Building a Solid Foundation for Your Zero Trust Framework

ENTRUST

SECURING A WORLD IN MOTION

Table of contents

INTRODUCTION..3

TOP CYBERSECURITY CONSIDERATIONS WITH ZERO TRUST...5

Why is Zero Trust Important?

Explicit Verification

Government Mandates and Compliance

THE ZERO TRUST JOURNEY...9

ZERO TRUST IS A STRATEGY..12

Secure Identities

Secure Connections

Secure Data

POST-QUANTUM PREPARATION..15

WHAT SHOULD I ASK?...17

THE CURRENT STATE OF ZERO TRUST.......................................20

LOOKING TOWARD THE FUTURE..21

WORKING WITH ENTRUST..23

Introduction

The explosive growth of digital and virtual connectivity comes with a price: In 2023, cybercrime is predicted to inflict damages of $8 trillion globally[1]. And that doesn't include the cost of reputation, lost customers, and impact on those who lose personal identifiable information – according to IBM, 60% of organizations increased consumer prices in 2022 due to a data breach[2].

No matter the industry, companies around the world are investing more time and resources in cybersecurity. This is why, more and more, organizations have begun to consider what we call a Zero Trust framework, aligned to the Cybersecurity and Infrastructure Security Agency's (CISA's) Zero Trust Maturity Model: an overarching strategy across tools and solutions that limits permissions based on roles and responsibilities and reduces the risk of cyberattacks.

Although it starts with concepts centered around identity and access management, this complex journey requires a more comprehensive approach. And this ongoing project can't be underestimated in its significance, importance, or need for serious consideration. **Zero Trust extends beyond secure identities across users, applications, devices, machines, and workloads; it's a comprehensive data security strategy for encrypting data at rest and in transit, spanning public and private cloud environments.**

[1] Cybercrime Magazine, Top 10 Cybersecurity Predictions And Statistics For 2023
[2] IBM, Cost of a Data Breach 2022

The results are well worth the time and investment. **Between 2020 and 2022, IBM reports data breach costs surged 13%. And organizations with a Zero Trust framework in place have an average cost of nearly USD $1 million less as a result of breaches** than the $4.35 million enterprise average[3]. Keeping this in mind, it's easy to see why Gartner predicts that **by 2026, 10% of large enterprises will have a mature, measurable Zero Trust program** in place compared to the less than 1% with this framework today[4].

So where should companies start with this complex journey? Read on for key considerations, what questions to ask, and key components of Zero Trust.

13%

is how much IBM reports data breach costs surged between 2020 and 2022.

$1M

is the figure organizations with a Zero Trust framework in place say they reduce their average cost when a breach occurs.

10%

of large enterprises will have a mature, measurable Zero Trust program in place by 2026.

[3] IBM, Cost of a Data Breach 2022

[4] Gartner, Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality, 2022

Top Cybersecurity Considerations with Zero Trust

Beginning a journey with Zero Trust means learning the facts. What are the top areas to consider? Why is this concept gaining traction and adoption, while poised to become even more visible and critical in the coming years?

How does the compliance landscape impact Zero Trust? And what should enterprises know as they start to investigate rolling out a Zero Trust framework across their organization?

Why is Zero Trust Important?

Companies can't ignore the threat of cyberattacks from a security, financial, or reputational perspective.

According to IBM, 83% of organizations surveyed have experienced more than one data breach, with 60% of these breaches leading to price increases impacting customers. And 59% of these organizations didn't have a Zero Trust strategy in place[5].

Between the rising number of breaches, their increasing complexity, and the growing concern of state-based actors, organizations must take their security seriously. **And while Zero Trust may not eliminate threats altogether, this framework can significantly reduce the risk of these attacks and their impact when they happen.**

That threat landscape only grows as companies continue to go digital. Moving data to the cloud, hybrid work, and remote work environments change and expand security concerns and how organizations must address them to protect sensitive systems and information while allowing for enabling business growth to improve operational and business efficiency.

Governments, in particular, have already begun the transition to mandating Zero Trust frameworks for federal agencies and organizations.

83%

of organizations surveyed by IBM have experienced more than one data breach

59%

of these organizations didn't have a Zero Trust strategy in place

Acceleration of digital transformation and distributed environments also contribute to the increasing risk of attacks. Organizations should take a practical look at the situation to address these new challenges. **Attacks are inevitable** – rather than fruitlessly assuming you can build an impenetrable wall around your network, taking a Zero Trust approach expects that bad actors can and will penetrate your network, and when they do you have controls and solutions in place to limit the damage caused.

Companies should adopt the Zero Trust security approach of "never trust, always verify," and then back it up with technology, policy, and process. It's a careful balance between preparing, protecting, and being able to practically run a business. But Zero Trust helps improve risk mitigation for critical assets and helps reduce the impact of a breach, creating a return on investment that can't be ignored.

[5] IBM, Cost of a Data Breach 2022

Explicit Verification

Zero Trust underscores the idea that when it comes to cybersecurity, companies can't ever assume trust. A large number of identities across employees, systems, and devices, permission sprawl, and poor security hygiene only make it that much easier for attackers to gain access to the information they want.

PERMISSION SPRAWL

When identities such as employees or contractors accumulate more access and privilege than they need to do their jobs. If a vendor who no longer works with the company retains their permissions — that's sprawl.

To combat this, it's important to **give people only the permissions they need, when they need it, to perform their work – nothing more.** Reducing permissions reduces the ability of bad actors to move laterally within the network and limits the damage caused when they breach an organization's defenses using a compromised identity.

Based on the principle of "never trust, always verify," there are 3 key tenets of Zero Trust:

Verify explicitly:
Establish trusted identities through the use of continuous authentication and authorization that includes evaluating context-aware risk signals.

Least-privilege access:
Limit access to only authorized users, machines, and devices, and enforce permissions to limit access based on a user's role and responsibilities to secure data without hindering productivity.

Assume breach:
With inevitable breaches, it's critical to minimize the blast radius during a cyberattack through strong encryption and segmentation of users, devices, and networks.

Knowing all organizations should expect to experience a data breach at some point or another, they should do everything in their power to limit damage ahead of time and reduce cyber risk.

Government Mandates and Compliance

In 2021, the White House issued a mandate to implement a Zero Trust program for all government systems[6]. With foreign agents constituting a significant threat, this move works to protect sensitive information throughout the different components across government agencies.

> “A Zero Trust framework allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, Zero Trust can ensure that the damage is contained. The Zero Trust framework security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity.”
>
> **Joe Biden, President of the United States**
> Executive Order on Improving the Nation’s Cybersecurity

An expansive mandate like this one only shows the seriousness with which governments take this concept. And with new cybersecurity systems in place, we can expect compliance laws to change over the next several years to incorporate this framework. With compliance’s impact on the cybersecurity insurance industry as a whole, organizations will likely need to meet minimum compliance regulations to maintain eligibility.

36%

of CISOs say they’ve already started to implement components of Zero Trust while another 25% plan to start doing so in the next two years[7].

[6] The White House, Executive Order on Improving the Nation’s Cybersecurity
[7] PwC, 2023 Global Digital Trust Insights Survey

The Zero Trust Journey

At the start of a Zero Trust journey, companies must first define what Zero Trust means to their specific organization.

A helpful way to do this is to look at CISA's Zero Trust Maturity Model.

CISA’s Zero Trust Maturity Model outlines 5 distinct pillars:

Identity

Devices

Networks

Applications and Workloads

Data

All underpinned by visibility & analytics, automation & orchestration, and governance.

Within this model, too, are **four stages of maturity** an organization works through during its ongoing Zero Trust journey.

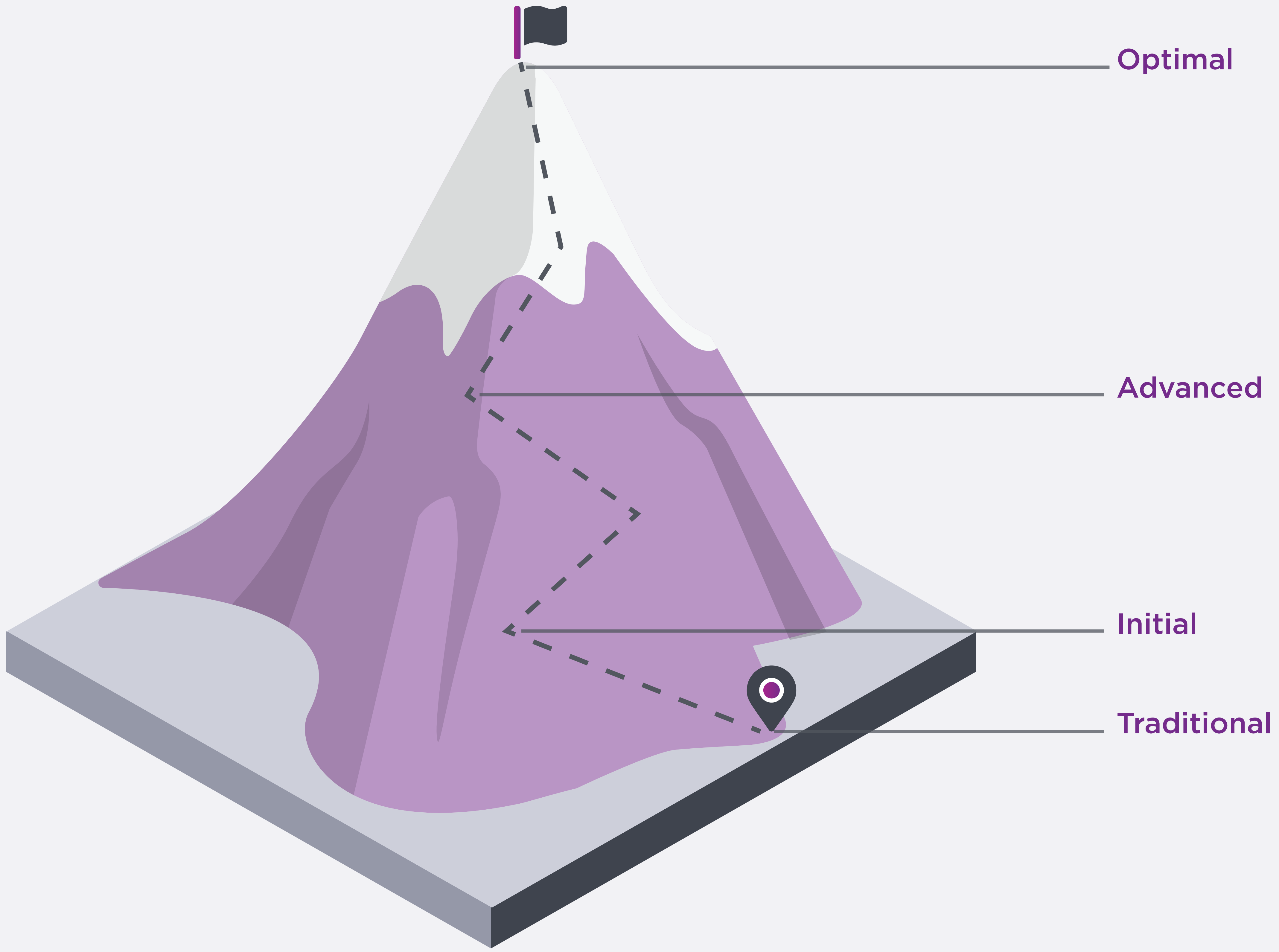
You can think of the four stages of this model like starting at the base of a mountain and climbing toward the peak. At its **traditional** stage, a company has yet to integrate the principles of Zero Trust and sees manual processes and responses, dependent systems, and limited coordination between those systems, which are largely external.

The **initial** stage introduces automation, responsive changes to privilege, and connection to internal systems.

The **advanced** stage includes automated controls wherever possible, centralized identity control, and a build toward enterprise-wide awareness.

Finally, when an organization reaches its **optimal** stage, its processes are fully automated, contain least-privilege access, and operate on continuous monitoring and risk assessment with comprehensive situational awareness.

Zero Trust Maturity Journey



However, this model isn't linear. It instead recognizes that each company will have its own particular Zero Trust journey depending on its size, goals, industry, and existing systems. This means each organization will start in a different place and move at its own speed. As companies embark on this journey, they'll need to determine their cybersecurity capabilities as well as their security and business objectives to determine the correct path.

Another critical consideration for organizations as they start a Zero Trust journey is to know that it never ends. As companies continue to expand and mature, their systems will change. Zero Trust must address both legacy systems and processes as well as new policies, products, and solutions necessary for business growth.

Constant evaluation of systems and threats and continuous changes to configuration and policy is necessary to make the most of any Zero Trust program. Key to ensuring a successful Zero Trust framework is strong enforcement of compliance and a comprehensive governance program across the many risk areas of Zero Trust. Falling behind with security considerations only leaves organizations vulnerable to even more attacks, rendering the investment on the initial Zero Trust project useless.

Zero Trust is a Strategy

Individual solutions and products come together to enable the implementation of a Zero Trust framework. It’s critical to remember Zero Trust is the sum of its parts: a complex system of tools, people, and processes that work in tandem to prevent threats or mitigate them.

At Entrust, we focus on three key components that make up the foundation for a robust Zero Trust framework:

Secure Identities

Secure Connections

Secure Data

Secure Identities

Weak or compromised credentials are one of the largest causes of data breaches. Securing identities with phishing-resistant multi-factor authentication (MFA) solutions helps mitigate identity-based attacks. These solutions include certificate-based authentication (CBA) and MFA that necessitates physical proximity as a required factor. Risk-based adaptive step-up authentication can further ensure that only verified and authorized users can access resources and help balance the user experience and security by only introducing friction in the process when needed.

Incorporating passwordless security, including secure alternatives like mobile smart credentials and FIDO2 passkeys, can also eliminate the likelihood of a bad actor gaining access to systems, devices, and networks by cracking a user’s password. This security instead uses information like biometric data for access along with cryptographic key pairs and physical proximity as a key requirement. In today’s world, with each of us being asked to remember multiple complicated passwords leading to password fatigue and re-use, this balances ease of use with increased security.

Secure Connections

Sensitive and confidential data currently moves over public and private networks, whether it's a user logging on to an online portal or sending an email, or – as is common in IoT – machine-to-machine communication that occurs without any human intervention.

All these connections and endpoints need to be secured with a digital certificate. Those certificates are issued by a certificate authority, which can then verify that object and give it access, whether that's allowing someone access to your network or servers talking to one another.

With digital certificates being used for identity, encryption, and signing, it's no wonder there has been significant growth in the number of certificates organizations are issuing and managing. Not only that, but management challenges and complexities come with certain use cases, such as short-life certificates we see with public TLS/SSL and IoT.

In order to properly enforce your Zero Trust strategy, certificate lifecycle management becomes critical to ensure you have strong issuance protection for your certificates and can mitigate common risks such as issuing a rogue certificate that brings too much access or privilege.

Secure Data

In order to identify and protect access for these users, companies must be sure to use strong encryption for data in transit, at rest, and in use. **Encryption, PKI, and key lifecycle management** play a critical role in this.

Public key infrastructure (PKI) makes up an important part of Zero Trust by enabling users to securely exchange information with digital keys. PKI enables trusted identities by issuing certificates that establish devices and machines that make up part of a company's digital environment.

Once issued, security specialists use those certificates to identify devices within an organization, find their owner, and figure out what happens when that machine is decommissioned or sold off, or ownership is transferred. If companies aren't using the latest and greatest cryptographic technology, it can lead to security holes and breaches that stop business and cost companies money.

Protecting these certificates and keys is critical to understanding a company's digital landscape, safeguarding communication between devices and networks, and creating digital signatures that add another layer of security to the framework.

These encryption keys must be enabled from a multi-cloud perspective to protect a company's security. With companies using several clouds and data storage solutions, experts and decision-makers must look at the whole of their environments.

Post-Quantum Preparation

Another part of Zero Trust is **post-quantum readiness.** While quantum computers have yet to arrive, experts predict it's only a matter of time before attacks launched by these powerful computers create a significant threat to organizations' cybersecurity systems. In fact, bad actors are already using a "harvest now and decrypt later" strategy to steal and stockpile encrypted data that can be decrypted later when quantum computers are available on a large scale[8].

Through their Zero Trust journey, an organization must keep this in mind. Planning to mitigate post-quantum risks by deploying a strategy for crypto-agility can keep your security system prepared to adapt when post-quantum algorithms land.

[8] Security Week, Solving the Quantum Decryption 'Harvest Now, Decrypt Later' Problem

The quantum threat may not be here, but it's on its way.

- Scientists in China announced that their 56-qubit quantum computer took 1.2 hours to complete a task that would take 8 years for the world's most powerful supercomputer to accomplish.
- Risk experts expect that quantum computing, or something related, will compromise security between 2027 and 2033.
- In 2020, Alphabet's CEO Sundar Pichai predicted that "in a 5-10 year time frame, quantum computers will break encryption as we know it today."
- McKinsey and Co. predicts there will be about 5,000 operational quantum computers by 2030[9].

Entrust takes this threat seriously. We and our partners are already working to mitigate the risks by incorporating PQ-ready solutions across the key risk areas of Zero Trust.

Risk experts expect that quantum computing, or something related, will compromise security between 2027 and 2033.

[9] McKinsey & Co., What is quantum computing, May 2023

What Should I Ask?

With Zero Trust entering the consciousness of more and more business leaders, company decision-makers and those involved with the planning and implementation of these programs need to know the right questions to ask. Here are a few different questions organizations should begin asking themselves as they look into and prepare to execute this framework.

What are our goals and objectives with Zero Trust?

Zero Trust won't look the same for every organization. This framework depends upon each company's specific pain points, existing networks and systems, strategies, goals, and more. These factors should all be a part of the conversation when determining the best starting point and path forward when creating a Zero Trust framework.

Who should be responsible for our Zero Trust program?

Conversations about ownership of Zero Trust should begin early to establish key decision-makers and those who must be involved with internal and external meetings. As soon as an organization knows they're looking to create this framework, it's important to determine whether a team should be involved to lead the foray and who should participate. What powers will this team have to effect change? A key part of implementing a Zero Trust strategy involves changes to policy and procedures that can affect day-to-day operations across several teams and users.

What budget should we allocate to a Zero Trust initiative?

Zero Trust is a multi-year journey that requires ongoing investments through both technology and resources to configure and maintain the controls put in place on an ongoing basis as part of this new framework.

How does my solution integrate with the rest of my IT ecosystem?

It's critical for organizations to understand their existing cybersecurity and IT environments – everything from gaps to risk areas to systems already in place and any that might be implemented soon. This includes both homegrown systems and partner solutions: everything that might impact the overall strategy or specific solutions and tools put in place.

How do I prevent vendor lock-in for business and IT agility, specifically public cloud lock-in?

A new Zero Trust framework may require changes to partners or vendors, necessitating the transition of data, products, or services. This practice may become costly and difficult, resulting in a customer's dependence on a specific solution. As Zero Trust requires the ability to adapt and remain flexible, it's necessary for organizations to investigate ways to prevent lock-in and to identify solutions that lay well in an integrated ecosystem.

How are we going to communicate with and educate our employees?

Moving toward a Zero Trust framework may require a change in processes and workflows for employees across the organization. Creating buy-in will help ease any transitions and motivate employees on related teams to care about their work on the project. Straightforward communication about any changes – and the absolute necessity of having the best possible security – will help employees understand and participate in the process.

What should the user experience look like?

A move to Zero Trust should, overall, minimally impact the average employee's day-to-day experience. Ensuring the process stays relatively painless as possible will only increase buy-in on the project from most of the organization. That said, some level of friction isn't a bad thing – it's feedback that the system is in place and working, and gives users insight and awareness of cybersecurity risks.

What questions should I be asking my partners about how to do this?

While flexibility begs the question of potential changes in specific tools and solutions, companies should work with their existing partners to understand where they may experience disruptions or changes and how best to create the overarching network that fosters Zero Trust. Starting conversations early with those vendors can put you in the best possible position to implement this strategy.

ZERO TRUST QUESTION CHECKLIST

As you begin planning, make sure to ask each of these questions of your internal and external partners:

☑ What are our goals and objectives with Zero Trust?

☑ Who should be responsible for our Zero Trust program?

☑ Where are we now on the Zero Trust Maturity Model, and where do we want to be?

☑ How does my solution integrate with the rest of my IT ecosystem?

☑ How do I prevent vendor lock-in for business and IT agility, specifically public cloud lock-in?

☑ How will we report progress on this journey?

☑ What gaps or vulnerabilities remain in our environment and what will it take to address them?

☑ What should the user experience look like?

☑ What questions should I be asking my partners about how to do this?

The Current State of Zero Trust

While Zero Trust isn't yet part of most organizations' existing cybersecurity infrastructure, more and more companies are looking to implement their own programs as soon as possible. And those companies with a mature Zero Trust framework saw the dividends. Companies with a mature Zero Trust deployment had breach costs more than $1.5 million lower than breaches at organizations with early adoption of Zero Trust.

All in all, **Zero Trust-enabled companies saw savings of 20.5% during these breaches**[10].

Companies in the technology world are taking this framework seriously and beginning to implement these programs across their enterprises.

[10] IBM, Cost of a Data Breach 2022

Looking Toward the Future

With cyberattacks already in full swing – and only poised to become more prevalent and carry greater impact – companies must begin to research, plan for, and implement a Zero Trust framework to protect their data, their customers, and their businesses. Remote work and rapid adoption of public and private cloud environments have only expanded the attack surface alongside state-based actors looking for their opportunity to infiltrate.

Threats such as phishing, which are both probable and create significant disruptions to business on top of costing millions, necessitate the implementation of these kinds of security measures. Companies can protect themselves both now and in the future, reducing the likelihood of attacks as well as the impact they leave behind, by instituting secure identities backed by phishing-resistant passwordless multi-factor authentication.

Additionally, the looming inevitability of post-quantum cryptography means that companies who aren't already beginning to investigate how to create Zero Trust frameworks that involve PQ-ready solutions should change focus immediately. Planning for the future can only put you and your business in the best possible position to protect yourself.

Zero Trust may look like a daunting project requiring an inordinate investment of time, effort, workforce, and budget. But those who begin preparing themselves and having conversations about how to create this framework will not only be protecting themselves in the future from attacks and disruption that could dismantle their business but they also will be impacting their company's bottom line.

Working with Entrust

As a company with a focus on helping our customers and partners implement these frameworks, Entrust is uniquely positioned to help you build a mature Zero Trust framework for your organization. We specialize in providing industry-leading solutions with a broad portfolio that helps secure identities, devices, applications, networks, and data – whereas most vendors only focus on a single niche area. We're a leader in a limited field with unique expertise in post-quantum encryption armed with resources and best practices. With Entrust, you can be sure we'll be a trusted partner that can help identify your goals, pain points, and ways to work with you and your partners to achieve the best results.

About Entrust

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions entrusted to them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most entrusted organizations trust us.

For more information, visit **www.entrust.com**.

About the Entrust Cybersecurity Institute

The Entrust Cybersecurity Institute shares news, analysis, insights and commentary for IT and business leaders charged with protecting and enhancing IT infrastructure.

Learn more at **www.entrust.com/cybersecurity-institute**