NETSCOUT

| WHITE PAPER |

Why Cyber Resilience Is Needed in the Post-Pandemic World

SECURITY

TABLE OF CONTENTS

Pandemic Accelerates Digital Transformation and Expands Threat Landscape

Although it's difficult to say when the world will finally see the end of the COVID-19 pandemic, many of the changes the pandemic wrought on the work environment are likely here to stay—at least to some degree. To wit, in a survey of 2,000 full-time American workers who have been working remotely during the pandemic, 87 percent say they want to continue doing so, and 42 percent say they'll look for work elsewhere if their current company doesn't continue to offer long-term remote-work options.

Continuing to support remote and work-from-home (WFH) initiatives will create long-term new realities for enterprises, as well. In the rush to support remote and WFH initiatives, 96 percent of business leaders said their digital transformation journeys were accelerated by an average of 5.3 years. As such, enterprises were forced to relax security policies to support remote work, creating a number of security issues, including the following:

- Employees were allowed to connect personal devices to the enterprise network, leaving the business exposed to whatever endpoint security software and patching schedule was (or wasn't) being utilized.
- Remote workers used employer-supplied computers for personal use, exposing enterprise networks via actions such as clicking on a phishing link within a personal email.
- Employees accessed the enterprise network remotely, using Wi-Fi networks that had lax or no security policies in place.
- Policies that limited or blocked the use of USB devices were relaxed.
- Home routers became the new enterprise edge or security perimeter. IoT devices connected to home routers also became the new enterprise perimeter, because such devices share the home router with computers used for work.
- Most virtual private networks (VPNs) granted open and indefinite permissions to access entire suites of corporate applications or data assets, with no contextual verification checks or other security updates.

Expediting digital transformation also forced enterprises to significantly increase their dependence on the cloud, with 90 percent of executives indicating that their cloud usage is now higher than planned before the pandemic. The unintended result for many enterprises has been abandonment of mature cloud migration plans that were expected to take months or years to cover design, develop, test, deploy, and review phases.

Nevertheless, worldwide spending on cloud services, the hardware and software components underpinning the cloud supply chain, and the professional/managed services opportunities around cloud services, is forecast to surpass $1.3 trillion by 2025. Yet despite that expected growth, 83 percent of enterprises indicate that security is a challenge. The reality is that the pandemic has changed the cyber landscape and given attackers the ability to develop more-advanced threats.

63% of leaders say COVID-19 made their organizations embrace digital transformation sooner than they had expected, resulting in greater investments in technology. 49% admitted that digital transformation was not a strategic priority prior to the pandemic's outset, but it's become one since.

– What We Know Now: The state of digital transformation today, Celerity

Attackers Adjust and Thrive During Pandemic

As enterprise IT has had to react and adjust to network changes triggered by a massive shift to remote work, cyberattackers also have reacted and adjusted the ways in which they target and attack enterprises, with major shifts occurring in attacker capability, the types of attacks being made, and the ways in which attacks are being carried out.

Indeed, attackers saw the pandemic as an opportunity to increase activity by exploiting the vulnerability of employees working from home, evidenced by the fact that one recent survey found 47 percent of people fell for a phishing scam while working at home.

According to the latest NETSCOUT® Threat Intelligence Report, attackers launched 5.4 million DDoS attacks in 1H 2021. For just the first quarter of 2021, attack frequency increased by 20 percent over the same period in 2020. But attackers didn't simply increase the number of DDoS attacks launched: They also developed new ways to target the attacks and monetize them.

A perfect example is the triple extortion attack now offered in a number of ransomware-as-a-service (RaaS) portfolios. Here's how it works:

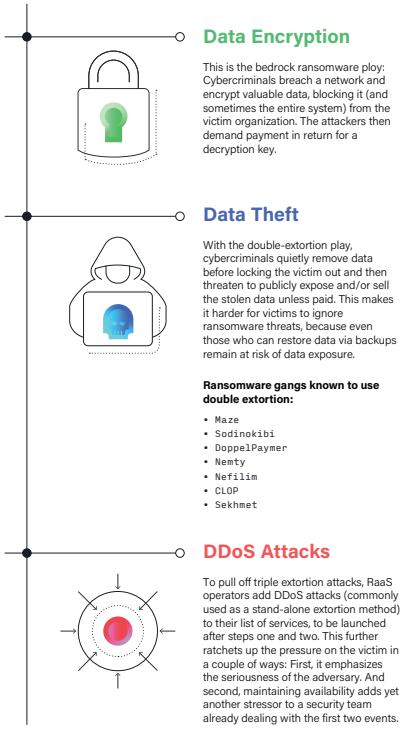
1. **File encryption:** With the traditional ransomware attack method, cybercriminals breach a network and encrypt valuable data, making it (and sometimes the entire system) unavailable to the victim organization. Attackers then demand payment in return for a decryption key.
2. **Data theft:** Attackers then exfiltrate the data before locking the victim out, while also threatening to expose and/or sell the stolen data publicly unless paid. This second level of extortion makes it harder for victims to ignore ransomware threats, because even those who can use backups to restore data remain at risk of data exposure. Clearly, it's a valuable monetization tool: It's estimated that nearly half of ransomware cases in the third quarter of 2020 used exfiltration tactics.
3. **DDoS attacks:** The final step is a DDoS attack, which RaaS operators added to their list of services to be launched after the first two steps. This further ratchets up the pressure on the enterprise by emphasizing the seriousness of the adversary, while also placing more stress on security teams that must maintain availability and deal with the first two events.

By combining file encryption, data theft, and DDoS attacks, attackers have essentially hit a cyber-extortion trifecta designed to increase the possibility of payment. From the attacker's perspective, adding DDoS attacks to a list of ransomware services is a smart business move. DDoS attacks are incredibly cheap and easy to launch, and they increase the chance that a victim will pay.

But attackers aren't stopping there. They've also developed new malware to attack and infiltrate systems. Prior to the pandemic, about 20 percent of cyberattacks used previously unseen malware or methods. During the pandemic, that proportion rose to 35 percent.

Some of the new attacks use a form of machine learning that adapts to its environment and remains undetected. For example, phishing attacks are becoming more sophisticated and use different channels, including SMS and voice. News about vaccine developments has been used for phishing campaigns.

Hackers also are using credential-stuffing techniques to gain access to employees' credentials, subsequently selling the stolen data to other cybersecurity criminals. Credential stuffing is a form of cyberattack whereby hackers use previously stolen combinations of username and password to gain access to other accounts—made possible by people who use the same username/password combination across multiple accounts. Increasingly, credential stuffing is being used to give attackers access to virtual meetings, where they obtain confidential or sensitive information that is then sold to another party or made available to the public to damage a company's reputation.



Moreover, attackers have focused renewed attention on devices that enterprises increasingly have had to rely on to support remote work and digitization. For instance, by attacking on-premises virtual private network (VPN) concentrators that enable remote work, threat actors know they now can disrupt an entire organization. Prior to the pandemic, such an attack might have disrupted only 10 to 20 percent of the workforce. Another example is a spike in brute force remote desktop protocol (RDP) attacks, as well as User Datagram Protocol (UDP) reflection and amplification attacks. Increasingly, enterprises are experiencing a substantial rise in secondary and tertiary extortion after initial infection.

Cyber Resiliency Takes Center Stage for CIOs and CSOs

All of these factors are leading enterprises to prioritize cyber resiliency—the ability to predict, resist, recover from, and adapt to attacks. Ultimately, cyber resiliency centers around creating visibility across the enterprise and improving the ability to identify and measure risk, taking into account how your business operates, its value chain, how information and data flows across the enterprise, and critical applications and systems.

The changes wrought by the pandemic on enterprise networks have, likewise, moved cyber resiliency from a security initiative to a business strategy. In fact, 66 percent of enterprise security professionals plan to invest in cyber resiliency this year, according to a recent study, and 75 percent have increased cybersecurity budgets as a result of the pandemic to do so.

Enterprise security teams have identified the following as the top four most challenging aspects of incorporating cyber resiliency in their organizations:

1. Digital business is growing too quickly to keep up: 79 percent
2. COVID-19 has changed the cyber landscape: 71 percent.
3. Threats to the organization are more advanced today compared with 2019: 68 percent
4. We don't have the right tools or technology: 60 percent

The impact of these changes for CIOs and CSOs is twofold. First, there's a need for organizational change to better align cybersecurity and IT. Security teams should detect, validate, investigate, and respond to threats on an ongoing basis. But security also is a strategic priority for network teams. In fact, a reduction in security risk is among the key measurements of success for network teams—even before service quality, network visibility, and end-user experience.

Today's complex digital infrastructure demands collaboration between network and security teams to gain better clarity on whether an IT service event is a performance issue or a security incident. Cross-team collaboration will drive cost and operational efficiencies, reduce overall risks, and quicken the pace for resolving security incidents.

IT leaders can encourage this collaboration by providing a transformational security view across operations and infrastructure that includes:

- A data store built for use by both security and network teams
- A toolset that enables collaborative workflows
- Documented policies, controls, and best practices that formalize cross-team collaboration

Second, enterprises need to resolve technical issues to achieve greater network visibility with intelligent edge defense and enable automation on par with attackers. This ultimately means that critical IT and network infrastructures must be available at all times, with easy access remotely to data, applications, and internal services. Poorly performing infrastructure will have adverse impacts, including loss of productivity, poor customer service, a significant reduction in revenues, and additional vulnerability to cyberthreats.

Improved visibility takes on even greater importance given that today's enterprise networks are extremely complex, covering physical and virtual offices, public cloud environments, and more. Ensuring a secure network requires enterprises to capture data from various sources or touchpoints and apply threat intelligence and business analytics. Factors that should be considered when choosing a solution include:

- **Scalability:** Highly scalable network instrumentation that delivers comprehensive visibility across distributed digital infrastructures.
- **Intelligence:** Threat detection using curated threat intelligence, behavioral analysis, open-source data, and advanced analytics.
- **Contextual data:** Cyberthreat investigation and hunting that is contextual, using a robust source of metadata and packets.
- **Automated blocking:** Stateless packet processing technology that automatically blocks threats at the perimeter—including DDoS attacks, cyberthreats, and outbound indicators of compromise.
- **Visibility:** Comprehensive and consistent network visibility across disparate digital infrastructure.

LEARN MORE

For more about how your company can benefit from cyber resiliency, get in touch with NETSCOUT today.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_023_EN-2101 20/2021