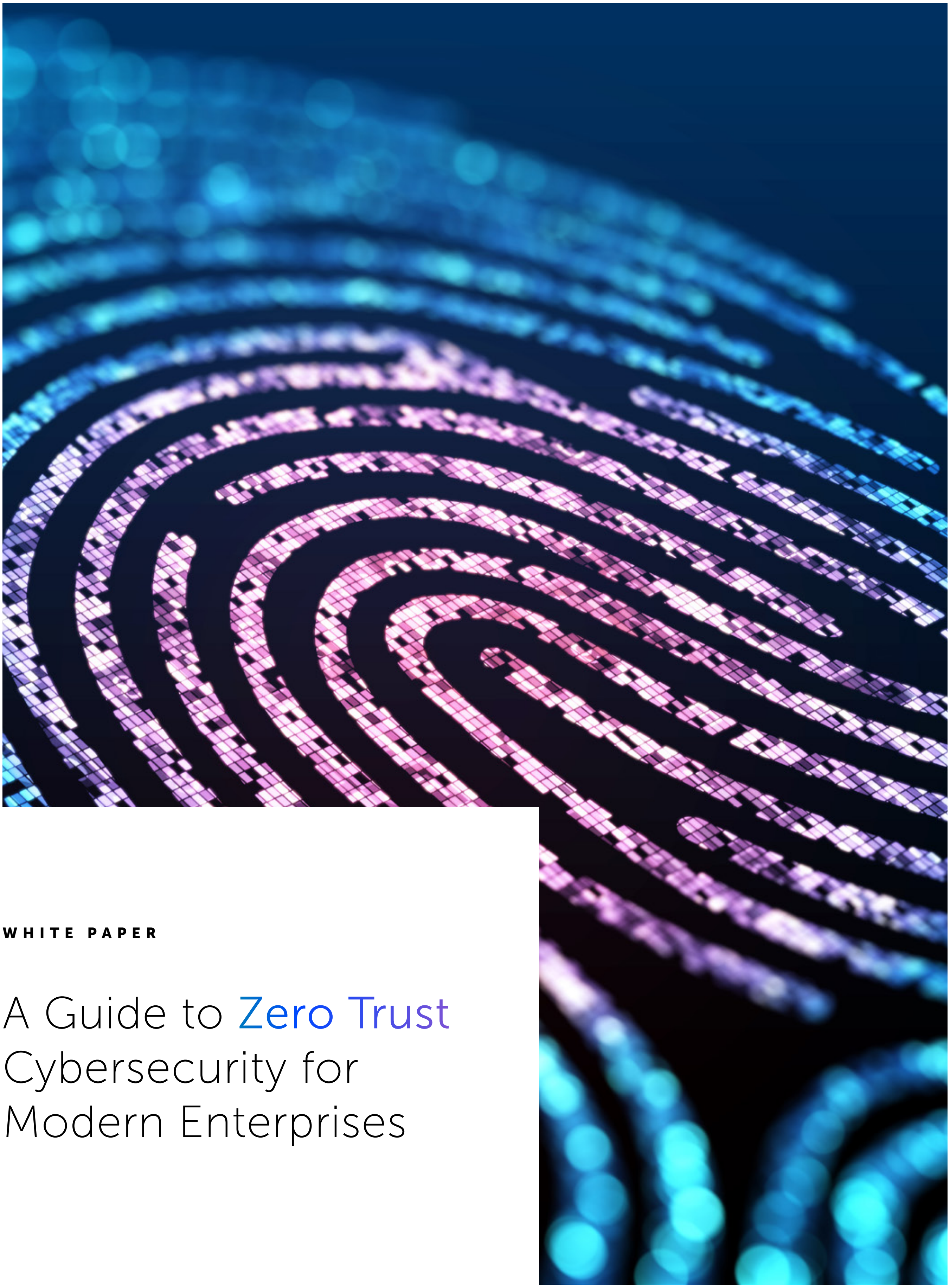


WHITE PAPER

A Guide to Zero Trust Cybersecurity for Modern Enterprises

Contents

Introduction

Enterprise digital ecosystems face more security challenges than ever before. As companies and the technology they use become web-based and more complex, traditional cybersecurity becomes more porous, leaving businesses vulnerable to exploitation. The work-from-home model has further tested the outdated notion that perimeter security is adequate protection.

Cyberattacks have become pervasive and their sophistication is growing exponentially, which makes it much harder to detect and respond to them. In 2022, it took an average of 207 days for an organization to identify the breach and 70 days to contain the breach, according to an IBM report.

As companies employ SaaS solutions, APIs, cloud computing and other modern tooling to stay agile and competitive, these transformation initiatives add complexity to organizational processes, making it vital to hit the reset button on security. Lateral attack, cross contamination, and direct access to assets is far more likely for the attacker.

The price of not rethinking your security strategy has skyrocketed...

CYBERCRIME COSTS ARE EXPECTED TO REACH

$8 trillion

GLOBALLY IN 2023

No matter the industry or company size, old-school ring fencing and firewalls alone are no longer sufficient. Zero trust is an enterprise imperative.

- Fluid network perimeter with many shades of grey between the clear inside and outside. Critical assets, applications and data are no longer in a single location but cross domains, networks and often cloud vendors.
- Close to impossible to rely on a reliable source of trust in this dynamic.
- Attacks are mostly on the app/API level now.

This calls for verifying every interaction for legitimacy and because of the scale of transactions, this needs to be far more frequent on authN and verification. Trust is never assumed and access is never granted by default. No user or service, whether internal or external, is automatically granted access.

Hackers and the malware they employ have become more sophisticated and more damaging, impacting all industries and companies of every size. As a result, enterprise cybersecurity must be just as agile as any other business practice, monitoring and adapting in a continuous loop.

What is Zero Trust?

The National Institute of Standards and Technology (NIST) describes zero trust as "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

NIST also makes it clear that building a zero-trust architecture (ZTA) is not a one time initiative. As technology continues to evolve at an alarmingly fast pace, enterprise cybersecurity must also be continuous.

ZTA is not a product or set of products. It's a *holistic strategy;* one that can and should iterate over time. It starts with a company taking a thorough assessment of its current state to get a true understanding of its security posture and find vulnerabilities before they can be exposed.

For decades, companies gave employees access to everything in their network. The assumption was that everyone inside the firewall was trustworthy and everyone outside was not. That thinking doesn't fit with the current threat landscape, and assumptions now come with more risk. Companies can no longer trust the firewall because important users are outside of it and bad actors can get inside.

There is considerable debate around how to achieve a strong and resilient ZTA. From our perspective, we see ZTA supported by three core principles:

01

NEVER TRUST, ALWAYS VERIFY

The cloud, applications, data storage and networks — everything is dynamic and software-defined now. We cannot assume perimeters, identities or even APIs to be static and persistent anymore. With more nodes being ephemeral, spinning up and down runtime, and more network changes on the fly, companies need to adopt a security model that will be as strong and flexible as the ever-changing environment.

02

EXERCISE LEAST PRIVILEGE

Since ecosystems are so dynamic and users are accessing from many different points, companies must grant the least amount of privilege and expand privileges only when users, or software services, prove themselves trustworthy. Privilege should always be time-boxed and never granted perpetually. Whenever possible, you must require traceable promotion processes and service accounts to see when they are requested.

03

EMPLOY COMPREHENSIVE MONITORING

Always watch and verify everything using fine-grain transactions (or smaller units). Do not assume the call five minutes ago will be from the same source just because the speaker claims to be — challenge it, reduce the rekey and recycle token time and make it difficult for nefarious actors to fake sources and transactions. Whether a request for access comes from inside the corporate network, using internal hybrid cloud, or corporate laptops and services, do not automatically assume the user or service is safe. Assume others have visibility into your network. Assume services could be hijacked. Assume everyone is unauthenticated until verified and proven otherwise, and even then, they should be trusted for the single transaction only.

Why Zero Trust?

Enterprises have always been prone to risk. But the stakes have changed drastically — the scale and impact of bad actors today has led to some of the biggest breaches we've ever seen, and breach is imminent for all.

It's the "weakest link" problem. Companies that increasingly rely on third-party software services are only as safe as their most vulnerable app or device. One of the most notable recent cases of this is the **SolarWinds network management software breach**. Companies, organizations and even federal agencies like the U.S. State Department were infiltrated as a result. The attack was so immense that top federal government cybersecurity leaders **called for a zero-trust approach**.

Another high-profile breach stemmed from firewall vendor Accellion when **hackers exploited vulnerabilities** in the company's outdated technology, impacting major enterprises and institutions including Kroger Co., the State of Washington and Harvard Business School.

There are several trends that have exponentially increased risk in recent years, including:

More organized cybercrime

Cybercrime has become much more organized, with exploits that are harder to detect. For example, **crimeware-as-a-service** (or cybercrime-as-a-service) has enabled both technically inexperienced criminals and advanced threat actors to rapidly orchestrate sophisticated attacks.

More distributed working models

The way we work has changed fundamentally, especially after the 2020 COVID pandemic. According to **Verizon's 2022 Mobile Security Index**, 45% of organizations surveyed suffered a mobile-related compromise, with 73% regarding the impact as major. This growth is likely related to the ongoing shift to hybrid work models, a proliferation of mobile devices and a general increase in cyberattacks.

More to lose with consumer trust

With the majority of breaches involving personally identifiable information (PII), cyberattacks can have long-term costs from loss of consumer trust that are hard to quantify and even more difficult to overcome. New regulations to increase cybersecurity requirements for PII and PHI data are constantly emerging around the world, adding more complexity to the enterprise security strategy.

More complexity brought by transformation and modernization

As enterprises undergo transformation initiatives and modernize their technology to achieve increased agility and innovation, they bring in unnecessary risk if they don't weave security into the very fabric of their strategy. Between the API economy, digital supply chain and SaaS, cloud computing, software-defined networks and data analytics, hackers have more valuable assets to exploit and more attack vectors to access than ever before.

Guidelines for Moving Toward a Zero Trust Model

Although ZTA has developed to include a wide range of practices, there are 10 zero trust concepts that underpin any program:

01

UNIFIED IAM FOR CORPORATE TOOLS

Corporate tools must support fine-grain controls aligned with the enterprise identity model, regardless of whether the host is internal or external (SaaS).

02

GATE WITH LEAST PRIVILEGE/PAM ACCESS

Start from no-access/no-privilege, and then grant limited access upon verification that the user needs it and build up from there. Permission is only granted when necessary on a need-to-know, need-to-access and need-to-share basis.

03

VERIFY CONSTANTLY & USE SMALLER UNITS

Make sure that your transaction and access tokens are verified and constantly challenged. Break up large units of work into smaller ones to both help reduce any one-time loss, and also to give your detection and response team more data and time. Improve observability, ingest your logs and use insights.

04

AUTOMATE & MICRO SEGMENT: NETWORK, WORKLOAD & DATA

Build security into your process and architecture and automate as much as possible. Isolate and segment network, workload and data to reduce the blast radius and speed up containment when necessary. A solid review process will go a long way.

05

SECURE ENDPOINTS

Companies are habituated to assuming client endpoints are secure. They should do their best to secure endpoints, while simultaneously anticipating there could be a breach, so transfer only what is needed to endpoints.

06

VERIFY SERVICES

Do not use static bindings on services. Instead, companies should make sure they have a resource access model that is aligned with their identity access management (IAM) strategy across all SaaS, online applications and API providers.

07

SECURE DEVELOPMENT PRACTICES

Companies should employ the secure software development model (SSDM) and constantly monitor the continuous integration/continuous delivery (CI/CD) pipeline and, when possible, keep the infrastructure immutable.

08

TRUST NO RUNTIME

Runtimes must be hardened and, when possible, immutable. Furthermore, there should be extra layers and checks for sensitive data residing on virtual machines.

09

TRUST NO NETWORK

Companies should assume others can monitor their packets, regardless of whether they are in their corporate network, using a virtual private network (VPN) or bridged, and security controls should be layered. (Traditionally, a VPN grants a trust zone to an endpoint or another trust zone but that's no longer recommended.)

10

THINK LIKE A HACKER

Think from an outside-in perspective. Look at your system and think of what could (and would) others do with it? Don't focus only on your own assets because you could be a steppingstone to a bigger prize. Either way, think defensively.

The above 10 concepts are woven within the five main pillars to ZTA, which are all reliant on each other and critical to a ZTA program's success. Below you'll find high-level characteristics of the pillars followed by a more in-depth explanation of how you can build a solid ZTA foundation by employing each.

01

IDENTITY

- Unified identities for customers, employees and partners
- Multifactor authentication
- Policies around identities and weighted attributes

02

NETWORK

- Micro-segmentation and isolation
- Distributed firewalling
- Dynamic, software-defined networks and perimeters

03

WORKLOAD

- Fine-grain API transaction controls
- Layered, secure and contained execution environment
- Immutable pipelines and environments
- Segment-bound workload and sandboxes

04

DATA

- Fine-grain, classified and segmented data
- Distributed object-level encryption
- Data immutability

05

DEVICES

- Device compliance monitoring and asset management
- Real-time risk analytics of data access
- CI/CD deployment of devices
- Document protection

01

IDENTITY

The identity pillar is the typical starting point for ZTA. This stage is where a company unifies and controls identities across its entire ecosystem, including all partners, customers and employees. With so many day-to-day business operations defined by the internet, it's impossible to verify security credentials without breaking down transactions into smaller units. ZTA exerts control by linking the identity of the user, device, service or network to the requested transaction.

In this pillar, it's vital to strengthen how we authenticate each identity using multifactor authentication (MFA) and challenge-response authentication (CR). Machine learning (ML) should be deployed to help detect anomalies in user behavior. It's important to limit token access and reduce the time granted with any token. The **most common initial attack vector in 2022** was stolen or compromised credentials, responsible for 19% of breaches at a global average cost of $4.5M USD. Putting an identity-centric model in place mitigates the risk around stolen and compromised credentials and, once a solid foundation is in place with the identity approach, the stage is set to tackle the rest of the pillars in a ZTA strategy.

02

NETWORK

The key to the network pillar is building distributed and layered network isolation structures. Doing so largely comes down to micro-segmentation, which means building small and well-defined boundaries using a next generation firewall that is logically distributed across your entire enterprise, with both on-prem and hybrid cloud coverage. This limits lateral attacks by making access more difficult and reduces the blast radius when a breach occurs. And today, it's a matter of when, not if.

As enterprise network boundaries start to fade and extend right up to the edge, using a secure access service edge (SASE) solution could improve your company's ability to react and respond with a relative real-time cadence. SASE simplifies wide-area networking (WAN) and security by focusing on a distributed model that stretches out directly to the edge. It provides a framework that combines software-defined WAN (SD-WAN), secure web gateway (SWG), cloud access security broker (CASB), zero-trust network access (ZTNA) and firewall-as-a-service (FWaaS) in a unified solution.

03

WORKLOAD

Securing applications and APIs during runtime is paramount because this is where hackers hit paydirt. The execution environment must be layered and secured, like the network pillar, by breaking everything up into smaller units. Companies should separate runtimes on multiple levels:

- Each computer cluster must be bound to a distinct micro-segmentation
- Every node must be contained properly with the right configuration
- Endpoint protection should be used wherever possible
- Sandboxes should be used for testing code or monitoring for malware

Containerization is compatible with ZTA because it calls for breaking down an operating system into smaller units so that applications can be segregated and run independently. That means if bad actors gain access to one app, they won't automatically get access to everything else. Establishing a secure software development life cycle (SSDLC) process is imperative to tie all this together.

04

DATA

Encryption is essential to providing a level of protection against unauthorized access and visibility for company assets. However, a crypto scheme is only as good as a key management policy would protect or allow. It is extremely risky for any organization to trust their entire data store and lakes to only a handful of crypto keys (root keys). This is where 'break once run everywhere' (BORE) attacks could compromise an entire system in a short period of time. ZTA calls for understanding how and where data is coming in and going out. Then, organizations can limit liability by breaking up all data into smaller units and giving them unique tags so that each transaction is siloed.

The complexity of modern data dissemination across the net makes it much harder to protect data visibility. Every data lake, every copy of a data set, every persistent login and cache presents a new attack surface for an organization's data. It's critical to protect not just the central store, but also the entire data set. Some fundamental steps to properly securing data include:

- Classify all company data assets and label each unit to understand what needs to be protected and how. Follow the data movement and provide end-to-end protection across all usage (in transit, at rest and in use).
- Create a strong and granular access model that binds working data labels to specific identities and make sure these fine-grain transactions can be continuously verified. Do not rely on simple "trusted zones" but instead verify the authentication.
- Include controls to scan for usage of data that is potentially out of compliance. For example, flag data sets moving out of a particular geography or in use by applications that aren't whitelisted.

The benefit of breaking everything up into units is that it increases work for bad actors. With ZTA, a hacker would still have to decrypt each unit if they got through, significantly decreasing the ROI for the bad actor.

05

DEVICES

The device pillar focuses on monitoring and managing servers, laptops, virtual machines and IoT devices through modern asset management tools. Many organizations have this for most of their assets, but some legacy devices may slip through the cracks. Once every device is visible, companies can begin understanding where their riskiest assets lie and begin programs to tackle those challenges. As bring-your-own-device becomes more commonplace in the workforce, it's crucial to ensure that those devices comply with organizational and regulatory requirements.

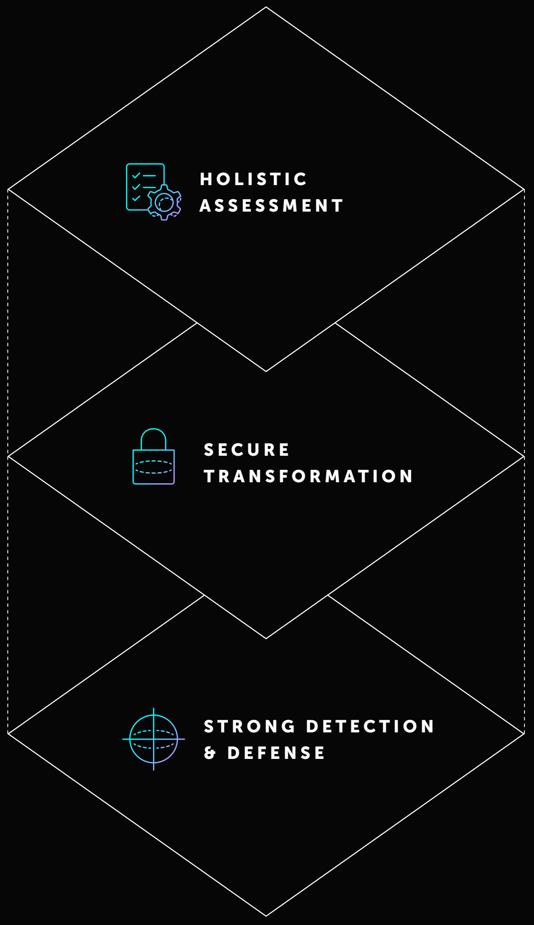
Endpoint management and protection should be enabled on every device to protect your organization. Device enrollment allows a company to have live attack visibility and offers a real-time ability to mitigate those attacks by removing compromised devices and disabling services.

Both the device pillar and data pillar enable access control policies to protect devices and user access to data. Local storage of sensitive documents should be controlled and enforce sharing policies. The technology for document protection isn't perfect, and there are still ways for users or malicious actors to get around it, such as git commits to external repositories.

→ All five pillars are reliant on the others and are crucial to a ZTA program's success.

Transitioning to Zero Trust

Moving toward zero trust can be broken down into three stages:



01

HOLISTIC ASSESSMENT

Moving to ZTA requires an honest, comprehensive assessment of a company's existing identity strategy, network design, all business processes (including data flows and workflows), storage topology, application deployment and more. Without this information, it's impossible to identify vulnerabilities. In the assessment phase of implementing a ZTA program, there are three important steps:

Identify, classify and document the interfaces to your assets.

Identify all assets, including sensitive, valuable or regulated assets. Know where they are and how they could be reached.

Threat model your inputs and outputs.

Start looking at interfaces as not just features but liabilities, as well. Reducing the attack surface means controls will more naturally map to the interfaces.

Understand the business impact.

Prioritize and understand the liabilities and risks from a business perspective. Is the organization holding data keys or root keys? Sensitive information? Personally identifiable information (PII)?

With this information, it's then possible to map out what is needed to move to a dynamic, zero-trust enterprise security model.

02

SECURE TRANSFORMATION

Security is always a continuous practice. Nefarious actors are always looking for gaps and new ways to breach our defenses, and that's why it's so important to improve our security posture, consistently and constantly.

However, most organizations are still stuck in the old siloed, audit-based security model. For a company to be secure while transforming, security must be built into the organization process, culture and digital platforms to function in this digital age.

It's not just about buying more tools or solutions. Constantly evaluating new options is helpful if you can afford the effort and investment. It's much more important to have security initiatives tied to specific business objectives. For a successful transition, they need to be structured:

Get Commitment at the Top

The executive level must understand and commit to transforming enterprise security initiatives to successfully move toward a zero-trust model. As it requires total buy in from across the organization from disperse and siloed groups to achieve a complete adoption.

Start with a Healthy "Run" State

Make sure there's a concrete set of practical security policies and procedures. Nothing is perfect, but it's important to have the necessary policies aligned with your annual loss expectancy (ALE) calculation.

Invest in Continuous Improvements

Invest in a continuous improvement program that includes an incident retrospective process, procedure and policy change management and so on. Our adversaries are constantly learning and adapting and so should we.

Employ Practical Validation

Use a practical, continuous red-teaming process. An outside-in view from a third party can spot what your internal teams cannot find to further bolster your defenses.

Invest in Detection & Response

An enterprise must have an agile cyber detect and incidence response team (CIRT) that has the capability and capacity to handle the existing annual rate of occurrence (ARO) plus enough time to implement any necessary improvements.

Align Digital Risk Management

Align risk management and governance toward a software-defined model, while automating as much of the verification and audit process as possible. Use industry recognized publications such as NIST 800-207 to help build compliance into your system.

Technical and administrative controls at endpoints provide another crucial layer of security that could help improve a company's overall cybersecurity posture. When pulled together with other security measures, it could also give the CIRT a better level of visibility, as well as more tools to identify and mitigate threats.

Employee education must be part of any secure transformation to zero trust. Internal users who don't understand the risk of downloading a suspicious attachment in an email or trusting their local coffee shop's WiFi add risk to the organization. Social engineering remains the number one cause of data breaches, as well. So, it's incumbent on companies to provide ongoing and thorough risk management training to staff.

03

STRONG DETECTION & RESPONSE

Defense is really about time — increasing the amount of time you have to respond, reducing the time needed to narrow down and respond, and cutting the time needed to recover and bring your organization back to a normal, strong state. This is why security operations are so important.

Detection, both the speed and breadth of it, is critical in order to reduce the time needed for the CIRT to contain, mitigate and recover. Detection and response in the new zero-trust architecture is a much more agile process, and it has to be since you are working with finer-grain transactions. Therefore, teams must access a higher volume of data, and must be ready to identify patterns across small transaction units. It's not so much about patching a route or managed detection and response (MDR) services, although those are still part of your critical baseline security. Teams need to detect and react to a much more dynamic and software-defined environment.

Finally, you must move closer to real-time data, analytics and response capabilities. All this needs to be adapted to an agile model so your team can learn and pivot quickly.

Bringing Agility to Cybersecurity

Zero trust is not about eliminating threats because no one can promise that. It's about redesigning security by automating and embedding security measures in your development process. Zero trust will dramatically improve the prevention of breaches and contain the damage that can be done with any successful hack, making companies better equipped to thrive in a software-defined environment.

Digital transformation is no longer optional and organizations must ensure they move forward safely. Cyberattacks have become more common and more costly than ever before, and that means you have to bring the same agility you use in any business process to security.

No product or suite of products can guard adequately against increasingly sophisticated bad actors. By adopting a zero-trust mindset and following the guidelines that will keep your company thinking like a hacker, you can protect your business, your customers, your employees and your bottom line.

Although nothing is ever 100% secure, a company's security posture should balance risk tolerance and benefits. Have a baseline, then prioritize the rest proactively, constantly adjusting.

The primary goal is to buy time: to detect, to respond, to contain, pivot, so should the risk profile and security.

INCREASE LEVEL OF EFFORT

And expertise and time needed by nefarious actors to breach

REDUCE YIELD

And damage radius in case of an incident, both short- and long-term

IMPROVE RECOVERY & EVIDENCE

To make it harder to get away ("clean exit")

It's also critical to balance priorities based on business objectives, which should adjust as the business grows and evolves to account for recovery posture.

COST

Security is never free; there are costs in time and design, in tools, in CPU, in storage and more

USABILITY & PERFORMANCE

To make something "relatively" secure, useable and high performing is difficult

SUSTAINABILITY

To maintain, detect and respond constantly is a must, and it's often costly

Resources & Contact Info

Have questions or comments? Reach out to:

Sam Rehman

TITLE

Chief Information Security Officer, SVP

CONTACT

Sam_Rehman@epam.com

About EPAM

Since 1993, EPAM Systems, Inc. (NYSE: EPAM) has leveraged its advanced software engineering heritage to become the foremost global digital transformation services provider — leading the industry in digital and physical product development and digital platform engineering services.

Through its innovative strategy; integrated advisory, consulting, and design capabilities; and unique 'Engineering DNA,' EPAM's globally deployed hybrid teams help make the future real for clients and communities around the world by powering better enterprise, education and health platforms that connect people, optimize experiences, and improve people's lives. In 2021, EPAM was added to the S&P 500 and included among the list of Forbes Global 2000 companies.

Selected by Newsweek as a 2021, 2022 and 2023 Most Loved Workplace, EPAM's global multidisciplinary teams serve customers in more than 50 countries across six continents.

As a recognized leader, EPAM is listed among the top 15 companies in Information Technology Services on the Fortune 1000 and ranked four times as the top IT services company on Fortune's 100 Fastest Growing Companies list. EPAM is also listed among Ad Age's top 25 World's Largest Agency Companies for three consecutive years, and Consulting Magazine named EPAM Continuum a top 20 Fastest Growing Firm.

Learn more at **www.epam.com** and follow EPAM on **Twitter** and **LinkedIn**.

Headquarters

41 University Drive, Suite 202
Newtown, PA 18940, USA

P: +1-267-759-9000
F: +1-267-759-8989