

Trust No One & Automate (Almost) Everything

Building a Modern
Zero Trust Strategy

The New Stack

Trust No One and Automate (Almost) Everything: Building a Modern Zero Trust Strategy

Alex Williams, Founder and Publisher

Ebook Team:

Ben Kubany, Project Manager

Celeste Malia, Marketing Consultant

Colleen Coll, Sponsor Advocate

Danni White, SEO Editor

Emily Omier, Author

Gabriel H. Dinh, Executive Producer

Heather Joslyn, Ebook Editor

Judy Williams, Copy Editor

Supporting Team:

Benjamin Ball, Director of Sales and Account Management

Joab Jackson, Editor-in-Chief

Michelle Maher, Assistant Editor

© 2022 The New Stack. All rights reserved.

20220616.1

Table of Contents

Sponsor.....4

Introduction5

Why the Castle and Moat Approach to Security Is Obsolete7

What Is Zero Trust?.....11

What Do Authentication and Authorization Mean in a Zero Trust Network?.....15

The Cultural Changes Zero Trust Security Demands.....20

Zero Trust in a Cloud Native World.....24

Automation Holds a Key to Zero Trust Implementation27

Conclusion31

About the Author32

Disclosure33

Sponsor

We are grateful for the support of our ebook sponsor:



Torq is a no-code automation platform for security and IT operations teams. Easy workflow building, endless integrations, and out-of-the-box templates deliver value in minutes — not weeks. Torq and The New Stack are under common control.

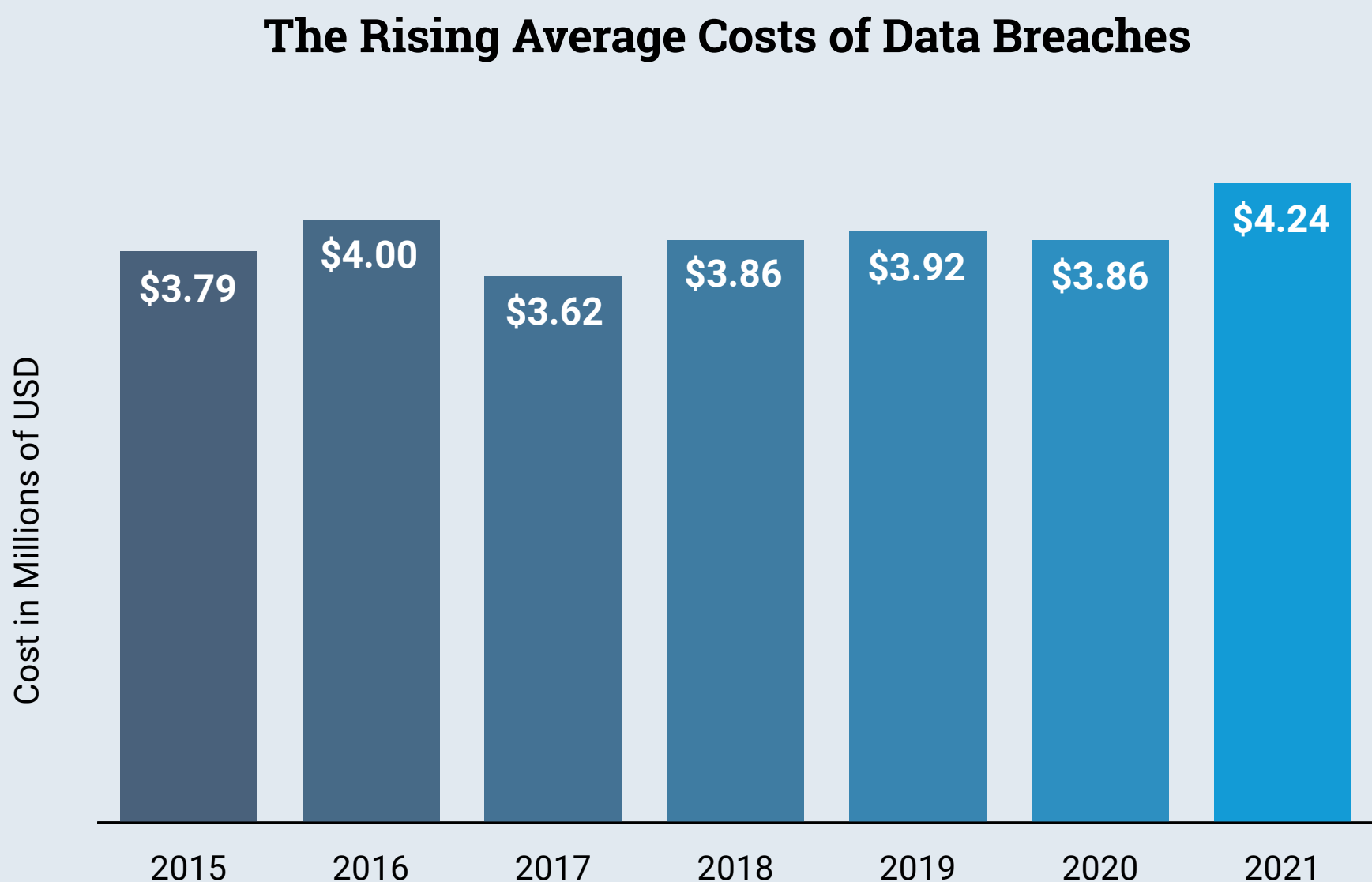
Introduction

Distributed networks that run on multiple and/or hybrid clouds are making many things easier, such as scaling up to meet demand. But one thing that's gotten much more complicated is [security](#). The old castle and moat approach doesn't work, because in a distributed, [cloud native](#) architecture there are many castles, geographically scattered, and more may appear or disappear at any time.

As the castle and moat approach to security goes the way of real castles and moats, it is being replaced by zero trust, a security strategy that involves eliminating the idea of “trusted” anything — no trusted users, no trusted devices.

In addition to the focus on identifying, authenticating and authorizing every user, human or computer, at every access, zero trust also aims to help security programs become more strategic and aligned with the business's core interests.

FIG 0.1: *Data breaches are growing more costly for organizations.*



“Executives, CEOs and boards of directors are much more intrigued with zero trust than engineers,” said [John Kindervag](#), senior vice president, cybersecurity strategy at ON2IT, who is often considered the creator of zero trust.

When we think about it, it is ridiculous to think that all of an organization’s assets are equally valuable — they clearly aren’t. This is why it’s a high-level decision: a major part of implementing zero trust is not just figuring out how to authenticate and authorize, but also how to prioritize which surfaces to protect.

The turning point in cybersecurity, according to Kindervag, was with the [breach at the retail giant Target in 2013](#), because that was the first time a data breach resulted in the CEO being forced out.

Zero trust is about allowing executives to be more involved in defining goals for their organizations’ security programs, while also providing a framework for securing digital assets in a distributed system, and with ephemeral applications and [data](#) stored in data centers, on the cloud and [at the edge](#).

“A major part of implementing zero trust is not just figuring out how to authenticate and authorize, but also how to prioritize which surfaces to protect.

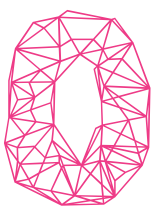
The ultimate goal of zero trust is to prevent data breaches. The secondary goal is to make any and all cyberattacks unsuccessful. Zero trust does not promise to prevent cyberattacks — a subtle but important distinction. The core goal, however, is data protection.

“If you lost my data, you can not un-lose it,” said [Leonid Belkind](#), chief technology officer and co-founder of Torq, a security automation company.

So preventing data breaches of all kinds, including the kind that got Target into the news in 2013, is the core goal. Here’s why organizations need zero trust and how they can go about implementing it.

CHAPTER 01

Why the Castle and Moat Approach to Security Is Obsolete



Once upon a time, IT resources lived in castles (also called “data centers”) and were protected by moats (firewalls) and knights (your friendly security specialists). In these days of yore, the assumption was simple: everything in the castle was warm and fuzzy, everything outside the castle walls was hostile wilderness.

This worked well in the long-ago time, before the 1990s. [Though zero trust](#), as either a practice or theory, didn’t evolve until much later, it was in the ‘90s that the cracks started to show in the castle walls.

This context is important, because although zero trust is often discussed in terms of cloud native systems, the need for zero trust and the move away from perimeter-based security started much earlier.

The Castle

When the entire IT system lived in one central data center, network security was much easier.

“The perimeter type of approach, the historical approach, was working fairly OK,” said [Jonas Iggbom](#), director of sales engineering at [Curity](#), an identity and access

management (IAM) and application programming interface (API) security technology provider. “It was one point of entry that the firewall could control.”

With all of the IT assets on a segment of the network that was protected by a firewall, and limited access points that could be strictly patrolled, the system worked acceptably well. There were still limitations: If the firewall was ever breached, there was no security inside the network, so breaking through the firewall once gave attackers near complete control over the system.

The problem first started with laptops and road warriors. What should the IT security think of the files on their salespeople’s 20-pound laptops? What about when you access your corporate email from a Blackberry?

“Should we treat it as if it was inside?” asked Belkind, of Torq. “The reality of businesses being digital — adopting mobility, allowing people to work from everywhere, from every device — is that this deteriorated this whole approach of a very clear ‘who’s outside, who’s inside.’”

Then came the cloud, he noted, in the form of both Software as a Service (SaaS) and Infrastructure as a Service (IaaS).

The castle was sliding into ruins before the rise in [containers](#) or [microservices](#) or anything that we would call cloud native now. It requires a completely different approach to security.

A Fortress of One

At first, the shift in security strategy went from protecting one, single castle to a “multiple castle” approach. In this scenario, you’d treat each salesperson’s laptop as a sort of satellite castle.

SaaS vendors and cloud providers played into this idea, trying to convince potential customers not that they needed an entirely different way to think about security, but rather that, by using a SaaS product, they were renting a spot in the vendor’s castle.

The problem is that once you have so many castles, the interconnections become increasingly more difficult to protect. And it’s harder to say exactly what is “inside” your network versus what is hostile wilderness.

Zero trust assumes that the castle system has broken down completely, so that each individual asset is a fortress of one. Everything is always hostile wilderness, and you operate under the assumptions that you can implicitly trust no one.

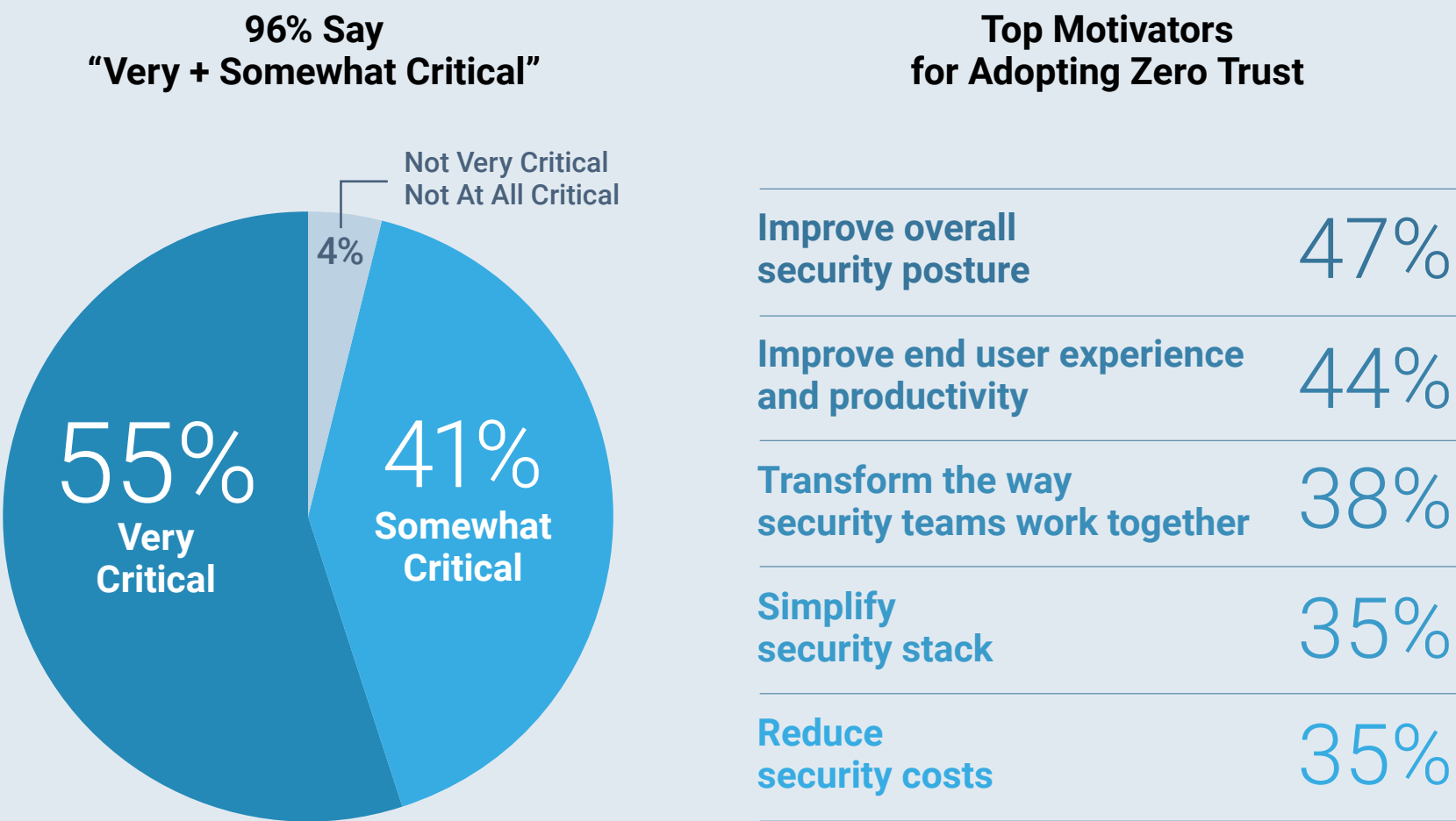
It’s not an attractive vision for society, which is why we should probably retire the castle and moat metaphor. Because it makes sense to eliminate the human concept of trust in our approach to cybersecurity and treat every user as potentially hostile.

Adopting Zero Trust

Ninety-six percent of security decision makers consider zero trust critical to an effective security posture, according to a [survey published by Microsoft in July 2021](#).

FIG 1.1: Tech decision makers overwhelmingly believe a zero trust approach to security is critical to their organization.

IT Leaders Believe Zero Trust Is Critical



But while support for the idea of zero trust is close to universal, vanishingly few companies are implementing it effectively.

Sixty-five percent of companies use shared logins and 42% use shared SSH keys, according to a [2022 survey by strongDM](#). Both practices run absolutely counter to zero trust principles. Zero trust requires not just rethinking your security program, but also rearchitecting your application to make the new strategy possible.


Implementation starts with granular authentication systems, which means forcing any users, human or server, that want to access a resource to prove that they are who they say they are.

Once you've authenticated a user, the next step is to follow that up with authorization or enforcement: Is that user allowed to perform the action it wants to perform? According to Iggbom, authentication is fairly widely adopted, but far fewer organizations follow that up with zero trust authorization systems.

Most systems would previously have been set up so people could authenticate into a castle — a group of actions. One of the things that sets zero trust apart is that it requires extreme granularity, allowing users to access or alter only the very specific resource they've requested access to, at the specific time they've requested that access.

CHAPTER 02

What Is Zero Trust?

 ero trust is a security philosophy, not a set of specific best practices or a checklist for security teams to follow. As cyberattacks have increased and executive leadership is held responsible for data breaches, zero trust has grown in popularity among executives and other business leaders.

“You don’t need to convince people why zero trust is a good idea,” said Belkind.

This doesn’t necessarily mean that every organization is [implementing it in practice](#). Though most business decision-makers agree that zero trust is a good idea, it represents an ideal state that companies will always be striving towards, rather than declaring “achieved,” and that very few companies are even close to reaching.

We spoke with Belkind about the ideas behind zero trust, why security teams have had to [re-imagine cybersecurity for the cloud native world](#), and how zero trust works when put into practice.

The New Stack: How would you define zero trust?

Leonid Belkind: Zero trust is a theoretical state where any consumer inside a network not only doesn’t have any permissions, but is not aware of what else there is in the network around them.

In a zero trust network, there are both human users and service users, that each have an identity that can be cryptographically validated. But in “peacetime,” they don’t have access to anything.

Can you tell me about how security has evolved and what role zero trust plays in the evolution?

In a traditional network security segmentation, which was the predominant way of doing this, you would have secure controls on the network topology level. For example, everything coming from this network can go to that network, everything coming from this particular device in this network could go to this network, that sort of thing. That would be the basis for a corporate access-control policy.

Even before the cloud, though, this emphasis on devices and networks became meaningless if we’re talking about users. Now it’s the user that matters, and the user could connect from home, from an internet café, from a shared office location. At that point, we need a user-aware policy, which is not zero trust yet. But the idea there is that, if I can verify that it’s a particular user, I’ll give them all these network privileges.

So these matters, beginning with introducing user identity, then thinking about restricting your permissions and general least-privileged access or just-in-time access, are all kind of brewing up towards zero trust.



SUMMARY

Cybersecurity teams need new strategies to address the increasing scale and velocity of modern enterprises. Automation and orchestration tools need to be part of the solution, but traditional security orchestration, automation and response (SOAR) platforms pose significant technical and operational barriers.

KEY PRODUCT

Torq is a no-code automation platform for security teams that can help people of any skill level automate complex workflows to streamline and reinforce security processes.

KEY PARTNERS

Armis, Hunters, Orca Security, SentinelOne, Snowflake, Snyk, Wiz.

How does zero trust work exactly?

Your trust network assumes there's an entity called the network controller, that can be accessed by all the participants in the network. The network controller can identify the accessing party — either a human or service user — in a very strong way, assess their security posture, and so on.

The network controller can be asked to provide very, very limited — not only time-restricted, but actually operation-restricted — permissions to do a very specific job.

So instead of, “I have network access to the data center, where I could look up customer records, where I could update the employee data,” for every operation, I would go to the controller and I would say, “Hello, this is who I am. This is my job. This is my identity. This is my device. Here's the security posture of my device. What would I like to do? Update employee data for Jane Doe as an employee.”

“First, you have to understand that there is no lever that you could pull and say, ‘OK, bam, zero trust enabled.’ It's rearchitecting your network.”

—Leonid Belkind, chief technology officer and co-founder, Torq

And I would be given permissions to do just that, and not an iota more. I can update Jane Doe's records — and just right now. It's a network that bears zero implicit permissions, only what you asked for, with a very granular and strict policy. That's the notion of zero trust as a theory.

What do things look like in the real world? Are there trade-offs? How do people put zero trust into practice?

An enterprise first and foremost needs to be pragmatic. There is no such thing as “Oh, I'm turning all of our communications off.”

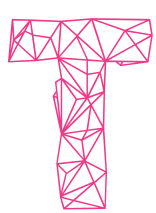
First, you have to understand that there is no lever that you could pull and say, “OK,

bam, zero trust enabled.” It’s rearchitecting your network.

In many cases, after you handle the actual critical things, you will get at a certain point to a state where you will say, you know what, the cost of re-architecting this particular access is higher than the benefits I will get from tightening the security. You’re not running with a banner that says “Zero Trust at Any Cost,” and throwing away the business demands.

CHAPTER 03

What Do Authentication and Authorization Mean in a Zero Trust Network?

 he foundation of putting zero trust principles into practice is [authentication and authorization](#). What they mean is actually quite simple, but the specifics of how authentication and authorization work in zero trust versus other systems are different.

Authentication simply means proving that the user, whether a human or computer user, is in fact who they claim to be.

Authorization means establishing, once we are certain of the user's identity, that this person or service is permitted to access the resource that it is requesting access to.

“Authentication and authorization don't necessarily change their meaning in a zero trust context,” said Belkind.

“If at all, authentication becomes much stricter, if you're granting it properly, and authorization becomes much more granular,” he said. “Instead of asking, ‘Could I access my corporate data center and do whatever I like with it?’ you would ask to access this particular document inside this particular application, inside this particular section of my data center, from this particular location, using this particular device at this particular point in time.”

Authorization depends on authentication. It makes no sense to authorize a user if you do not have any mechanism in place to make sure the person or service is exactly what, or who, they say they are.

Most organizations have some mechanism in place to handle authentication, and many have role-based access controls (RBACs) that group users by role, and grant or deny access based on those roles. In a zero trust system, however, both authentication and authorization are much more granular.

To return to our castle analogy, before zero trust the network would be considered a castle, and inside the castle there would be many different types of assets. In most organizations, human users would be authenticated individually — have to prove not only that they belong to a particular role, but that they are exactly the person they say they are.

Service users can often also be granularly authenticated. In a RBAC system, however, each user is granted or denied access on a group basis — all the human users in the “admin” category would get blanket access, for example.

It was also not possible to give a user access to only a portion of the resources inside the castle: The knight standing at the drawbridge could either come in and get full access, or be turned away.

In other words, one could not grant granular access. In practice, this generally means both human and computer users are granted excessive permissions.

According to the most recent [Cloud Threat Report](#) by Prisma Cloud of Palo Alto Networks, 99% of cloud users, roles, services and resources are granted permissions that they don't use — in other words, permissions that they do not need.

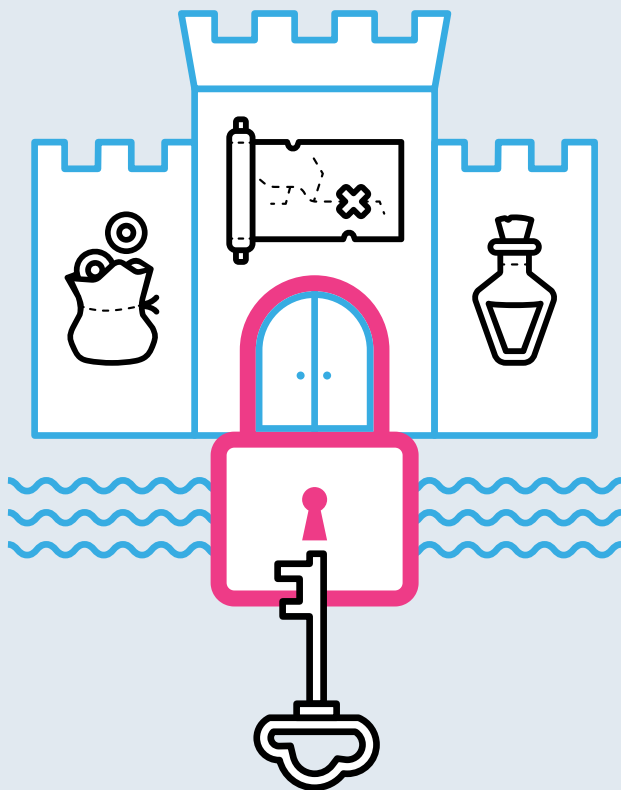
Getting Granular

One of the most important aspects of zero trust is granularity. In a zero trust system, granting access based on roles is not security enough. Access requests have

What Do Permissions Mean in a Traditional Vs. Zero Trust Architecture?

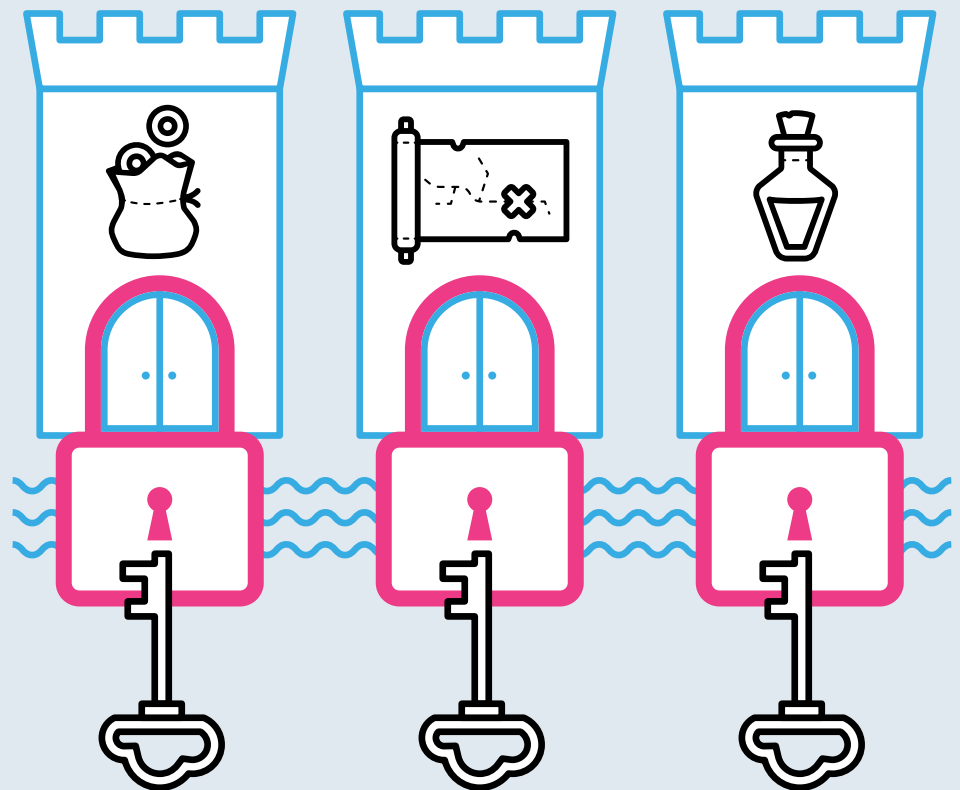
Traditional

Infrastructure and data live in a single location (or "castle"). Access is granted broadly to an authenticated user.



Zero Trust

The network is distributed among many "castles." Authenticated users are granted granular, time-limited access to specific assets.



Source: The New Stack

© 2022 THE NEW STACK

FIG 3.1: A zero trust strategy helps cut down on granting too many unnecessary permissions, which can easily be used to gain illicit access to a network.

to be granular, and access is granted to only that single resource, for only a set amount of time.

This requires organizations to break up their castles into single-resource fortresses. This particular analogy does a good job at illustrating the architectural shift that has to happen to move to zero trust: Granting granular access is only possible once you have created the proper structure around it.

The idea of breaking resources into more granular components is the same as the principle behind microservices in general. As services and data are broken into smaller pieces, it becomes more possible to grant access granularly.

When all of your resources are clustered together in a "castle," with no mechanism for sending people away from a particular room once they are inside, it isn't possible to implement zero trust.

The Role of Automation

In talking about authentication and authorization in a zero trust environment, there is sometimes an assumption that the process must always be 100% automated.

That's not true.

Clearly, without some automation tools it would be impossible to get anything done in a zero trust system. But some types of requests can, and should, be reviewed manually by a human.

“In fact, for zero trust network access of users, the system could be semi automated, it could involve people in the loop,” Belkind said. “I don't necessarily assume that we are talking about machine-to-machine communications.”

Time-Limited Authorization

One of the most common misconceptions about zero trust systems is that once a user is authenticated and authorized, that user becomes a “trusted” user. The user is able to come and go from the fortress at any time.

However, there are no trusted users or trusted devices in a true zero trust implementation. Users have to be authenticated and authorized each time they attempt to access a resource.

And in a true zero trust architecture, there will be a time window on the authorization: this user is allowed to do this particular action in this time window. Neither the user nor the associated device becomes trusted.

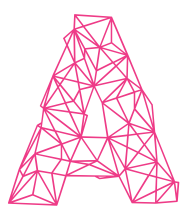
Out in the real world, the vast majority of security leaders acknowledge the importance of zero trust security. “You need to first take the step of authentication of users and systems, and not everybody even has that basic step implemented,” Iggbom said.

“But then you need to enforce the fact that, yes, you're Jonas, but are you allowed to access this information? That enforcement is even less implemented in

organizations. At this point, there's still a reasonably heavy lift for organizations to actually implement that."

CHAPTER 04

The Cultural Changes Zero Trust Security Demands



At the core of a zero trust strategy is re-thinking how companies approach security, from who is involved to what the goal is. “Zero trust is a strategy designed to stop data breaches, and then to make other cyber attacks unsuccessful,” said Kindervag, of ON2IT. In most cyberattacks, the goal is to exfiltrate some kind of sensitive data, and zero trust is a framework for designing a system in which that won’t happen.

Prioritizing Security

The basis of a zero trust strategy is to force security decision-makers to step back and think more like CEOs — or to get the CEOs themselves involved.

In many organizations, IT teams, especially security teams, have been so segregated from the business leadership that they don’t, during their everyday responsibilities, pause to think about how the organization earns money. Security teams often have very narrow scopes of work, and focus on meeting compliance demands rather than thinking strategically about how to actually protect the company.

As Belkind said earlier, businesses ultimately have to be pragmatic and can’t just turn off all communications. When working on projects with enterprises, he said, the starting point is always to ask what are the things that could hurt the

organization the most if they were compromised, and start there.

Top Down, No Silos

Because zero trust focuses not on checking off compliance boxes or blindly following established company protocols but on aligning the security program with the business realities, the strategy is often (but not always) adopted first by executives and imposed on the security team in a top-down manner.

This is a cultural shift: It's telling the security team that they need to move their focus from protecting laptops from malware to ensuring the company's core assets are as protected as possible and on a zero trust network.

“When working on projects with enterprises, said Leonid Belkind, of Torq, the starting point is always to ask what are the things that could hurt the organization the most if they were compromised, and start there.

Success with zero trust also has to include restructuring the organization. “If you look at traditional organizational structure, they're organized to stay in silos — the developers, platform engineers, the security teams — and it's like a relay race where they pass the baton down,” said [Ratan Tipirneni](#), CEO of [Tigera](#), a cloud native application observability company.

“That type of organizational structure will not work when implementing these types of security models. You need to design security policies upfront, even when the code is being built.”

The need for organizational change is one of the reasons Tipirneni thinks that strong executive leadership is nearly always required for success with zero trust. Though not everyone interviewed for this ebook said that executives must be the champions, Kindervag and Belkind agreed that there is often high-level involvement in moving to zero trust, and involving executives and aligning security with business interests is critical.

Incremental Improvement

Often security folks are hesitant to make changes because they fear being blamed for disruption. It's possible to dramatically improve zero trust maturity without disrupting the usual IT operations, but the key is incremental improvement.

Start with something that is absolutely critical. "If we're a bank, we might protect the SWIFT gateway," Kindervag said, referring to the secure cross-border payment and financial messaging system.

"That's a manageable project, in contrast to if I say, 'We're going to turn the whole network into zero trust,' everyone's going to just say, 'How do we do that?'"

Eliminate Trust

Security experts talk about "trust" — trusted users, trusted devices — and design security programs that assume that some humans and computers are by default "trusted."

But, Kindervag noted, "Trust is a human emotion that has been injected into digital systems for no reason."

He gave the example of infamous data leakers Edward Snowden and Chelsea Manning for how the trust model fails to protect digital assets, as well as for underlining the role that identity management should play in zero trust systems.

In both cases, Snowden and Manning — a former National Security Agency computer intelligence contractor and a former U.S. Army soldier, respectively — were "trusted" users, using "trusted" devices. They were able to get past powerful authentication systems. They were also authorized to access information that they never should have had access to, and then downloaded the information.


Moving from a scenario where there's a user who's trusted to one in which, by default, all users are denied unless they have a reason to access the data in question, is both a technical challenge as well as a core philosophical/strategic shift. Both are

key to zero trust. Considering that, as we learned previously, 62% of teams are using shared team logins, it's a pretty heavy cultural lift.

The main takeaway is that zero trust is a strategy, philosophy, architecture — and not a tool or technology. There are tools that will help you implement zero trust, but effectively implementing zero trust requires much more than purchasing software.

CHAPTER 05

Zero Trust in a Cloud Native World

 If you're going to move to a cloud native architecture, you need a matching security model. Is there any way other than zero trust to secure a cloud native system? “The short answer is no,” according to Tipirneni, of Tigera. He's seen people try, but they invariably end up with a very weak security posture.

Zero trust emerged as people started to use laptops and connected to email from outside the corporate network. The concept of zero trust has proved useful as more companies have moved to the cloud, [a trend accelerated](#) by the pandemic.

By “cloud,” we could mean cloud native applications as well as traditional cloud SaaS applications, like Salesforce, or even running a monolith application in the public cloud.

Connecting to an application, like Salesforce, would make a perimeter-based security approach ineffective, because in such a scenario a portion of your company's resources are located “outside” of your secure network. They would be hosted by Salesforce, which has to integrate into your system, creating access points that have to be secure yet able to communicate.

A distributed, cloud native application — whether it runs in the public cloud, hybrid

cloud or even in a private cloud — also can't be adequately protected with a perimeter-based system, because both users and resources are ephemeral and distributed.

“Effective zero trust has to be applied at all layers of the stack. This is one of the reasons that legacy organizations often have a hard time putting zero trust into practice — it will often involve rearchitecting applications from scratch.”

“There are so many access scenarios today within the enterprise network, from computer-to-computer users, to external or internal computers, and so on,” said Belkind. “As enterprises are going to the clouds, the amount of such scenarios grows.”

To implement zero trust, security organizations need to evaluate all of the different access points into the surface they want to protect. In a cloud native environment, the number of access points can be enormous and ever-changing, as Kubernetes clusters spin up and down.

“They could also be accessing cloud services,” Tipirneni said. “For instance, maybe they're talking to an API, like Twilio. Maybe they're accessing an application like Salesforce, or maybe they're accessing a cloud service like AWS RDS [relational database service].”

So you need an architectural map to understand everything the application is connected to. If you have a zero trust strategy implemented, everything will be set to deny access by default. So proactively allowing the necessary requests, from the appropriate places, has to be part of the application development process.

Designing Architecture for Zero Trust

Successful implementation of a zero trust strategy has implications not only for how the security tools or security program is structured, but also for the architecture of the application itself.

In addition, effective zero trust has to be applied at all layers of the stack. This is one of the reasons that legacy organizations often have a hard time putting zero trust into practice — it will often involve rearchitecting applications from scratch.

Focusing on Identities, Not Networks

Regardless of where your deployment target is, zero trust requires security teams to fundamentally stop thinking about networks.

“You cannot keep thinking that, at the end of the day, it will be passing through switches and routers,” Belkind said. “Your security policy supersedes that.”

Zero trust focuses on identities instead of networks, so a conversation about zero trust would instead be about access points, identity controls and attack surfaces. You cannot build a zero trust system without a robust identity infrastructure, including both authentication and authorization.

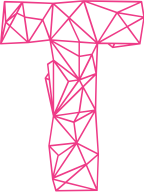
“Identities exist in just about every medium — whether you’re talking about cloud infrastructure, a private network and, obviously, SaaS applications,” said [Yoav Nathaniel](#), co-founder and CEO of Silk Security, a stealth startup. “Identities can be assigned to human users, system users, servers, network requests, you name it.”

So thinking about identities, in addition to users, is critical to securing an organization’s assets, particularly in a cloud context.

Zero trust is the best strategy for securing your entire stack — including all your data — in a cloud native ecosystem, because its focus on identities and limits on access remain just as relevant in a cloud native environment as in any other scenario, unlike perimeter-based security.

CHAPTER 06

Automation Holds a Key to Zero Trust Implementation

 hough zero trust is a security strategy rather than a set of tactics, implementation details do matter. There is nothing in the zero trust philosophy that says its processes must use automation, and it would theoretically be possible to have a zero trust system that depended on, for example, manual authentication and authorization.

However, once we're talking about dynamic, cloud native applications, manual security management goes from theoretically feasible to even theoretically impossible.

"If you use the architecture of firewalls, where you have to configure a rule for each of these points of access, you would have a pretty unwieldy model," said Tipirneni, of Tigera, about handling security manually.

"But it becomes impossible after the fact that most modern cloud native applications are dynamic in the sense that these containers get spun up and spun down. To go manually configure rules, it's infeasible at best. And this is where automation comes in."

[According to a data breach cost report](#) released in July 2021 by IBM and the Ponemon Institute, security automation made the single biggest difference in the total cost of

Data Breaches Cost More Without Zero Trust and Automation

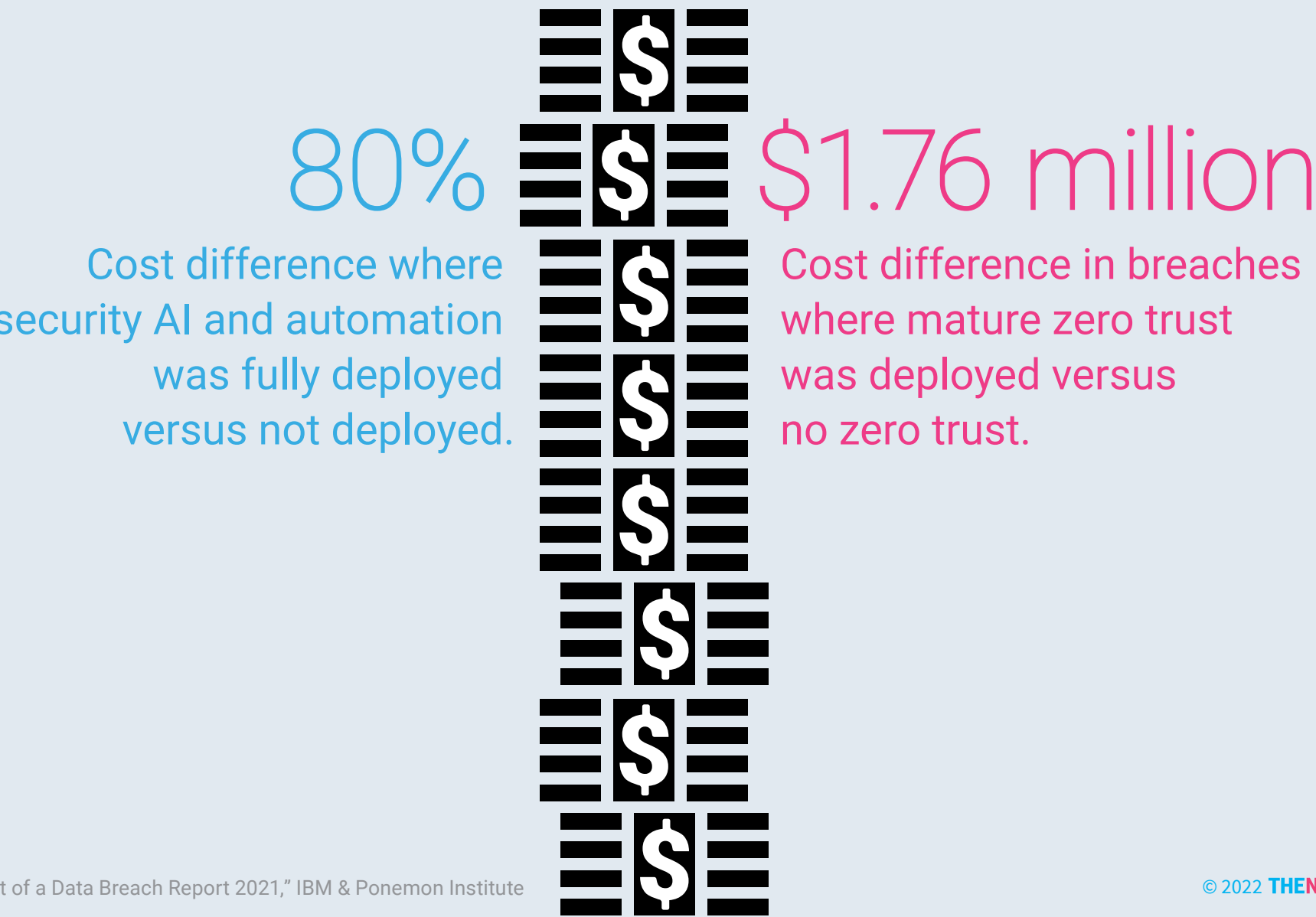


FIG 6.1: As an organization scales, automation grows more crucial to maintaining a zero trust security strategy.

a data breach. Automation makes it more likely that security best practices will be followed without fail and makes responses to anomalies much faster than if a human had to intervene.

The default in a zero trust environment is to deny access. Every time a user, computer or human, wants to access a resource, it has to ask for authorization from the network controller. Without automation, this process would be a huge bottleneck on the system.

“If your response to a security event is, ‘OK, I’ll have somebody look at it,’ you’re going nowhere,” said Belkind, of Torq. “It does not scale. The talent is scarce. The events are very heterogeneous, and business needs dictate more SaaS, more cloud, more hybrid infrastructure.”

Designing Your Automation Right

Automation is critical for zero trust, but it also has to be implemented correctly. Simply adding more automation to the mix will not help — and could even hurt, if those automation tools are allowing access too permissively.

A zero trust strategy has to inform the architecture of your automation tools, as well the rules you set those tools up to enforce.

“The only way to build a proper security automation architecture is actually in a zero trust fashion, then it falls to machine-to-machine, service-to-service communication,” Belkind said.

Security automation tools have the power to deny or allow access to any user, and if they were to be compromised it could have devastating consequences. This makes it particularly important both that security automation vendors bake in security and that users manage their automation tools carefully.

Given that reality, a new generation of security tools is emerging to support companies that need to use automation to carry out their zero trust strategies. Some of these security automation tools are low or no code, so that security specialists without programming skills can set up the automation without relying on the development teams.

The philosophy behind Torq, one of the builders of these new generation tools, is that many organizations have to manage similar security tasks, and that it’s possible to create generic security workflows that any company, regardless of industry, could use. These include automation tasks like continually updated threat intelligence, threat hunting, security bots and identity management.

“Some security processes in your media conglomerate wouldn’t be fundamentally different from my financial services company,” Belkind said.

Torq makes it possible to share not only common tools and technology, but also

common practices, so that organizations can easily learn from each other and aren't building their security strategy from scratch, either in terms of automation or cultural best practices.

Conclusion

Malicious actors aren't likely to get slower or less sophisticated anytime soon, and they will continue to attack any digital assets they can. If you create a virtual machine on any public cloud and expose it to the internet, Belkind said, within 15 to 20 minutes someone will have scanned it, identified it and taken full control.

And recovery from an attack can cost not only money and lost business and reputation, but also another precious resource: engineering time. It takes an average of 287 days to identify and contain a data breach, according to [the 2021 study](#) by IBM and the Ponemon Institute.

High-level executives are also likely to continue being held responsible for data breaches, so cybersecurity can't just remain a backwater of the engineering department. It has to be a part of the organization's strategy.

Zero trust principles, combined with security automation, are likely many organizations' best defense against the increasingly sophisticated attacks they face on a daily basis.

“Cybersecurity can't just remain a backwater of the engineering department. It has to be a part of the organization's strategy.”

Zero trust should inform both what is protected and how access is controlled, while security automation helps put those zero trust principles into practice. Together, zero trust practices and automation can also help organizations remediate incidents as quickly as possible and ensure that the initial zero trust architecture remains secure as events happen.

“It's not an autopilot thing,” Belkind said about ensuring tight security. As events happen, you have to respond to them, prioritize them and address them before they become too critical. Automation makes that feasible, ensuring that what started as a zero trust environment stays one.

About the Author



[Emily Omier](#) helps the founders of open source startups succinctly describe what their projects and products are and why people should care about them. Omier is a longtime contributor to The New Stack, where she writes a monthly column on entrepreneurship for engineers. She also hosts “Cloud Native Startup,” a podcast focused on helping technical founders with technical products build their business skills and learn from each other.

Disclosure

The following companies mentioned in this ebook are sponsors of The New Stack:
Curity and strongDM.

The New Stack is a wholly owned subsidiary of Insight Partners. TNS owner Insight Partners is an investor in Tigera, which is also a sponsor of The New Stack.

