CISCO
SECURE

Cisco's Guide to Zero Trust Maturity

How to find quick wins

cisco SECURE

Table of Contents

I. Executive Summary

Zero trust has evolved from being a buzzword to becoming an international mandate. Governments such as the United States, the United Kingdom, and Australia have all announced requirements consistent with a 'never assume trust, always verify' stance.

Business leaders adopting zero trust are making solid progress towards building security resilience for their organizations. In fact, Cisco customers have decreased the risks and costs of a data breach by nearly half, and others have achieved a 191% ROI by enabling hybrid work and optimizing the security team's performance.

By driving efficiencies, zero trust can accelerate a SOC team's response – we have been able to deliver a 90% increase in SOC efficiency for our customers. Clearly, zero trust can deliver value.

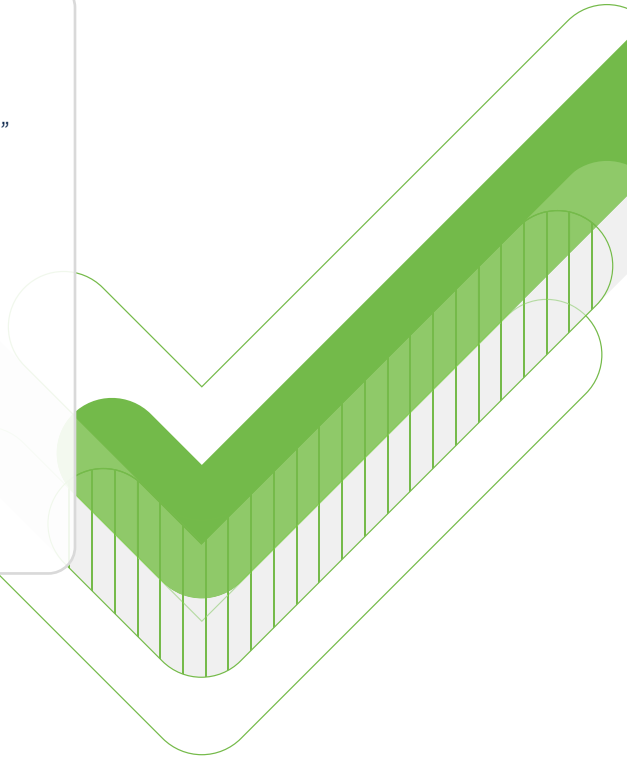
That said, confusion still exists in how to implement the zero trust principles in ways that are consistent with material business benefits. And yet, many enterprises, including Cisco, have made measurable progress towards adopting zero trust security with material rewards as proof.

So, what's different about these organizations? What are the secrets to their success?

About the data used in this guide

We used findings from the Cisco Security Outcomes Study, Volume 2, an independently verified report that seeks to answer the question "why" certain security practices are so successful. The study interviewed 5,000+ active IT, security, and privacy professionals from 27 countries, across various industry sectors to discover what can improve security capabilities and outcomes.

Cisco has also been organizing regular Zero Trust Workshops to help attendees understand the zero trust adoption journey, engage in hands-on activities, perform a gap analysis and develop an action plan. To date, there have been ~3000 IT and security leaders as well as practitioners who have registered for these workshops. This guide calls out the survey responses we have received from these workshops.



We leveraged field data collected and analyzed by the team that brought you the Cisco Security Outcomes Study, Volume 2, as well as the responses from the attendees of the numerous Zero Trust Workshops that Cisco has organized in the past year.

Figure 1: Respondent progress on zero trust adoption

Some of the findings from the data we collected provide insight for teams pursuing zero trust:

- **Zero trust progress can be achieved no matter the size of an organization or the level of complexity in the IT infrastructure.** Across the spectrum of simple to complex IT environments, we discovered that organizations, large or small, can make measurable progress towards zero trust security.
- Organizations that reported a mature implementation of zero trust were more than **twice** as likely to achieve **business resilience** (63.6%) than those with a limited zero trust implementation.
- Organizations that achieved mature implementations of zero trust were **twice** as likely to report excelling at the following five **security practices**:
  - Accurate threat detection
  - Proactive tech refresh
  - Prompt disaster recovery
  - Timely incident response
  - Well-integrated tech
- Organizations that claimed to have a mature implementation of zero trust were **2X** more likely to report excelling across desired outcomes such as **greater executive confidence** (47%), **peer buy-in** (45%), **keeping up with the business** (46%) and **creating a security culture**.
- Organizations with **modern IT infrastructure** are **more than twice** as likely to have a mature implementation of zero trust.
- **Integrations drive zero trust maturity**. And even within organizations that chose integrations, a platform approach of sourcing **integrated technology from a preferred vendor** was prioritized by **51%** of organizations with mature implementations of zero trust compared to out-of-the-box integration at **28.8%**.
- Organizations with mature zero trust implementations leverage **automation** (64.4%) in order to improve the actions a zero trust security model can take.

This guide to zero trust maturity is designed to help you determine where you are today with zero trust, how to find the quick wins, gain momentum, and continue to make progress towards zero trust security.

II. Introduction

Zero trust is here to stay. But why is it so challenging? And where can teams gain momentum for what feels like such a Herculean task?

We believe that organizations can learn from teams who have achieved more mature implementations of zero trust. What are their secrets? What do they do that we can share with the rest of the world?

Specifically:

1. What security outcomes do successful teams achieve and at what success rates?
2. What do they prioritize when selecting zero trust vendors and providers?
3. What is their integration and automation strategy for deploying zero trust?
4. Which zero trust standards do they align to?
5. To what degree have they automated their security processes?

III. What is Zero Trust?

Zero trust is a **strategic approach** to security that centers on the concept of **eliminating implicit trust** from an organization's environment.

Trust is neither binary nor permanent. We can no longer assume that internal entities are trustworthy, that they can be directly managed to reduce security risk, or that checking them one time is enough.

The zero trust model of security prompts you to **question your assumptions of trust** at every access attempt, no matter where it comes from.

A zero trust strategy deploys a "Never assume trust, always verify, and apply least privileged access" policy for every connection request to every corporate resource. Always verifying trust before granting access across your applications, devices, and networks ensures that only those who should have access to the information do.

The responsibility for making and enforcing this determination falls on to policy decision points (PDP) and policy enforcement points (PEP). In fact, it could be argued PDP/PEP is the differentiating architectural feature. These components enforce the zero trust principles and extend or revoke trust boundaries based on what's observable when connecting.

Zero trust is NOT:

- One product or technology, but a security framework
- Something to "buy" or "sell" but an opportunity to position a solution within the framework
- A one-and-done project, but an ongoing effort towards achieving better security

The simple truth is that business moves too fast for security to get in the way. And despite security innovations, risks have never been more impactful. Too often, a single cybersecurity incident can represent an existential threat to an organization's future.

At Cisco, we believe that the promise of a zero trust security strategy should be securing access in a way that frustrates attackers and not users.

A. Why now?

Zero trust is not a new concept. But today's rise in adoption reflects a fast-changing reality: boundaries that once existed to secure access to corporate data no longer exist. Businesses now operate as integrated ecosystems with their suppliers, partners, and customers. These connections expand the attack surface area, increasing risk and complexity, and make it more difficult to recover from attacks.

Because of the impact of cyber-attacks on their bottom line, business leaders are now ready to consider a new way of implementing end-to-end security – guided by zero trust access principles – provided these changes don't impact productivity or operations.

> The stakes are so high and the material impacts so potentially devastating that transformative change is now welcome. Hence the wide acceptance of zero trust security principles.

Zero trust progress can be achieved no matter the level of complexity in the IT infrastructure. Across the spectrum of simple to complex IT environments, organizations can simultaneously make progress towards zero trust while also improving outcomes.

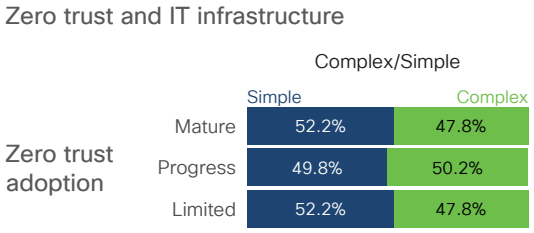


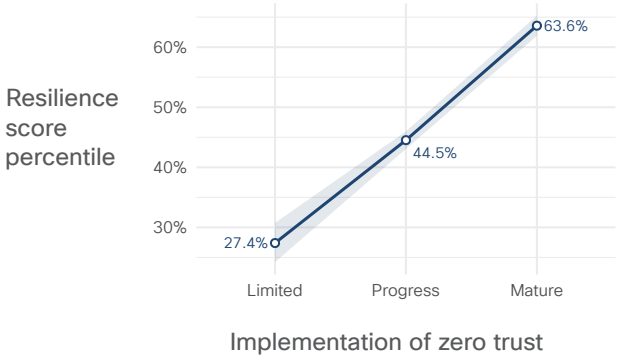
Figure 2: Zero trust adoption across organizations with simple and complex infrastructure

Zero trust can increase business resilience. While zero trust may seem like just another marketing buzzword, the truth is that moving towards a zero trust architecture can secure the entire organization, elevate business performance, and accelerate threat response.

We found that organizations with a mature implementation of zero trust were more than twice as likely to achieve business resilience than those with a limited zero trust implementation.

We created a "resilience score" using 4 of the 12 security outcomes that are particularly relevant to resilience:

- Keeping up with business (security should enable, not impede)
- Avoiding major incidents (and the business impact that ensue)
- Maintaining business continuity (operate even when disaster strikes)
- Retaining talented personnel (can't stay on top when top staff don't stay)



A higher resilience score means better success rates across these outcomes.

The challenge is that organizations don't know how 'to do zero trust' or where to start because of a fear of impacting productivity or endangering business agility and operational resilience.

But the key is to get started somewhere and focus on doing certain things right. We found a clear correlation between mature implementations of zero trust and five security practices that are referred in the Cisco Security Outcomes Study, Volume 2 as the "Fab Five" drivers of security program success:

- Accurate threat detection
- Proactive tech refresh
- Prompt disaster recovery
- Timely incident response
- Well-integrated tech

Organizations that achieved mature implementations of zero trust were twice as likely to report excelling at these five security practices.

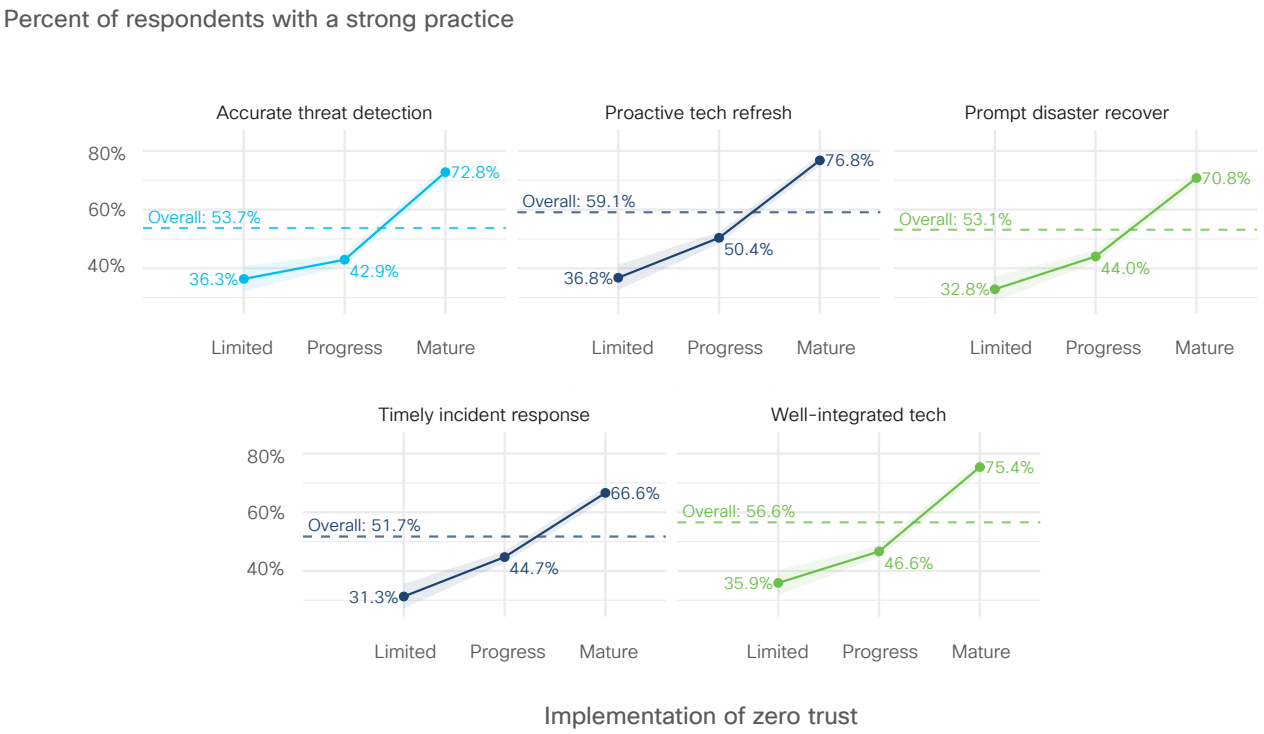


Figure 3: Zero trust adoption level and security practices

Pro-tip: Now that zero trust claims a $20 billion market share (and climbing)[1], it's important to carefully consider a partner who can meet you wherever you are, can integrate across the pillars of zero trust, and has gained progress along their own journey.

[1] According to Grandview Research, the global zero trust security market size was valued at USD 19.8 billion in 2020 and is expected to register a compound annual growth rate (CAGR) of 15.2% from 2021 to 2028. https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

IV. Secrets of the Successful

A. Start with culture

The leading factors of successful zero trust implementations are the ability to get buy-in from the top, support from peers, and build on the security culture. Security teams struggle when they lack the buy-in and budget, and when the security program runs afoul of the culture.

> Nothing stops an initiative quicker than culture push back.

As we see from our own Cisco case study, these factors were all present from top-down leadership and across the organization. The Security Outcomes Study reflects this too, with mature implementations reporting **greater executive confidence** (47%) and **peer buy-in** (45%). We also see corresponding trends in **keeping up with the business** (46%) and **creating a security culture** (48%). In fact, **organizations that claimed to have a mature implementation of zero trust were 2X more likely to report excelling across these areas.**

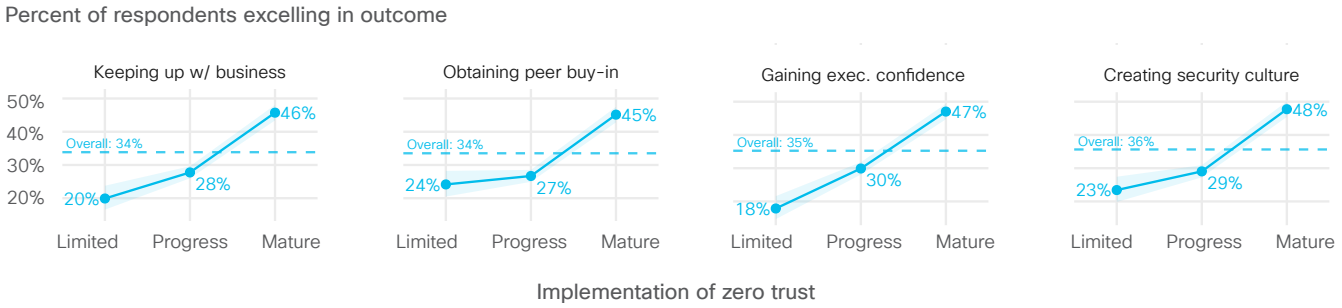


Figure 3: Zero trust adoption level in the context of desired outcomes

Relationships drive organizational change. Before picking up a whiteboard marker and sketching out a plan, and before opening the console and configuring policy, begin by strengthening the relationships between the security team and the executives. This includes peers in IT, networking, architecture, project management, and auditing. These relationships enable us to mature our zero trust programs much faster and therefore realize higher degrees of success – critical factors for transformational change.

Change starts at the top. When we have good support, we have a clearer path forward. When the CEO is calling to make zero trust an initiative, or when our customers are demanding it as part of their supply chain management, it becomes a matter of tying the zero trust initiative to the business. If those things are happening, capitalize on them and use that momentum to push the program forward.

Build a culture of trust. Before we talk about technology, and before we make the business case for zero trust, security leaders need to first work on building the trust and confidence of their peers and executive buy-in. Frame the conversation in a way that's consistent with the organization's culture.

Look to strengthen relationships. When architecting and implementing zero trust, identify ways to bolster these connections. The process of mapping out our workflows, putting in place policy engines, having conversations around what zero trust will mean to the organization, focusing on enabling the business while preventing threats: all these steps strengthen relationships.

As is clearly demonstrated by case studies and the data, these are crucial factors in successful zero trust implementations.

B. Make a strong business case

We have seen in Cisco Zero Trust Workshops, and in the broader market, a clear trend with zero trust initiatives.

Early zero trust projects were pilot programs. Security leaders heard the term and wanted to try it to see what worked and what didn't. These early pilots provided a sense of what it might look in their organization. From 2018 to 2020, there were many zero trust initiatives because of an executive mandate, a customer requirement, or need to modernize.

Shift towards business outcomes. Recently, there's been a clear shift away from making the business case on a standalone zero trust initiative, towards business cases which satisfy a business need while applying zero trust principles. Examples include a remote-first workforce, digital-first customer base, digital transformation, cloud migration and IT modernization. Successful zero trust programs look for opportunities to improve the organization while increasing security at the same time.

Prioritize the user experience. Now, one of the primary focal points of zero trust in business cases is the user experience. This is the trust component of zero trust. Mature programs improve the user experience so that when the workforce is performing normal day-to-day business activities, security is unobtrusive. Security controls should only interrupt when there's actual risk, such as when it's an untrusted connection or where there may be an adversarial action.

Make security more efficient. Another business case consideration is manageability. **The Security Outcomes Study finds that organizations with mature implementations of zero trust report running cost-effectively (47%) while minimizing unplanned work (43%)**. Attendees of Cisco Zero Trust Workshops regularly list tool consolidation as an objective, ranked only behind increasing visibility. Successful organizations reduce the workload to maintain security while increasing their capabilities to protect the organization.

Simply put, the driver for the zero trust business case is to frustrate the attacker, not the user.

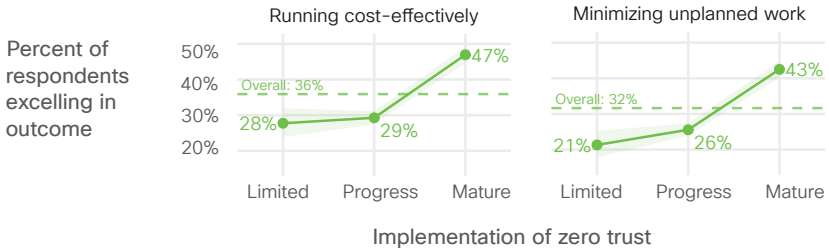


Figure 6: Cost efficiencies of zero trust security

Reduce the attack surface. This is the "zero" component of zero trust: reducing excessive and implicit trust to decrease security risks. What most organizations have in mind are threats such as phishing and ransomware, but more broadly, they are using zero trust to reduce the attack surface.

Leverage the audit. There is increased demand for zero trust by compliance mandates, specifically in the U.S. federal sector. We expect that compliance component will only increase as organizations adopt zero trust and move towards implementing it as part of supply chain risk management.

Bottom line: Business cases must satisfy a business need first, and by satisfying that need, apply zero trust principles to advance security.

C. Secure the IT stack

Zero trust is about creating a dynamic boundary: one that is short-lived, tightly scoped, enforced by policy, and informed by trust signals and telemetry. It's a trust boundary between a subject, typically a person on their device — and a resource, generally an application the person is accessing.

The IT stack needs to support establishing these trust boundaries on a per-session and per-connection basis.

Mature zero trust implementations are more likely to be modern than outdated (68% versus 31.3%) and to be cloud-first than on-premises (46% versus 23.6%). These modern cloud-first stacks offer greater support for the policy demands of establishing per-session and per-connection trust boundaries.

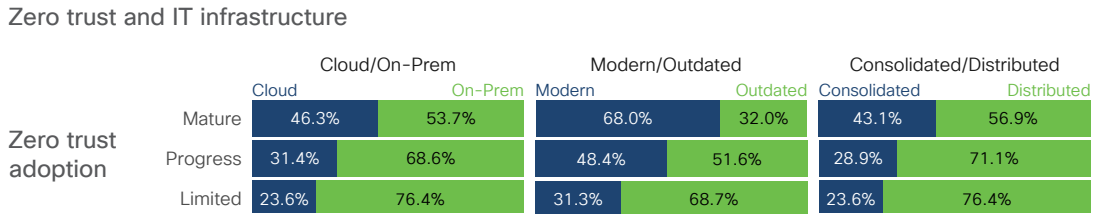


Figure 7: Zero trust adoption in the context of IT infrastructure attributes

Connect the dots. The control points for zero trust include people, devices, networks, application workloads, and data. Distributed, these controls can potentially become silos requiring duplicate work and coordination. It's not surprising, therefore, that the **mature implementations favor consolidated over distributed infrastructure (43.1% versus 23.6%).** It's the principle of economy of mechanism coming alive in the data.

Push those patches. Keeping the environment up to date is a success factor. Zero trust continues to evolve the architecture patterns, standards, protocols for authentication and authorization, and the protocols for shared trust signals.

Organizations with more mature zero trust implementations rely on a vendor-driven strategy for upgrades over proactive upgrades (45.8% versus 30.9%). Rather than waiting for a planned update and having technology stagnant for multiple years in the traditional, multi-year update strategy, relying on SaaS applications which are updated automatically appear to provide organizations with a greater degree of flexibility and policy control over those SaaS apps in the cloud.

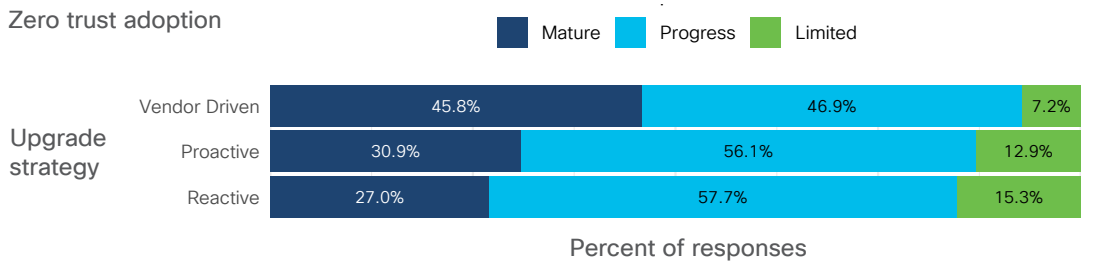


Figure 8: Zero trust adoption level in the context of upgrade strategy

Centralize identities. Organizations with federated identity on a modern tech stack will have an easier path to reach a mature state. However, organizations on the journey towards that stack are uniquely positioned to apply zero trust principles and architecture patterns earlier on in the journey.

No legacy tech left behind. One of the ongoing challenges with zero trust is applying these principles to legacy environments and to edge cases. We see that in a variety of different security controls where the leading edge of the security control is pointed at the leading edge of IT – and that can leave many environments behind.

Bottom line: Much like the transition to cloud, the transition to zero trust will take a hybrid approach mixing legacy and new security models.

D. Start with users, apps, and devices

Zero trust as a security program is aimed at specific use cases. When we look at successful organizations, many of these use cases are present. These include:

- Protecting the workforce
- Application modernization
- Securing Internet of Things (IoT), IT, and Operational Technology (OT) systems

...and providing all the above protection in context such that any is protected and run through a policy engine.

Additionally, there are several other complementary security programs that need to be considered, those that align with zero trust principles. Let's start with the foundational operational domains:

- Identity and access management – who are my authorized users, how do I know, and which resources (think apps) do they need access to?
- Asset management – what are the devices that comprise my IoT, IT, and OT environments? How do I know if they're configured securely?

Getting answers to these questions is not a trivial endeavor.

For example, people attending the **Cisco Zero Trust Workshops** often share having significant difficulties with their identity management program. **74% of attendees reported their organization's identity strategy was undefined, unclear, or somewhat clear.** When we suggest identity is the new perimeter, the lack of identity controls is problematic.

Another area which continues to be challenging for zero trust is asset management programs. **55% of attendees reported no, low, or partial visibility into devices.** The trust boundary is established between a person on their devices and their application. If we don't have that visibility or a good configuration management database, how are we able to provide zero trust?

One possible answer may be to move from thinking of identity and device management as a point-in-time exercise towards an on-demand activity. Something that is done when people authenticate, or something that's done when the device accesses a resource.

By contrast, some security programs that are related to and support zero trust show a great deal of success. **Mature zero trust organizations report better outcomes from their risk management programs (49%)**. These correspond and collaborate to ensure that zero trust is, by policy, enforcing the right risk posture and right risk decisions that are identified through a risk management program.

We also see that **organizations with mature zero trust implementation are correlated with better outcomes for incident response (43%) and business continuity (41%) programs.**

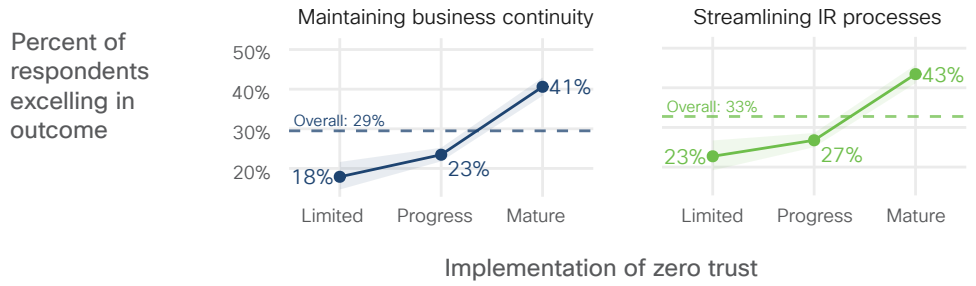


Figure 9: Zero trust adoption level and business continuity and incident response

The emerging theme is combining the zero trust program with other ongoing security programs to achieve better outcomes. Security teams are moving away from traditional manual processes, be it asset management, identity management, or detect-and-response activities. We must automatically act when we see things that are not according to policy when the context and conditions indicate that we should not trust them.

Bottom line: Successful zero trust implementations build on strengths in other programs through collaboration and technical integration.

E. Zero in on zero trust capabilities

Zero trust should bring several capabilities to bear when building out the business case, building out the program, and applying it to a modern tech stack.

Aim high: Analyze, integrate, and automate. Visibility, integration, and automated and orchestrated workflows are the capabilities of zero trust that are present in the 'optimal' range of maturity models and reference architectures. These are the signs to look for and build towards.

Mature organizations are focused on integration. The data reflects an ongoing debate in the industry: Is it better to buy tech with out-of-the-box integrations into their existing infrastructure (28.8%) or is it better to establish zero trust by sourcing solutions from a single vendor so they're natively well-integrated or part of a larger platform (51%)? **Organizations are reporting success with both approaches, which likely indicates an evolving product market.**

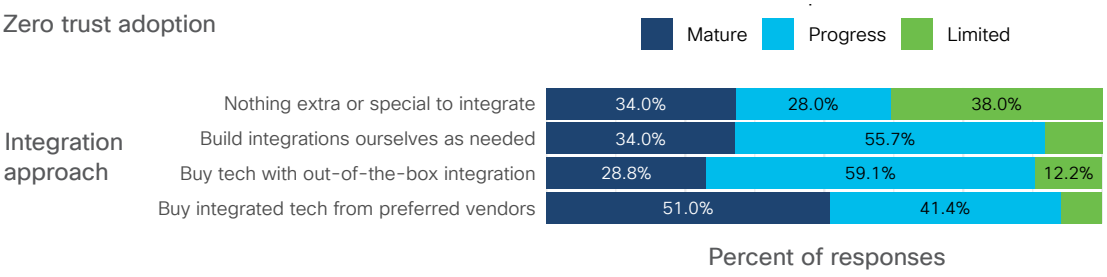


Figure 10: Zero trust adoption in the context of integration strategy

Shared signals drive an informed policy. One way achieve zero trust maturity is to bring a greater degree of integration with other trust signals to **detect** threats, **identify** vulnerabilities, **protect** assets, **respond** to incidents and **recover** operations quickly. In other words, from a policy enforcement perspective, what are we consuming and using to make a trust-based decision? What are the signals we are using and applying to extend that trust boundary? Answering these questions requires well-integrated technology, which mature organizations report at significantly greater levels.

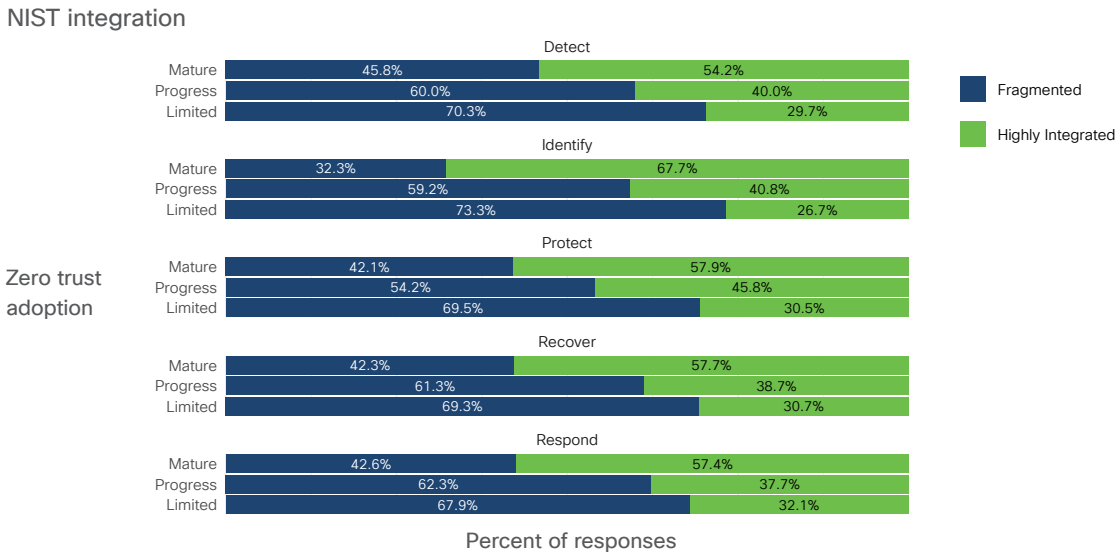
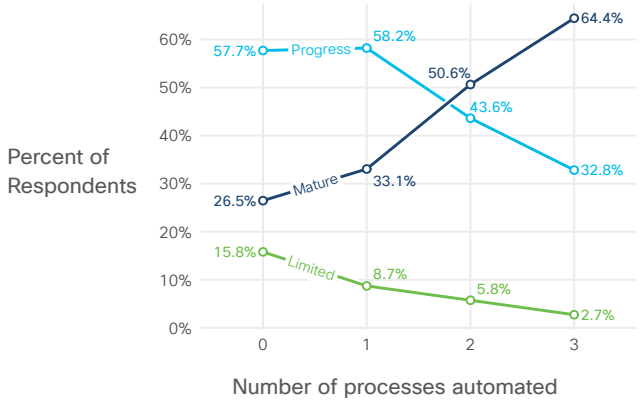


Figure 10: Zero trust adoption in the context of integration strategy

Automation and orchestration make zero trust actionable at scale. As integration improves the policy decision making, automation and orchestration improve the actions zero trust can take. **Mature implementations of zero trust report the highest level of automation across threat monitoring, event analysis, and incident response (64.4%).** These integrations are being driven as policy decisions are made, and as that data is made available for retroactive inspection, or proactive prevention, of an ongoing threat.



The more automation the better. Automation and orchestration can apply to a number of different items such as changing trust boundaries, changing privilege levels, adjusting roles, and adjusting the very context that the identity is operating in, until such a time that the trust is improved.

Figure 12: Orgs with mature zero trust implementations leverage automation

We are seeing that mature implementations of zero trust are reporting a greater number of automated processes, and that reflects this overall theme towards applying orchestration and automation across the board.

Key takeaways: For zero trust capabilities, get the policy in place first as the foundation. Next, ensure visibility across those policy enforcement points. Plan integrations between policy engines and an ever-growing set of trust signals. Finally, increase automation and orchestration to be able to take action on a greater set of environments. Take it one step at a time.

F. Prepare for the journey forward

The concern with describing any security program as a journey, however, is sustaining the executive support and the peer buy-in over a longer term.

It's not a marathon or a sprint: Zero trust programs provide a way to embed security into the way we do business.

Align to business values and priorities. Successful zero trust initiatives have a series of steps which tie the zero trust principles to something of business value, something that's of interest to the executive team and the peers, and something that is of importance to the security function. This delivers the results in a timely fashion.

Leverage reference architectures and project management frameworks. This is a transformation effort and should leverage enterprise architecture and project management. These functions can establish a consistent means of implementing zero trust principles for a variety of environments, with varying identities such as people, services, and devices. Basically, an early first step in establishing zero trust is to establish the governance.

Connect your architecture with your governance. If your organization has a strong enterprise architecture team, one area for them to begin is to establish a reference architecture for zero trust. If your organization has a strong GRC (Governance, Risk, and Compliance) team, begin to work on the progression of applying the principles of zero trust towards guidelines, standards, and eventually codifying in policy. Use Zero Trust Policy Decision Points (PDP) and a Policy Decision Engine (PDE) to determine and enforce the GRC policies.

Establish and communicate key performance indicators (KPIs). We anticipate that effectively communicating zero trust controls to auditors will become challenging without first tying them to governance objectives. The GRC function in an internal audit can get ahead of this by determining how zero trust will be measured and reported, as well as by educating the third party and external auditors about what to expect. This is particularly important for business cases with compliance drivers or customer demands. Determine early how zero trust will be assessed and measured by third parties and socialize it with peers and executives.

Gain momentum from quick wins. Every organization is going to have differing degrees of strengths and weaknesses across their security stack. If you've got a very strong cloud access security broker (CASB) solution, you may have the ability to get a dynamic list of applications. If you've got a very strong single sign-on (SSO) or multi-factor authentication (MFA), you may have the ability to get a dynamic set of device data. What's important is taking your strengths and using that strong footing to gain visibility and contextual awareness.

Visibility is everything. Establishing visibility and setting up those inventory processes is an early quick win. Remember, this should include ensuring that multi-factor authentication and single sign-on are deployed to increase the policy enforcement visibility in those controls. Effectively what we're trying to do here is put the policy engine in place and start getting visibility while we decide what level of policy enforcement we are going to maintain. From there, define the collaboration points to other security programs.

The roadmap to move from "making progress" to a "mature" zero trust implementation

There are three points along the transition from making progress to a mature implementation:		
• The first is the **breadth of the implementation**, which is achieved by increasing the coverage of the controls. For example, having more people enrolled in MFA, having more devices under management, and protecting a greater number of applications.	• Second, **increase the depth of policy**. Leverage the telemetry, the context, and conditions within the policy engine to make better trust decisions. From there, expand the integrations to other security technologies.	• The third aspect of making progress to mature implementation is **increasing automation and orchestration**. What additional steps can we automate and that would happen when we notice there's something not trustworthy?

Bottom line: Zero trust is best implemented as a phased approach, with a series of steps, and those individual steps should be governed as individual security projects.

Each one can offer:

- Wider opportunities to strengthen security relationships and security culture
- Ways to jumpstart long-overdue security enhancements, from identity management to asset management, from incident response to disaster recovery
- Cost effective, well-integrated, and automated security technologies that provide business value

V. Zero Trust Implementation Takeaways

A. Use the CISA zero trust framework

As an architectural strategy, zero trust is best pursued when guided by industry expertise. When it comes to zero trust architecture, CISA sets the standard. CISA, or the Cybersecurity and Infrastructure Security Agency, was established in 2018 as a public-private partnership for securing our digital critical infrastructure inside the Department of Homeland Security (DHS), and "works with partners to defend against today's threats and collaborates to build a more secure and resilient infrastructure for the future."[2]

> "Zero trust is a key element to modernize and strengthen our nation's defenses." – Jen Easterly, CISA Director

The CISA Maturity Model for Zero Trust provides a roadmap for organizations looking to pursue zero trust. This framework outlines five key pillars of zero trust:

- Identity
- Device
- Network (or environment)
- Applications (or workloads)
- Data

[2] https://www.cisa.gov/about-cisa

Across each of these pillars includes requirements for visibility and analytics, automation and orchestration, and governance (or compliance). Additionally, for each of these pillars, there are maturity levels based on the strength of the control or the way it is deployed: traditional, advanced, and optimal.

CISA's Maturity Model for Zero Trust reflects the reality that zero trust security is an ongoing quest, not a 'one and done' project. Using this model allows teams to assess where they are, where they have gaps, and how to make progress.

According to the CISA model, and consistent with our survey data, optimal implementations of zero trust involve the use of:

- Automation
- Integrated workflows
- Continuous trust validation
- Data inventories
- Encryption
- Micro-perimeters

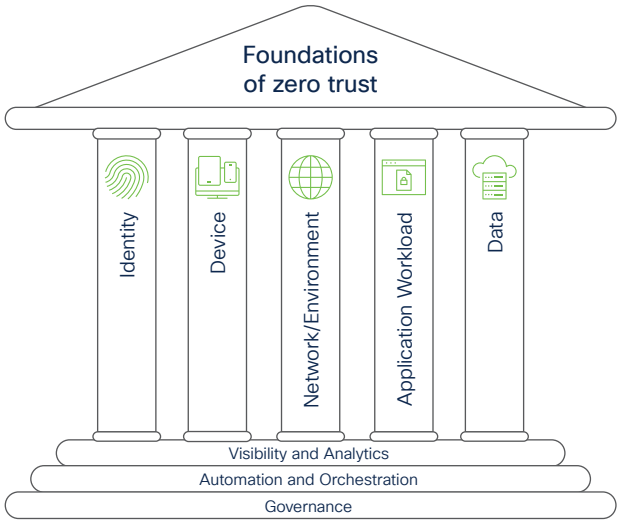


Figure 13: US Cybersecurity and Infrastructure Security Agency (CISA) zero trust pillars

CISA Zero Trust Maturity Model

	Identity	Device	Network/ Environment	Application Workload	Data
Traditional	• Password or multi-factor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in clouds or remote environments are encrypted at rest
Optimal	• Continuous validation • Realtime machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/ egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted

Visibility and Analytics | Automation and Orchestration | Governance

Figure 14: US Cybersecurity and Infrastructure Security Agency (CISA) Maturity Model for Zero Trust

US Government drives zero trust mindshare

In May of 2021, President Biden signed his first executive order (EO) on cybersecurity – mandating the federal government to move towards a zero trust architecture. In January 2022, the Office of Management and Budget (OMB) issued a memo that gave 'teeth' to the zero trust mandate, in terms of deadlines for specific requirements. Despite the limited scope of the OMB memo to civilian federal agencies, many industry analysts have relied on the CISA framework in their analysis of the commercial zero trust market.

B. Lessons learned from Cisco's zero trust experience

In 2020, Cisco set out to move from a traditional network-based perimeter and VPN model to a zero trust framework. From the start, the goal was to give users a secure, uniform experience accessing applications, wherever the user or application is located.

Our team set out to improve security and create a better experience for our 100,000+ users – a fundamental shift that took place in less than five months.

So, what does zero trust at Cisco look like? When we think about zero trust at Cisco, four things need to happen every time someone tries to access an application:

1. We verify the user using multi-factor authentication
2. We confirm that the device is up-to-date and healthy
3. We validate that a Cisco-managed device is being used
4. The application can be accessed without the VPN

And when we say every time, we mean it. Not once a day, not for one application, but continuously.

"It's not often that you can say you are improving security while also improving the user experience, but that's what we've achieved with this rollout."
– Josephina Fernandez, Cisco IT Director

C. Discovering the quick wins

Quick Win Discovery #1: Get buy-in with a simple message. One common mistake we saw with other initiatives was that high complexity made them hard to understand and sponsor. Our goal was to make the message simple, specific and timebound, so it would be memorable and easy to repeat to others.

Quick Win Discovery #2: Keep scope well-defined and status well-communicated. We communicated our goals clearly: improve the user experience, reduce risk, and improve governance. Any attempts to expand the project beyond these objectives were quashed, while we also made sure to keep all parties updated on the rollout status.

Quick Win Discovery #3: Create demand for zero trust. We started with the 10-15 most used applications so that improved user experience would have the broadest and most visible impact. Once users saw how easy it was to access their most important apps, demand grew inside the organization from application owners to department heads.

Quick Win Discovery #4: Start where you are, leverage what you already have. As our SVP, Chief Security and Trust Officer Brad Arkin says, "You're never starting with a clean slate." Our team decided which of the existing security controls could be used to advance zero trust goals, and which technologies would have to be retired.

Get the full story on the Cisco rollout of zero trust at scale here.

Zero trust at Cisco by the numbers

Pilot metrics	Monthly metrics	Annual savings
• 5-month timeline – including employees and contractors in 98 countries • 10-15 private apps protected without a VPN (now > 100) • <1% users contacting helpdesk (vs. 7%) • 170K devices secured	• 5.76 million health checks • 86,000+ devices self-remediated • 410,000 fewer VPN authentications	• $3.4M in savings from employee productivity gains • $500K in savings in IT help desk support costs

D. Build resilience: How Cisco Secure delivers zero trust

With Cisco, organizations can embed zero trust across the fabric of their multi-environment IT ecosystem and secure access in a way that frustrates attackers, not users. This protects the integrity of their business in the face of unpredictable threats and challenges and is essential to security resilience.

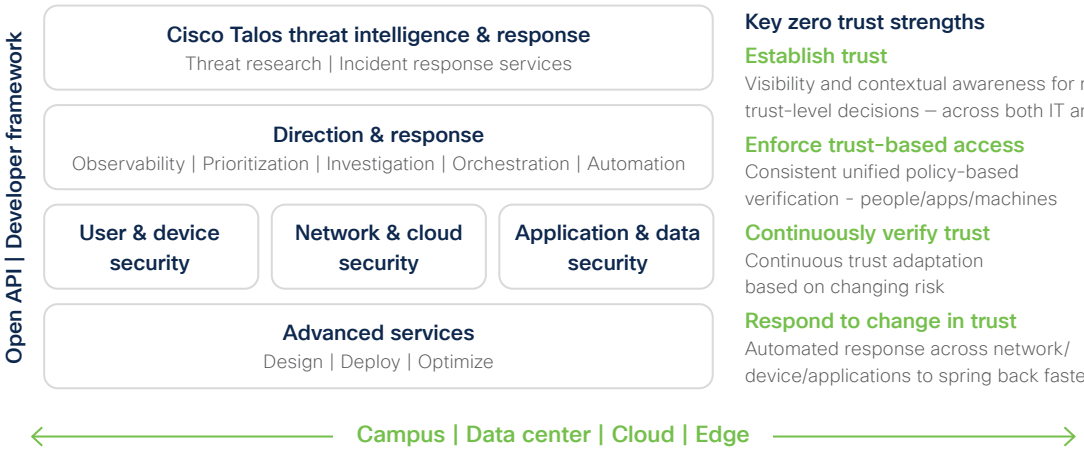
Cisco delivers key zero trust capabilities that enable organizations to:

With Cisco's integrated approach, organizations can successfully implement unified policy lifecycle management across their network, devices, applications, and clouds.

Ultimately, with Cisco, companies can unlock value and achieve their goals – with strong security AND high productivity – enabling teams to achieve better security, higher performance and faster threat response.

As a company that has implemented zero trust across its global operations, Cisco brings trusted expertise, helping more than 300,000 customers worldwide protect the integrity of every aspect of their business to withstand unpredictable threats or changes and then emerge stronger.

Cisco Secure platform



Our solutions span the five key pillars of CISA's Maturity Model for Zero Trust, delivering visibility and control across campus, cloud, and on-premises networks.

cisco SECURE

VI. Next Steps

Many of the customers and partners we work with on zero trust are looking to solve several critical challenges. Some see zero trust adoption as a way to secure their assets against targeted threats or elevate their business performance by securing hybrid work. Others have tied zero trust to mitigating supply chain risk and as well as protecting their cloud environments.

Escalating threats demand a new approach to security. By partnering with Cisco on zero trust, your organization can accelerate your threat response and build resilience with deeper visibility, reducing the impact of threats to recover faster and get back to business serving your customers.

Ready to take your first steps with zero trust? Ensure only the right users and secure devices can access applications, with a frictionless experience. Sign up for a free trial of Cisco Secure Access by Duo.

For more information on how to jumpstart your zero trust quest, register for one of the Cisco Zero Trust Workshops

cisco.com/go/zero-trust-workshops

DUO

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of Cisco Secure's Zero Trust offering, the most comprehensive approach to securing access for any user, from any device, to any IT application or environment. Duo is a trusted partner to more than 35,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.

Try it for free at duo.com.

cisco SECURE

Cisco has long established itself as the networking leader, while building an open, integrated portfolio of cybersecurity solutions along the way. Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use – and that it all works together. We're driven by the fact that people and our customers are at the heart of what we do. Cisco Secure empowers the security community with the reliability and confidence that they're safe from threats now and in the future on the SecureX platform. We help 100 percent of the Fortune 100 companies protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet.

Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.