SOLUTION BRIEF

Newtek TECHNOLOGY SOLUTIONS


# MAKE YOUR NETWORK **ZERO TRUST**-WORTHY

## MOVING THE PRINCIPLES OF ZERO TRUST INTO ACTION

Who can you trust in this world? Your pet dog, minus the occasional shoe chewing? Your best friend, minus the occasional unsolicited criticism of your wardrobe choices? Trust in 2021 is a precious commodity. In the networking and data protection world, there is only one answer as to whom you can trust: no file, no app, no user. Zippo. Sounds harsh? The reality is businesses are still suffering from data breaches caused by a plethora of actions: unauthorized access to a file, phishing attacks, unsecured devices used outside of a corporate network and a host of other events leading to painfully costly disruption.

> "Breaches continue to be a fact of life and must remain at the top of an organization's threat protection list."

Two recent high-profile cases:

- The hacker's group Dark Side in May successfully attacked Colonial Pipeline, the largest fuel pipeline in the United States. The ransomware threat shut down its entire network. It drove benchmark gasoline prices to a new high as the hack disrupted supplies across the Eastern U.S. The company expected it to take a week to return to full operations. Dark Side later released a statement to the effect it was just trying to make money, not cause the serious disruption that occurred.
- Reverb.com, a powerhouse online retail marketplace, in April experienced a data breach affecting 5.6 million members. The names, addresses, email addresses and phone numbers were exposed before the breach came to light. Interestingly, the breach was discovered by an external security researcher who alerted Reverb to the issue. The company advised members to change their passwords after the breach was known.

From wholesale disruption of fuel supplies to threatening musicians' livelihood, breaches continue to be a fact of life and must remain at the top of an organization's threat protection list. Some of the

current breach issues IT is facing include the increase in a remote workforce using devices that may not be fully secure; cyber threats from Russia's Foreign Intelligence Service, or SVR, and new virus permutations like Babuk, which operates on a ransomware-as-a-service model. Babuk hit the NBA Houston Rockets organization, for example, claiming to have stolen 500 gigabytes of Rockets'data, including sensitive financial data. Ransomware-as-a-service is also the model of the Colonial Pipeline and Reverb attacks, in which hacker groups essentially allow other threat groups to use their infrastructure, and then share in the funds obtained via ransomware payments.

## ZERO TRUST: THE BEST SECURITY OFFENSE

It's a common practice to talk about threat defense. In the current threat environment the best approach is offense, adhering to the concept and principles of Zero Trust. In applying Zero Trust, rather than focus on defending against a discrete attack, an organization assumes every request to access is a breach, and therefore each request must be verified as if it originated from an open network.

Zero Trust offense acknowledges not only the varied and highly creative cyberattack environment but also the way in which the security perimeter has changed. Remote working, for example, has forced organizations to rethink the perimeter as employees are using their own devices, and connecting to networks without all necessary access protocols fully in place. It is faster to share files with third parties using personal devices rather than log on to a corporate network, thereby inviting data breaches as the employee perhaps sends those files back to the corporate network at some point.

**A Zero Trust approach is the most effective offense** in protecting against threat sources—from inside or outside the corporate network.

Bypassing on-premises perimeter-based security models that rely on network firewalls and VPNs is increasingly common as people work in hybrid and cloud environments. Organizations need to think of the perimeter now as every access point that hosts, stores or accesses corporate resources. Remote working and the cloud have taken away the physical boundaries of the perimeter. As a result, a Zero Trust approach is the most effective offense in protecting against threat sources – from inside or outside the corporate network – and coming from a long list of access points.

## PRINCIPLES OF ZERO TRUST

'Never trust, always verify' is the Zero Trust mantra. Rather than assume some requesters are trustworthy, or the resource they want access to is allowed, all access requests are treated as threats. To implement Zero Trust these fundamental principles are in play:

> **Continual, Explicit Verification.** Users are authenticated, authorized, and continuously validated before they can gain access to applications or data. IT security can use all available data points for authentication, including user identity, location, device health, service or workload, and data classification. Verify that all sessions are encrypted end-to-end.

**Least Privileged Access.** Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices. Also re-examine all default access controls to further ensure access is being granted appropriately and is up-to-date for all users.

**Breach Control.** At the heart of Zero Trust is the assumption that any access point is a vulnerability and a breach will inevitably occur. Use microsegmentation to contain any attack surface by segmenting access by network, user, device and application awareness.

"At the heart of Zero Trust is the assumption that any access point is a vulnerability and a breach will inevitably occur."

**Real-Time Vigilance.** In parallel with least privileged access, enable real-time monitoring and analytics to improve visibility and identify and stop malicious activity.

## MOVING INTO ACTION

While some Zero Trust principles like user authentication should already be in place in your organization, following all these principles diligently will place your organization in a much stronger position from which to protect against threats.

READ MORE:

**THE FOUNDATIONAL ELEMENTS IN A ZERO TRUST ACTION PLAN.**

Top tips to achieve an optimal mature level of Zero Trust.

**Download here.**

Newtek® TECHNOLOGY SOLUTIONS

Newtek Technology Solutions, Inc. ("NTS"), a portfolio company of Newtek Business Services Corp. [Nasdaq: NEWT], provides a complete range of IT managed services, secure private cloud hosting, backup and disaster recovery, and full web ecommerce solutions. NTS has specialized in helping businesses leverage technology to drive innovation for over three decades.

**877.323.4678 | www.newtektechnologysolutions.com**

2500 W Union Hills Dr., Suite D104 | Phoenix, AZ 85027