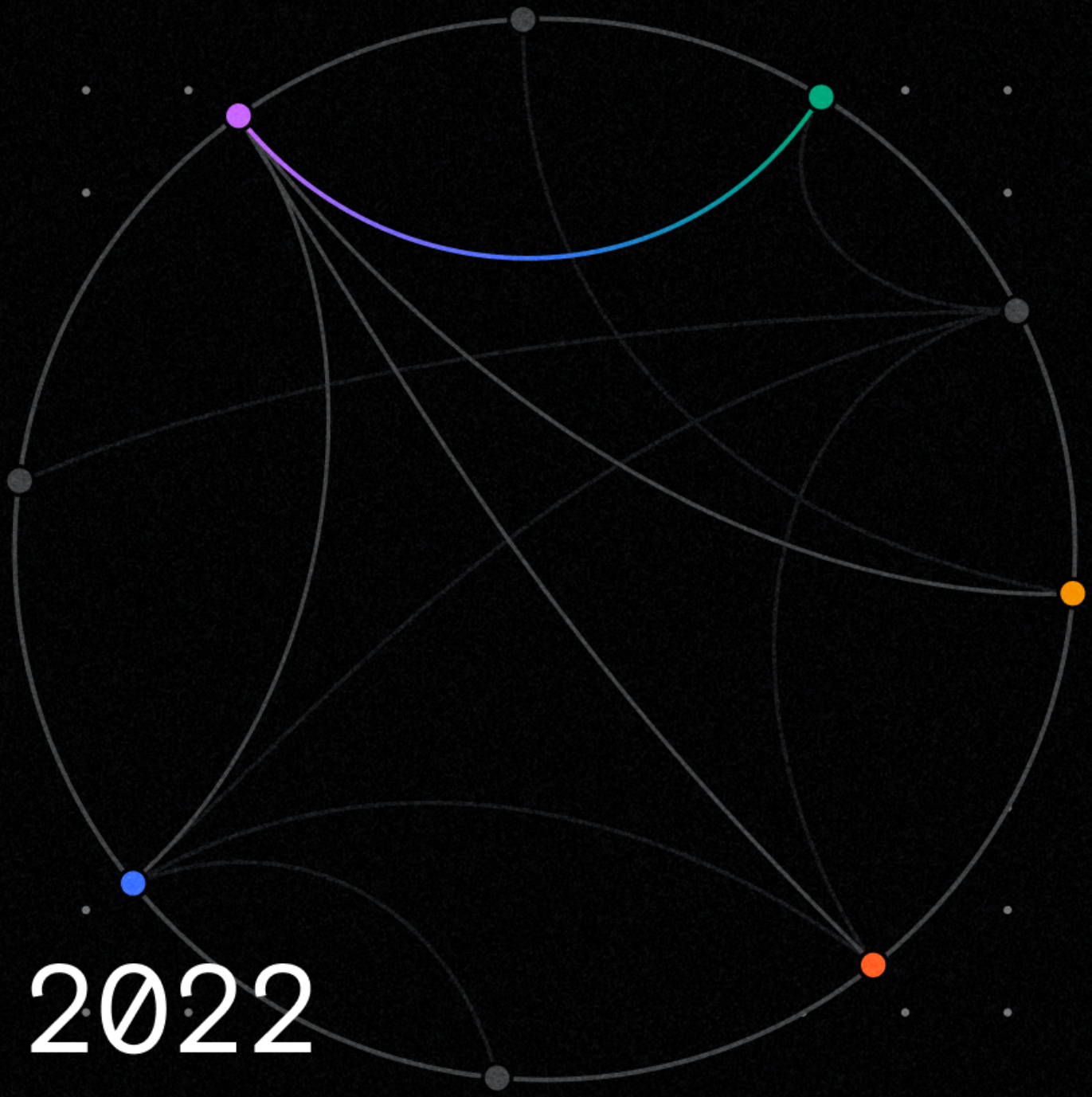


2022 Zero Trust Outlook Report

Twingate

March 2022

Intro

For the past decade, Zero Trust (ZT) has evolved from a mere concept into a trusted architecture adopted by some of the fastest-growing organizations worldwide. At its core Zero Trust is a simple framework that answers the question: should this user on this device under this context access this resource? 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 broad assumptions about who or what should have access to data.

NIST defines Zero Trust and Zero Trust Access (ZTA) as:

> A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
>
> Zero Trust Access (ZTA) is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.[1]

Of note, nothing explicitly states that users and machines can't be trusted; however, trust must be earned and verified frequently.

In 2022, several years into a global pandemic that rapidly pushed organizations to adopt remote and hybrid environments, Zero Trust is becoming table stakes for the future of networking and cyber security. In this brief white paper, we highlight how Zero Trust is changing, what is pushing the concept forward, why the U.S. federal government is adopting it, and the road organizations are taking to implement it as a strategy.

[1] The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207

Zero Trust By the Numbers

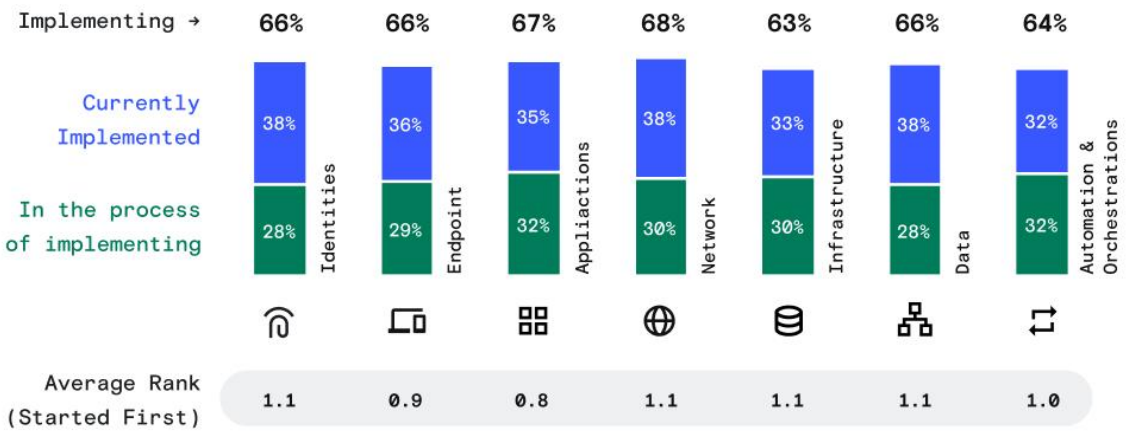
Zero Trust has been around for more than a decade in concept, but it has only begun seeing proper adoption over the past five years. Because of this, related research, success stories, and metrics are still budding; however, we've captured some of the latest industry trends to depict a greater picture of Zero Trust adoption and where organizations are getting started.

Priorities and Entry Points

According to Microsoft's *Zero Trust Adoption Report*, seven key areas drive organizations to pursue a Zero Trust strategy. Interestingly enough, their surveyed respondents identified that there was no single entry point to form a trend. Instead, current priority projects set for enhancement open the door for a Zero Trust strategy in place of a purely technology-based approach. This also shows the importance and maturity that Zero Trust adoption brings to the table and why it requires a top-down approach that spans multiple teams (IT, DevOps, security, etc.).

According to the 2021 report, Microsoft found that identities, the network, data, endpoints, apps, infrastructure, and automation and orchestration are the critical entry points for Zero Trust adoption.

Current Zero Trust Implementation - Security Risk Areas



Reducing the Average Cost of a Breach

In IBM's annual Cost of a Data Breach report, they make the assumption that threat actors are already within an organization's network. With that in mind, 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 this reinforces that Zero Trust is not a silver bullet, it indicates that preventing lateral movement in the event of a breach can dramatically reduce an organization's attack surface.

Security Maturity

As Zero Trust is still relatively young in regard to cyber security strategies, there are not many well-documented maturity models for it. In 2021, Cybersecurity and Infrastructure Security Agency (CISA) released a draft model for comment, which is now being finalized and is highlighted in a later section. However, data shows that forward-thinking security teams tend to align with Zero Trust

According to IBM's *2021 Cost of Data Breach 2021 Report,* "Those who have deployed zero trust tend to be in the middle or mature stages of deployment. Of respondents that have fully or partially or fully deployed zero trust, 14% are in early-stage deployment, 38% middle stage, and 48% mature stage. This means just 16.8% of organizations in the study have a mature stage zero trust approach (i.e., 48% of the 35% of respondents that have deployed zero trust)."

Rapid Rush to Remote Work

So what is driving the most immediate need for Zero Trust? This year, the U.S. Federal Government released their Zero Trust strategy to be implemented over the next few years, which will act as a catalyst, but the primary factor is the push to remote and hybrid work.

According to an UpWork survey, "in eight years, it's predicted that 73% of all teams will include remote employees. And, by 2025, their report predicts 36.2 million workers or 22% (an increase of 87% over the past three years) of U.S. workers will be fully remote. Not only does this confirm what we already know about the evolution of remote work, but it also shows that telecommuting will become acceptable in an even wider range of industries."

Today, only about 16% (according to Owl Labs) of all global companies are fully remote; however, each week, there is a new headline with companies such as Salesforce moving to fully remote teams while companies like Google continue to push out their return to the office. Unfortunately, this does create new challenges for IT and security teams. According to OpenVPN, 54% of IT professionals consider remote workers to pose a greater security risk than traditional workers.

Zero Trust Adoption

The reasoning for rapid Zero Trust adoption is clear: network perimeter walls are disappearing, and distributed teams are here to stay. According to Microsoft's report, "82% of companies implemented Zero Trust strategies within the past three years, with 21% doing so in the past 12 months."

That is a significant uptick in adoption spurred by the pandemic, and the U.S. Federal Government's push to a Zero Trust strategy by 2024 will only further invigorate it. However, of the 82% of companies already pursuing ZT, it's still a much smaller percentage of the pie. Today, only 35% of organizations have partially or fully implemented their Zero Trust strategy, with 65% saying they have not started. According to Microsoft's Zero Trust Adoption Report:

> "Security decision-makers (SDMs) say developing a Zero Trust strategy is their #1 security priority, with 96% stating that it's critical to their organization's success. The primary motivators for adopting a Zero Trust strategy are to improve their overall security posture and the end user experience. The shift to a hybrid workplace, accelerated by COVID-19, is also driving broader adoption of Zero Trust strategy: 81% of enterprise organizations have begun the move toward a hybrid workplace, with 31% fully there. However, 94% have concerns about transitioning, chiefly, employee misuse, increased IT workloads, and cyberattacks. Given this, key considerations for a strategy include increased training for employees and multi-factor authentication (MFA) to ensure a smooth user experience and transition."

This data is further backed by Statista's report that shows 30% of organizations have already begun implementing their Zero Trust plans, with 42% noting it as a priority in the next few years.[2] However, the latest major announcement on Zero Trust adoption goes to the U.S. Federal Government, which recently released its strategy for all agencies to adopt it by 2024.

---

[2] Statista Zero Trust adoption survey 2021

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.

In short, the strategy and memo kick off the initial steps towards a significant digital transformation that requires top-down changes, from policies to tools, and will impact every employee that works with the federal government.

According to OMB's *2022 Zero Trust strategy*, "Moving to a zero trust architecture involves changes to nearly every aspect of an enterprise's security posture. As a result, this strategy necessarily touches on a large number of enterprise security practices, which can intersect with other existing OMB policies."

For the private sector, this case study validates the role Zero Trust will play in the future of the connected world, especially as network perimeters become even more blended.

The strategy builds upon the White House's *Executive Order on Improving the Nation's Cybersecurity* released in May 2021, and the Cybersecurity & Infrastructure Security Agency's (CISA) existing Zero Trust maturity model and resources. The finalized strategy comes after an open comment period that was first introduced in September 2021 and was released as a memo titled *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* on January 26, 2022.

OMB loosely defines Zero Trust with the following statement: "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access." This aligns with Twingate's approach, which is that trust is not inherently given just because a device is connected to a particular network. Instead, granular access management and continuous authentication, down to the device level, are necessary to establish trust.

There are several common themes throughout OMB's Zero Trust strategy, such as pushing agencies towards MFA and not relying on SMS 2FA, moving towards identity-first networking vs. IP-based authorization and monitoring, continual verification and authentication, and a push towards making applications accessible securely on the public internet.

Push Towards Internet Connected Applications

One of the more relevant areas of OMB's Zero Trust strategy is the push to make applications internet-accessible. Today, many organizations still rely on on-prem resources, which doesn't align with the work from anywhere world we live in. While some organizations have looked towards virtual private networks (VPN) as a solution, they too were not designed for a hybrid or remote workforce. To truly move towards Zero Trust, OMB has tasked all agencies to make at least one application that is not currently accessible via the internet, accessible via the public internet within the next year by following a Zero Trust approach. Here is the specific request from OMB:

> Making applications internet-accessible in a safe manner, without relying on a virtual private network (VPN) or other network tunnel, is a major shift for many agencies that will take significant effort to achieve. As with all large-scale IT modernization efforts, its chances of long term success will be improved by beginning with an agile approach.
>
> To catalyze this work and facilitate early identification of obstacles, each agency must select at least one FISMA Moderate system that requires authentication and is not currently internet-accessible. Then, within a year of the issuance of this memorandum, the agency must take the actions necessary to allow secure, full-featured operation of that system over the internet.
>
> Accomplishing that task will require agencies to put in place minimum viable monitoring infrastructure, denial of service protections, and an enforced access-control policy. While implementing those elements, the agency should integrate this internet-facing system into an enterprise identity management system, as described in the Identity section above. Agencies will likely find it beneficial to gain confidence in their controls and processes by performing this shift first on a FISMA Low system before attempting to meet the requirement of doing so for a FISMA Moderate system.

Through this approach, OMB is pushing agencies to adopt Identity and Access Management (IAM), Identity Provider (IdP), and Zero Trust Network Access (ZTNA) models in place of VPNs and other dated concepts.

OMB Zero Trust Strategy Goals

If you've looked over or already begun implementing Zero Trust, OMB's goals (below) for implementing Zero Trust by 2024 should look familiar. Their approach aligns with the core elements that build towards a successful foundation, starting with what we refer to as identity-first networking. Following that up with device-related security, OMB's initiatives will help prevent vulnerable devices from accessing data and resources that would otherwise be granted in a standard architecture or those securing the perimeter via a VPN.

OMB's Zero Trust adoption goals:

1. Identity: Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.

2. Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices.

3. Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.

4. Applications and Workloads: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports.

5. Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

As agencies move towards Zero Trust adoption, we'll likely see a snowball effect where private organizations rely on these models to pursue the same. NIST, for example, offers several threat intel and threat response models which are now widely accepted, in collaboration with open standards that are currently being developed from the likes of Cloud Security Alliance, MITRE, and OASIS.

The Road to Zero Trust Implementation

As a concept and strategy, Zero Trust requires a digital transformation and impacts the entire organization. Because of this, there are several processes and milestones that lead to adoption. In the past year, CISA has helped define what this journey looks like and developed the Zero Trust Maturity Model draft.

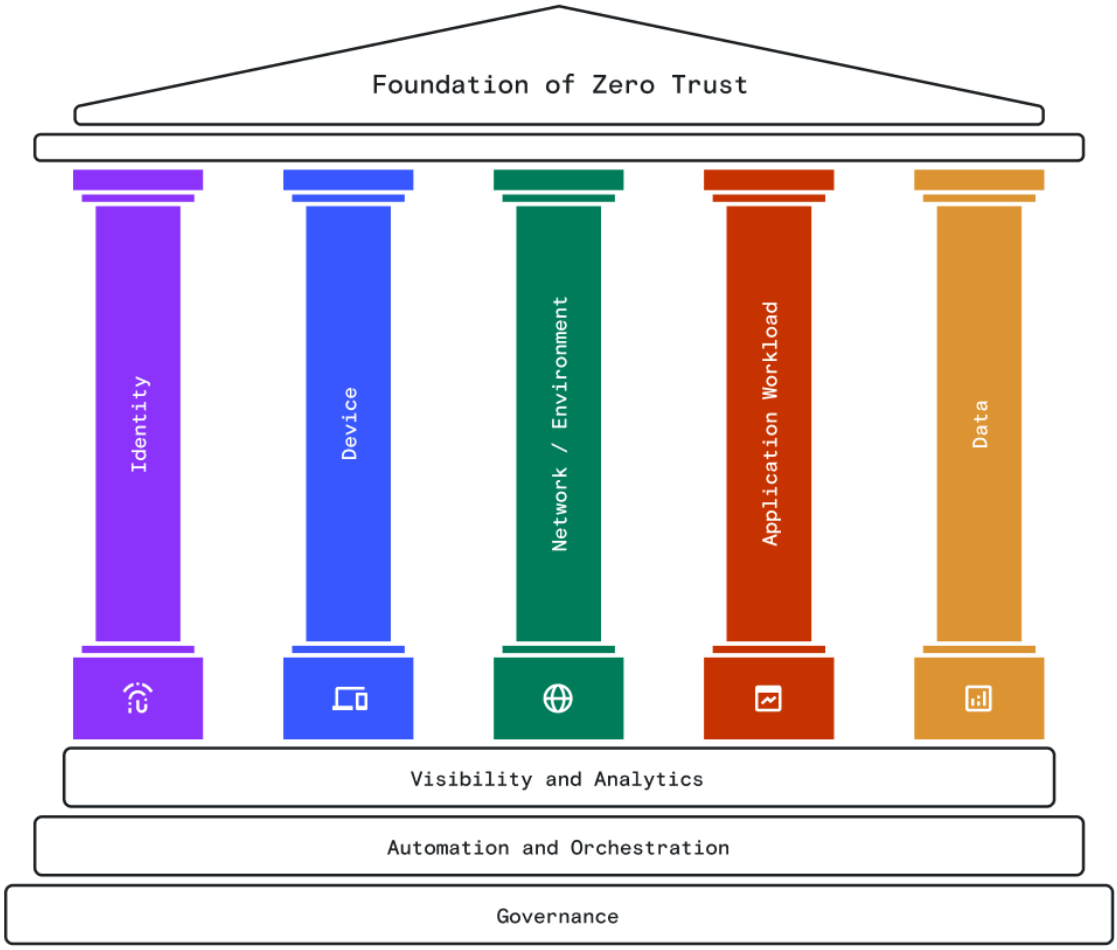
CISA, an agency under the Department of Homeland Security (DHS), is prioritizing Zero Trust in response to the increase in cyber threats and attacks.

> "Recent cyber breaches have had wide-ranging implications and demand a federal response. Cyber defense requires greater speed and agility to outpace our adversaries, substantially increased costs and risks to threat actors, and the durability and resiliency to recover immediately. These compromises demonstrate that "business as usual" approaches are no longer acceptable for defending the nation from cyber threats, and new requirements hold CISA responsible for defending the.gov in clearer, more sophisticated and risk-informed ways."

CISA also notes the primary challenge to Zero Trust adoption, which many enterprise organizations face, is that their existing infrastructure and network have been built around the idea of inherent trust. Depending on the entry point, this could mean rebuilding and reworking systems (moving on-prem to the cloud), and in others, it's finding a solution that offers an easy button towards adoption-Zero Trust Network Access (ZTNA) or software-defined perimeters (SDP), for example.

According to NIST, they suggest the following initial guidance towards transitioning to Zero Trust: 1. Identify Actors on the Enterprise. 2. Identify Assets Owned by the Enterprise. 3. Identify Key Processes and Evaluate Risks Associated with Executing Process. 4. Formulating Policies for

the ZTA Candidate. 5. Identifying Candidate Solutions. 6. Initial Deployment and Monitoring.



Following NIST's guidance, CISA refines this further by highlighting the need for improved governance, automation and orchestration, and visibility and analytics. These three areas offer the foundation the federal government is using to adopt zero trust. They have multiple-cross pillars, much of which mirrors what private organizations are prioritizing in their adoption journey, according to Microsoft's Zero Trust Adoption report.

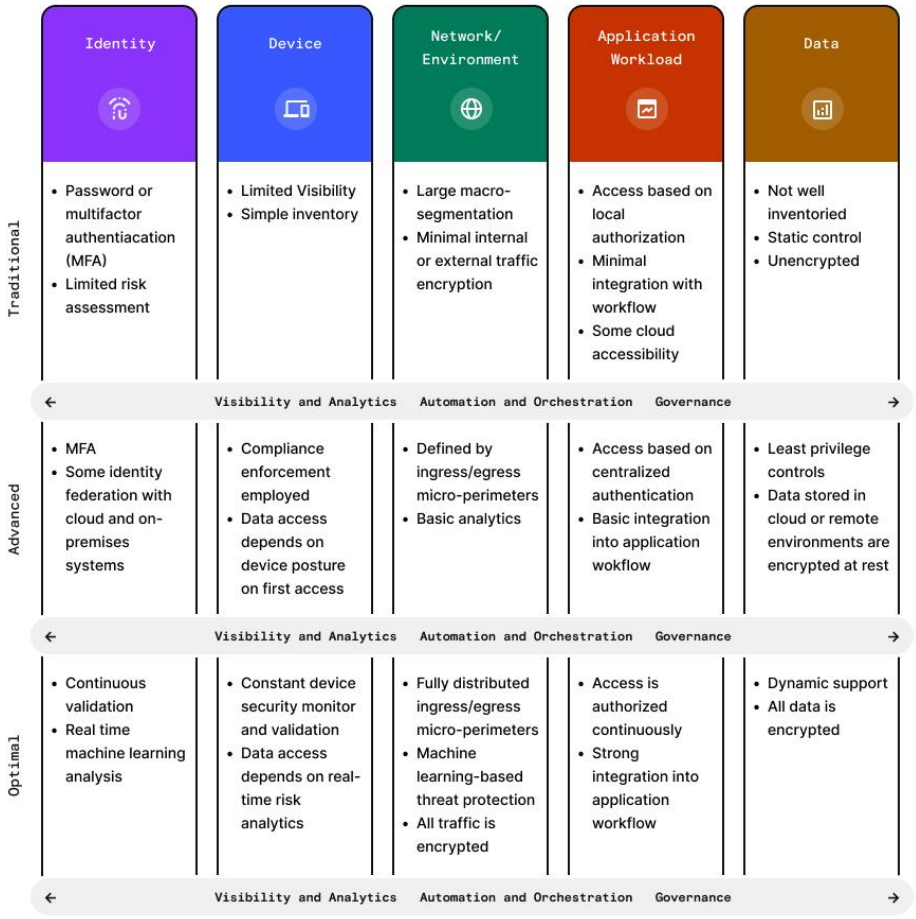
CISA's Three Stages of Zero Trust Maturity

With a foundation of processes, device inventories, and risk assessments, CISA suggests a three-stage maturity model that balances cost, effort, and an increasing level of protection.

Traditional – manual configurations and assignment of attributes, static security policies, pillar level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response, and mitigation deployment.

Advanced – some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to predefined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments.

Optimal – fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with historian functionality for point-in-time recollection of state.



Private Sector's Approach to Zero Trust Adoption

For most private organizations, there are two primary entry points to Zero Trust that Twingate has observed: 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 is due to increased remote work and historic highs for phishing attacks leading to ransomware attacks. Regarding Zero Trust, forward-thinking organizations are also moving to solutions with more granular access controls for an identity-first approach, making user analytics more human vs. the IP tracking counterpart.

On the other hand, secure access is replacing the common virtual private network (VPN) due to its limited capacity to support remote workforces and the inherent trust it gives to users. Zero Trust Network Access (ZTNA) or software-defined perimeters (SDP), like IdP, offer granular controls that limit post-breach lateral movement. These two approaches also function in tandem and lead towards application in threat hunting, automation, data encryption, and moving applications to the cloud.

Zero Trust in the Future

This report explores the current state of Zero Trust, and identifies why organizations are seeking to adopt the approach. 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. Over the following years, we'll continue to see organizations like NIST, CISA, OASIS, Cloud Security Alliance, and others jumping in to refine these models, making it easier to adopt Zero Trust, and security vendors better aligning with these needs.

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

support@twingate.com