SYNCDOG

Zero Trust – The Need for Zero Trust Is Driving Mobile Security Specialization

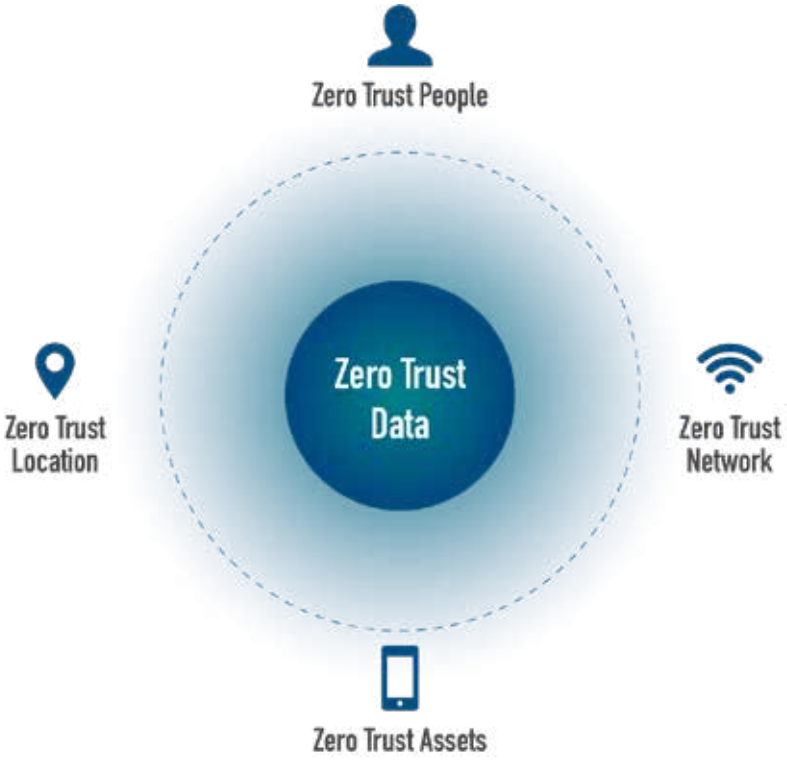
Enterprises have been trudging down the path toward a zero trust security model for a couple of years now, but the proliferation of mobile devices and remote work—and the risks associated with them—now has them sprinting toward the right solutions. The use of mobile devices is steadily growing, telework is increasingly common and mobile threats are becoming the biggest factor in the security landscape.

Aware of the threats, enterprises now see the need to shift their architectures toward a zero trust model, which is driving specialization within the mobile security and mobile device management markets. Companies are seeking an avenue where they can adequately secure and manage their employees' devices with one comprehensive solution.

Moving to a zero trust architecture can seem like an intimidating prospect, since it represents such a significant break from the traditional methods of security that have guarded networks for decades. But with the right platform and mobile security tools, the shift to zero trust can be a fairly simple step. Making the move should start with understanding the reasons for adopting a zero trust model in the current mobile landscape, and knowing what to look for in a solution that can help zero trust become a reality.

The Growing Mobile Threat

The traditional approach to protecting the network perimeter simply doesn't cut it anymore because so much of an organization's business takes place outside that perimeter. Mobile devices, remote work arrangements — accelerated by the COVID-19 pandemic—and an ever-expanding cloud infrastructure have stretched the environment well beyond the point where antivirus, intrusion detection and other traditional methods can be effective. And attackers have followed the data.



Corporate data is constantly being accessed outside of the perimeter of secure networks, putting that data and networks at risk. Verizon's Mobile Security Index 2021 found that 60% of respondents consider mobile devices their organization's biggest security risk. And although most expect the rate of remote work to fall from last year's highs once the pandemic subsides, 78% still say that remote work will remain more common than it was pre-COVID. Remote, mobile access is here to stay.

With enterprises outgrowing the traditional network perimeter, the focus of security has shifted from guarding the castle walls and gates to ensuring that the identities of people and devices accessing the network are who and what they say they are, and that they are authorized to access the resources they're connecting with. Organizations have implemented various identity and access management (IAM) solutions to track and manage both human and machine identities, then combined that with role and entitlements driven workflows that are all secured with advanced data encryption solutions, with the eventual goal of implementing a zero trust model.

Elements of Zero Trust

Zero Trust, as its name suggests, doesn't assume that a user or asset is trustworthy based on its location in the network or asset ownership (such as an enterprise owned or personal device), but instead seeks continuous authentication and authorization of users, devices and resources. It brings cybersecurity to a dynamic level that reflects the mobile, cloud-based environment. A zero trust architecture provides the framework, using zero trust principles to allow organizations to plan their enterprise workflows. It will allow an authenticated user access, but even then, only to the minimum resources they need to do their job. So if a device is compromised, the zero trust model can limit the damage.

A zero trust architecture for mobile devices should include several key features, including:

Mobile Device Management

Mobile Device Containerization

Mobile Threat Defense

Private App Store

Adopting a zero trust architecture is a critical step for enterprises in a mobile, cloud-based environment where traditional network boundaries have been obliterated. But making the transition doesn't have to be too onerous of a job. A lightweight, end-to-end security platform that encrypts data both in transit and on the device, authenticates and controls access of the users, provides a full array of protections against malware, phishing and other attacks, and enforces mobile security policies, all managed within a single console, can help make zero trust a reality even for any organization.

SYNCDOG

+1.855.SYNCDOG (1-855-796-2364)
info@syncdog.com

1801 Old Reston Ave, Suite 301
Reston, VA 20190