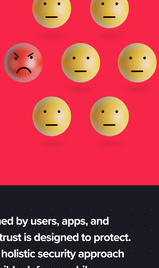
CyberRes

7 Reasons

Why You Need Identity Management in Zero Trust



In an age where data is consumed by users, apps, and devices around the world, zero trust is designed to protect. When done right, zero trust is a holistic security approach that provides the strongest possible defense, while ensuring that all identities can access the information needed, when it's needed.

Here are seven ways identity management helps zero trust improve security.

1

Zero Trust is Built for the Cloud

Traditional security focuses on protecting the network perimeter, but offers little protection for the hybrid and cloud-first business of today. **With zero trust, your policy determines exactly what identities can and can't do, in every environment.**

2

Zero Trust Protects Your Privileged Accounts

Privileged accounts—those with access to the "keys of the kingdom"—are the biggest draw for cyberthieves. **Zero trust provides extra protection for these accounts.**

3

Zero Trust Protects You from Insider Threats

Not all attacks come from malicious outsiders.

The Cost of a Data Breach Report shows that 19% of breaches occurred because of a compromise at a business partner.

In a recent State of Zero Trust report, almost 9 out of 10 claimed that they were on a path to a Zero Trust environment.

Zero trust treats all identities the same. Until an identity has been thoroughly verified, it doesn't get access.

4

Zero Trust Protects You from Third-Party Attacks

The Cost of a Data Breach Report shows that 83% of organizations studied have had more than one data breach.

Zero trust covers not just insiders, but also third-parties. It follows the least-privilege principle—giving them only the information needed, when it's needed.

5

Zero Trust Continuously Verifies Identities

Continued verification ensures that access isn't possible unless it is explicitly granted. And any access that is granted is continually monitored. Managing all users, devices, things, and services in this way reduces the overall risk to your organization and enables you to answer this question at all times: **who is doing what, where, and why?**

6

Zero Trust Understands Your Identities

Zero trust doesn't just control access—it notices what people do with it. By recognizing patterns, it distinguishes real threats from noise, resulting in faster detection and fewer false alarms.

7

Zero Trust Give You Complete Visibility and Control

Centralized identity management enables you to view and manage your organization's risk profile through a single pain of glass. You can tweak policies for any group, all from one location, and changes are automatically synchronized and enforced.

Security Built for Digital Transformation

By 2022, 80 percent of new digital business applications used by ecosystem partners will be accessed through zero trust systems. In today's multi-cloud, multi-device environment, stronger security is no longer an option. It's a necessity. It's time to take charge of your company's safety. It's time for zero trust.

About NetIQ

Zero Trust is part of an overall digital transformation. As organizations move to the cloud and incorporate IoT, they can also make the switch to zero trust. Doing so will deliver an enhanced security level to the ecosystem and even cover legacy technologies as they transition.

Identity and Access Management is the place to start to achieve Zero Trust. Our purpose at NetIQ is to help organizations protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. In other words, we help our customers achieve zero trust.

NetIQ

Learn more about NetIQ ›

CyberRes