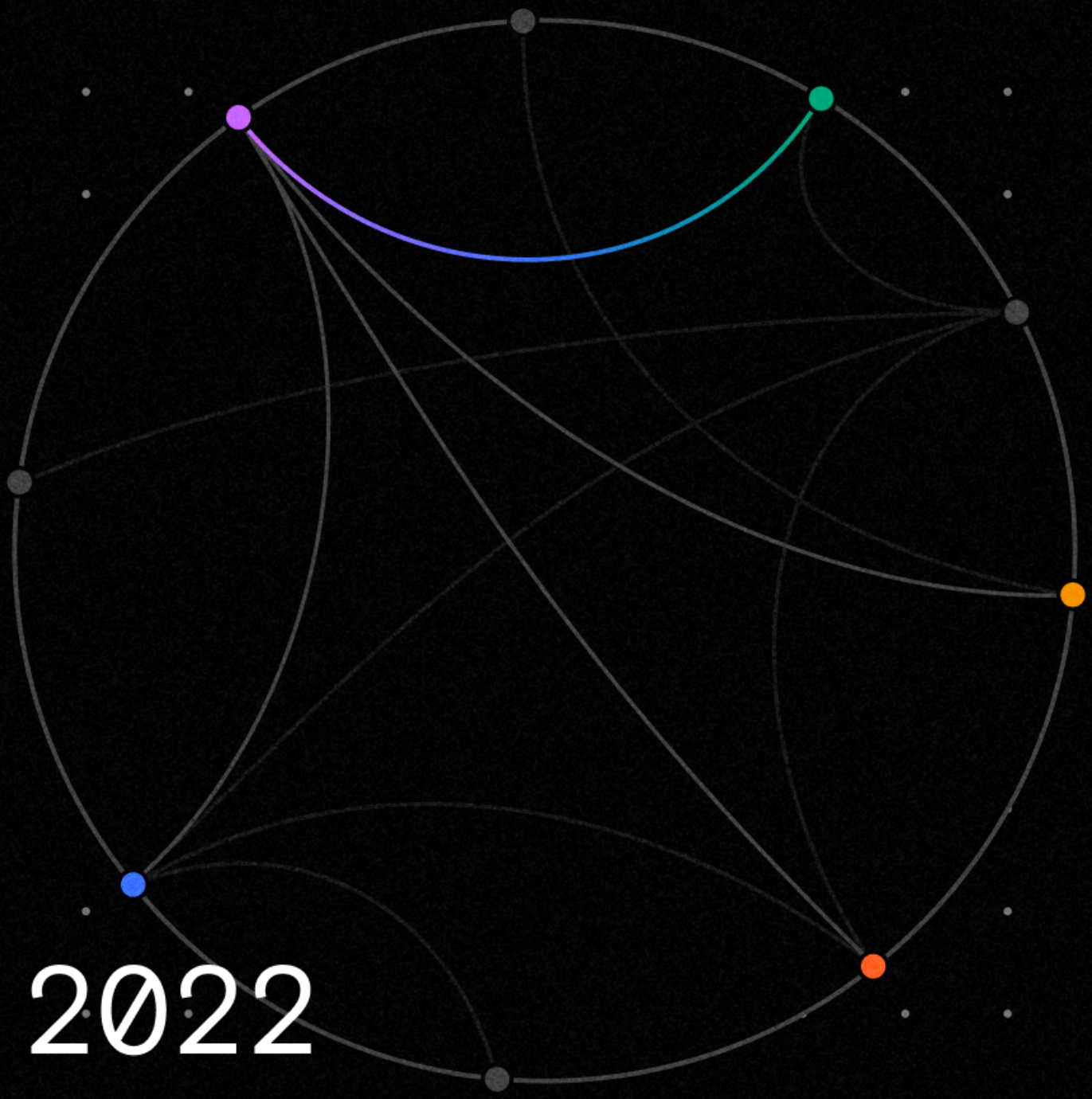


2022 Zero Trust Outlook Report

Twingate

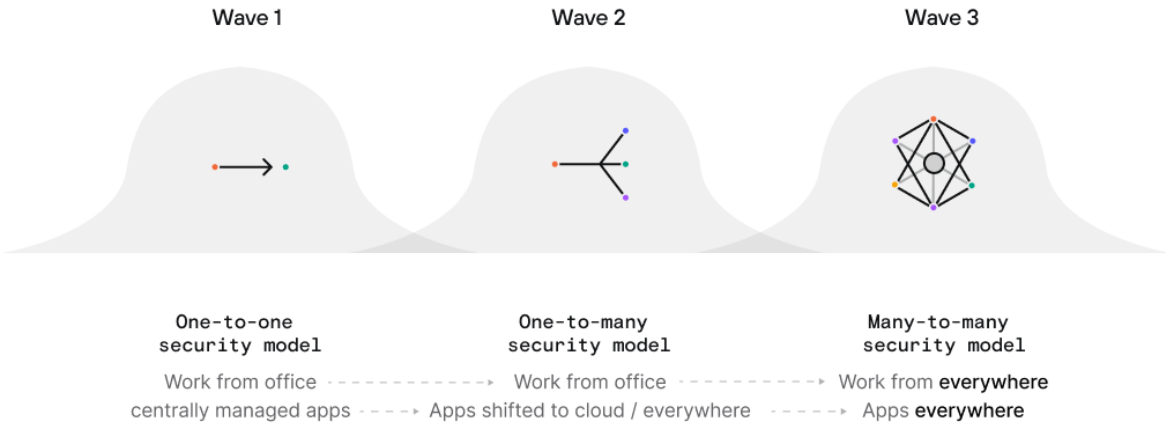
March 2022

2022 Zero Trust Access Outlook

Traditional network security models have fallen by the wayside. The original network perimeter model is no longer sufficient to protect organizations from threat actors as work is no longer inherently office-centric, and apps, cloud-based services, and BYOD are now commonplace. Today, following a rapid push by many organizations to adopt remote and hybrid environments, one thing is clear: network perimeter walls are disappearing, and distributed teams are here to stay. As a result, Zero Trust is becoming a cost of entry for the future of networking and cyber security.

As an architecture and a set of principles, Zero Trust offers a path towards securing a world that supports distributed workforces, a blended network perimeter, and does not make assumptions about access to resources. Zero Trust means there is no implicit trust, and security models start at a baseline of zero, and through granular access controls, device posture, and context, trust is established.

At its core, Zero Trust is a framework that answers a simple question: **Should this user on this device under this context access this resource?**



Zero Trust by the Numbers

Cyber incidents have surged over the last two years, and organizations of all sizes have been impacted. In IBM's annual Cost of a Data Breach report, they assume that threat actors are already within an organization's network. They found that organizations that have yet to adopt Zero Trust at any level have an average data breach cost of $5.04 million. However, the average cost is $3.28 million or $1.76 million less for organizations that have adopted Zero Trust in a mature state. While Zero Trust is not a silver bullet, it may prevent lateral movement in the event of a breach and can dramatically reduce an organization's attack surface.

U.S. Government's Push to Zero Trust by 2024

On January 26, 2022, the Office of Management and Budget (OMB) released the *Federal strategy to move the U.S. Government toward a Zero Trust approach to cybersecurity*. As part of the announcement, U.S. federal agencies have 30 days to select a point of contact to lead these efforts and 60 days to deliver a plan to identify how each agency will achieve set goals by the fiscal year 2024. Among their initial goals are to move on-prem software to cloud-accessible apps and ensure MFA is in place.

Private Sector's Approach to Zero Trust Adoption

Twingate has observed two primary entry points to Zero Trust for most private organizations: multi-factor authentication (MFA) and secure access. In particular, MFA through identity providers (IdP) is becoming the norm, and many organizations have rapidly adopted solutions in the past two years.

IdP adoption supports increased remote work, which has led to historically high levels of phishing attacks that can transform into more devastating ransomware events. Secure access replaces the standard virtual private network (VPN) due to its limited capacity to support remote workforces and the inherent trust it gives to users. Like IdP, Zero Trust Network Access (ZTNA) or software-defined perimeters (SDP) offer granular controls that limit post-breach lateral movement, effectively minimizing the damage a threat actor can do to a network.

Zero Trust in the Future

Zero Trust is more than a buzzword — it represents a complete paradigm shift of how we view security. The rapid year-over-year adoption of Zero Trust makes it clear that organizations see it as an alignment with our current and future work environments. We anticipate seeing continued alignment between organizations and security vendors to refine Zero Trust models and make adoption easier.

About Twingate

Twingate provides a secure access platform that replaces or augments legacy VPNs with a modern Zero Trust Network Access (ZTNA) solution that combines enterprise-grade security with a consumer-grade user experience. It can be set up in less than 15 minutes and integrates with all major cloud providers and identity providers. Twingate helps companies move towards a Zero Trust architecture by tying every network event to an identity—user, device, and service—giving businesses unparalleled control and visibility over activity across their entire network.

Twingate is delivered as a software-as-a-service (SaaS) product, with downloadable software components that are installed on end-user and other devices.

Contact Us

Twingate Inc.

541 Jefferson Ave, Suite 100

Redwood City, CA 94063

USA

Online

www.twingate.com

sales@twingate.com