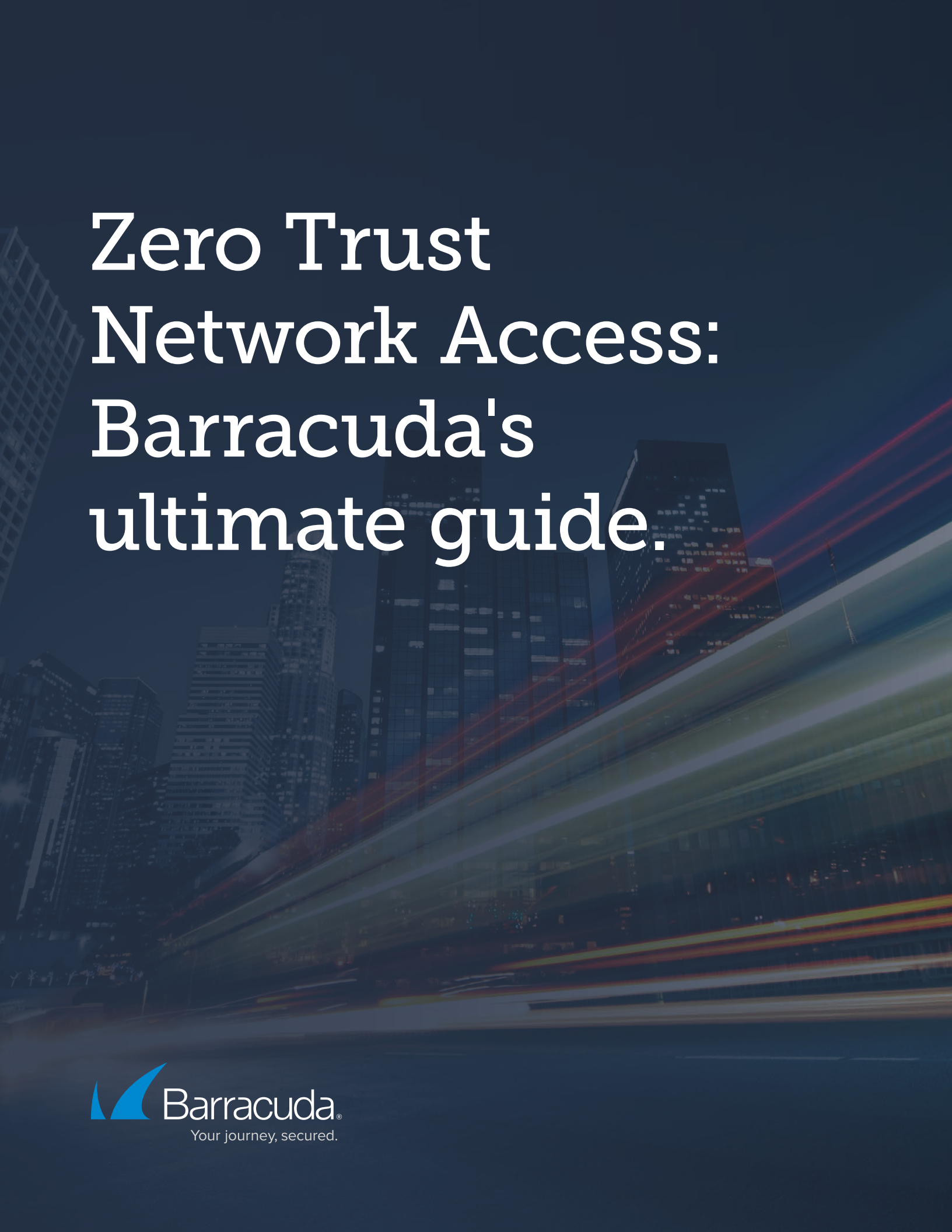
Zero Trust Network Access: Barracuda's ultimate guide.



Barracuda®
Your journey, secured.

Introduction

The cybercrime threat landscape is more saturated than ever, with attacks growing in sophistication and successfully hitting organizations in every sector. What's also growing is the financial damage to these businesses: IBM Security reported a 10% increase in the average total cost of a breach from 2020 to 2021 — the largest increase in a single year in the last 7 years.[1] To avoid the growing financial risks, businesses urgently need to rethink their security postures — traditional security methods are no longer cutting it.

[1] https://www.ibm.com/downloads/cas/OJDVQGRY

The need for Zero Trust Network Access

As remote work and the reliance on the cloud increased over the last few years, the cybersecurity industry has seen a rapid acceleration in the shift away from traditional perimeter security. The almost overnight adoption of remote and hybrid work led to a sharp increase in Bring Your Own Device (BYOD) policies, and with these, varying levels of security for individual workers. Organizations with workers accessing their networks on a multitude of devices and from a wide range of locations needed — and many still need — a way to ensure that all incoming traffic is genuine.

VPNs are no longer up to the challenge. They are frequently overloaded with too many users and often grant too much access to users who don't need it. On top of this, the mixed bag of legacy tech and security solutions that many organizations are using adds another layer of complexity and vulnerability. The combination of firewalls, VPNs, web gateways, and network access control solutions create a complicated infrastructure that is difficult to manage and gain accurate insights from. These pick-and-mix infrastructures lack visibility, making it difficult to fully account for who is attempting to access different parts of the network and where from.

Enter Zero Trust Network Access (ZTNA). While traditional network security was based around a 'trust but verify' model, ZTNA is a new approach of 'never trust, always verify.' Zero Trust is a philosophy revolving around the concept that no one should be automatically trusted with access to networks or assets. It involves managing permissions and access so that users are granted specific access to only the data or applications they need. Employing continuous verification, another tenet of ZTNA, reduces the potential of network breaches and lateral movement of any threats.

What is Zero Trust Network Access?

While 'Zero Trust' sounds somewhat negative, the model is actually one of enablement, not restriction. It allows for better remote access, improved performance, better productivity, and strengthened security.

A good way of understanding Zero Trust is to compare it to moving through an airport. When you arrive at the check-in desk, you need to authenticate your identity with your passport. This gets you through one stage of the process of making your journey across borders. However, this does not grant you permission to board the plane: You still need your boarding pass. Without both documents, you will be denied access.

Applied to network access, with Zero Trust, if you can't both authenticate your identity — your passport — and prove that you have the required permissions — your boarding pass — to access the network, you won't be able to continue your journey. Just as individual passengers are thoroughly checked at security and must prove their identity and authorization to proceed, Zero Trust requires that of every user as they attempt to access your network.

ZTNA has a multitude of benefits. Of course, there's the benefit of automatically blocking suspicious attempts to access your network due to the lack of permissions, which reduces the risk of a breach by a malicious actor. But another benefit that may be less immediately obvious is the robust system of record that it provides. The device, location, and identity of every user that attempts to access the network are recorded, providing you with an audit log and adding a layer of automated accountability that other solutions lack. In addition to security, this information is useful for compliance or audit needs.

This isn't the only example of how ZTNA employs automation. With this solution, there's no need for IT tickets or approval from management to gain access to new parts of the network. With these details predefined, the process is automated from the beginning, speeding up access and saving time previously spent on activities like manually authenticating users. The time saved with automation and the reduced need to sign in, along with benefits such as better remote access, improved performance, and productivity, makes ZTNA a solution that improves security for all users.

How to implement Zero Trust Network Access

To successfully implement ZTNA, first you need to map out the surface you will protect. This should include all the critical data that you hold — for example, personally identifiable information, credit card information, and any intellectual property. Applications, assets and devices, and services also fall into this category.

Next, identify who needs permission to access these data sources, applications, assets, and so on. Implement single sign-on (SSO), a method of authentication that allows your users to securely access multiple sites and applications with a single set of credentials. This allows you to create a single source of truth for users.

Enable multifactor authentication (MFA), which requires users to verify their authentication attempts with another device, ensuring that the request was genuine. This makes the source of truth more robust and reduces the likelihood of impersonation.

Lastly, make sure that there is a strict endpoint device validation process in place. Ensure that all devices for all users are registered and that you have a directory that includes the device ID, serial number, model, and operating system. Without validating these devices first, the user won't be allowed to access any part of your network or any data which is protected by the previous steps.

How Barracuda can help

As it becomes more apparent that employees are increasingly in favor of remote or hybrid work situations, the need for ZTNA applies to more businesses than ever before — and some that may never have expected to rely on devices outside of the traditional perimeter. Making sure that every single one of these devices is both secure and verified sounds like a massive task, but it doesn't have to be.

Try Barracuda's Zero Trust Network Access solutions for free.

Barracuda CloudGen Access is a single solution that allows you to enable Zero Trust Network Access from any device, anywhere. Our solution is quick to deploy and easy to manage, with unparalleled access control across your users and their devices without the drawbacks of a VPN. Providing remote, conditional, and contextual access while reducing over-privileged access and the associated third-party risks has never been easier.

Barracuda SecureEdge, a cloud-first SASE platform, enables businesses to easily control access to data from any device, anytime, anywhere, and allows security inspection and policy enforcement in the cloud, at the branch, or on the device. Barracuda SecureEdge includes Zero Trust Network Access (ZTNA), Firewall-as-a-Service, web security, and fully integrated office connectivity with Secure SD-WAN.

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level. For more information, visit barracuda.com.

Barracuda
Your journey, secured.

Try a full-featured demo of CloudGen Access or SecureEdge for free, or get in touch to find out more.

Zero Trust Network Access: Barracuda's ultimate guide. • US 1.0 • Copyright 2022 Barracuda, Inc. • barracuda.com
Barracuda and the Barracuda logo are registered trademarks of Barracuda, Inc. in the United States. All other names are the property of their respective owners.