic into and out of a remote employee's environment provides visibility into possible threats moving into and through the network.

Behavior insights Threat detection is aided by being able to observe and understand the online behavior of users and the devices with which they interact—and to detect aberrations in that behavior.

Orchestrated response Organizations need to be able to add context to threats—what are they targeting? something critical or inconsequential?—and orchestrate a response based on that context.

The big picture Ideally, the security team should be able to see the full attack landscape and understand the relationships between entities and assets throughout the environment.

5 ESSENTIAL TOOLS, 1 CONSOLIDATED PLATFORM

WHAT'S AT STAKE?

If poor security in the remote workforce leads to a data breach, the resulting exposure ranges from valuable corporate data to sensitive customer information. In the most recent edition of the RSA Data Privacy & Security Survey, 75% of participants most feared loss of their financial data (78%), security information (75%) and identity information (70%).[2]

The following tools are critical to enabling security teams to manage the risks that come with deploying a remote workforce. Even more critical is consolidation of multiple tools on one platform; this enables simultaneous visibility across the attack surface and facilitates a rapid, coordinated response.

Endpoint monitoring Continuous awareness of endpoint behavior and sophisticated analysis of threats that appear provide a first line of defense against the types of attacks that typically begin at endpoints.

Network monitoring The ability to capture network packet data is critical for the deep visibility needed to quickly detect, investigate and respond to network threats.

User and entity behavior analytics (UEBA) If you can establish what constitutes "normal" behavior for your remote workforce and the devices they use, you can identify threats based on behavioral anomalies.

Orchestration A system for coordinated, context-based threat response makes it possible to take quick and consistent action once threats are detected.

A platform-based approach To detect intrusions as they are happening, you need a threat detection platform that can provide complete, real-time visibility into all network and endpoint activity as well as the analytics to prioritize threats for response.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

For more information, go to netwitness.com

1 RSA Digital Risk Report, Second Edition, January 2020
2 RSA Data Privacy & Security Survey 2019

NETWITNESS