A Practical Guide To A Zero Trust Implementation

Roadmap: The Zero Trust Security Playbook

by Steve Turner, David Holmes, Chase Cunningham, Jinan Budge, Paul McKay, Andras Cser, Heidi Shey, and Merritt Maxim

March 3, 2021 | Updated: March 4, 2021

Why Read This Report

Zero Trust is becoming the security model of choice for enterprises and governments alike. However, security leaders often don't know where to begin to implement it, or they feel daunted by the fundamental shifts in strategy and architecture Zero Trust demands. However, Zero Trust does not require that you rip out all your current security controls to start fresh, and with the right approach you can realize benefits right away. Security leaders should read this report to understand the practical building blocks of a successful Zero Trust implementation roadmap.

Key Takeaways

Use Business Model Disruption To Disrupt Security

Unlike traditional perimeter-based security, Zero Trust enables the business while adapting security architecture to support new user populations (e.g., employees, partners, customers, and patients), customer engagement models, rapid cloud adoption, and new IoT devices and sensors. The COVID-19 pandemic has resulted in large-scale transformative change, requiring a rapid pivot to Zero Trust.

Start With Identity And Device Security

We consistently find that enterprises make rapid risk reductions by focusing on improving identity management and device security. These two core components of the Zero Trust eXtended (ZTX) ecosystem build confidence with executives that the organization can realize security benefits from its Zero Trust program quickly.

It's A Marathon, Not A Sprint

Zero Trust implementation is a gradual process. Defining a big-bang sprint project to move to Zero Trust is unlikely to be successful. Work with existing security capabilities and migrate gradually to the Zero Trust model. Implement significant, strategic change over a two year timeframe.

A Practical Guide To A Zero Trust Implementation

Roadmap: The Zero Trust Security Playbook

by Steve Turner, David Holmes, Chase Cunningham, Jinan Budge, Paul McKay, Andras Cser, Heidi Shey, and Merritt Maxim
with Joseph Blankenship, Stephanie Balaouras, Alexis Bouffard, and Peggy Dostie

March 3, 2021 | Updated: March 4, 2021

Table Of Contents

Related Research Documents

The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

Gauge Your ZTX Security Maturity

The Zero Trust eXtended (ZTX) Ecosystem

FORRESTER®

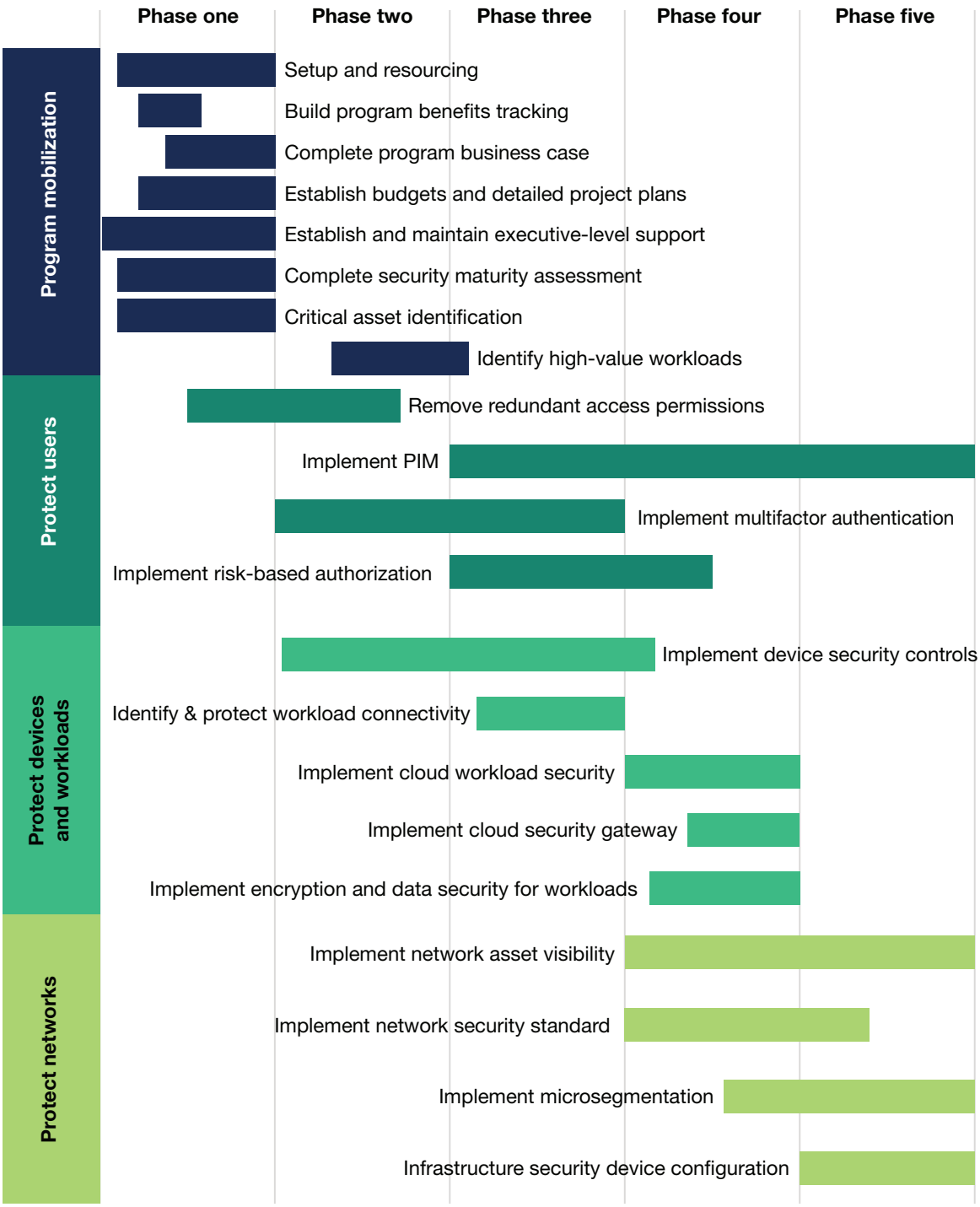
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

A Detailed Roadmap Is Vital To Achieving Zero Trust

Building on Forrester's original Zero Trust concept, Zero Trust eXtended (ZTX) is a conceptual and architectural framework for moving security from a network-oriented, perimeter-based security model to one based on continuous verification of trust.[1] While this sounds simple, it requires both a shift in mindset and major changes in the deployment and use of security technologies. Creating a detailed roadmap that outlines the main workstreams and projects necessary to implement your Zero Trust strategy is critical for success (see Figure 1). In addition, it shows executives exactly what you plan to deliver, how much they will need to invest, and what specific business and security outcomes they will achieve through this investment. Before you begin formalizing your roadmap, we recommend that you:

- **Use the Forrester ZTX framework to set your overall Zero Trust strategy.** Zero Trust (ZT) is the trend du jour in the security vendor community, giving it the stigma of a buzzword. Cut through the vendor hype and self-serving reinterpretations of Zero Trust by adopting the ZTX framework.[2] Our framework defines the seven core pillars, or components, of Zero Trust and then details the core capabilities necessary to deliver all the requirements of that particular component. For example, the data security component requires that your organization have the ability to inventory, classify, obfuscate, archive, or delete data according to policy. Today, no single vendor or provider can deliver all the capabilities and components of ZT; it will be necessary to partner with multiple providers. Building a practical and pragmatic roadmap will allow you to identify and evaluate the appropriate providers and individual technologies.
- **Recruit both business and IT stakeholders in the development of the roadmap.** Your Zero Trust implementation will require new investment or, at a minimum, shifting of investment, and it will also create an avalanche of technical and organizational change. Identify the key players that are critical for your Zero Trust strategy and recognize that you will need to include at a minimum: 1) the board members (who are often the ultimate decision-makers) and your business and IT executives (who will grant you the budget); 2) your enterprise architects and application owners (who will ensure ZT supports the broader IT strategy and other projects); and 3) your IT ops team (who will manage the infrastructure that you are building). You must understand the concerns of each stakeholder and address them. Use your interpersonal and communication skills to clarify your vision, listen to the feedback, and communicate in a manner that each stakeholder can comprehend.
- **Identify interdependencies with other security, IT, and business projects.** A Zero Trust effort needs to include existing security, IT, and business projects. In fact, these projects, from cloud migrations to engaging new business partners, can be the catalysts for Zero Trust transformation. As you recruit other stakeholders and participants, integrate the associated roadmaps into the Zero Trust effort. Ensure you properly map and clearly communicate project dependencies. Take care to consider existing requirements in your zeal; for example, microsegmentation that is too granular could disrupt existing network functions and hamper the overall schedule of IT ops' own projects.

FIGURE 1 Sample Zero Trust Roadmap

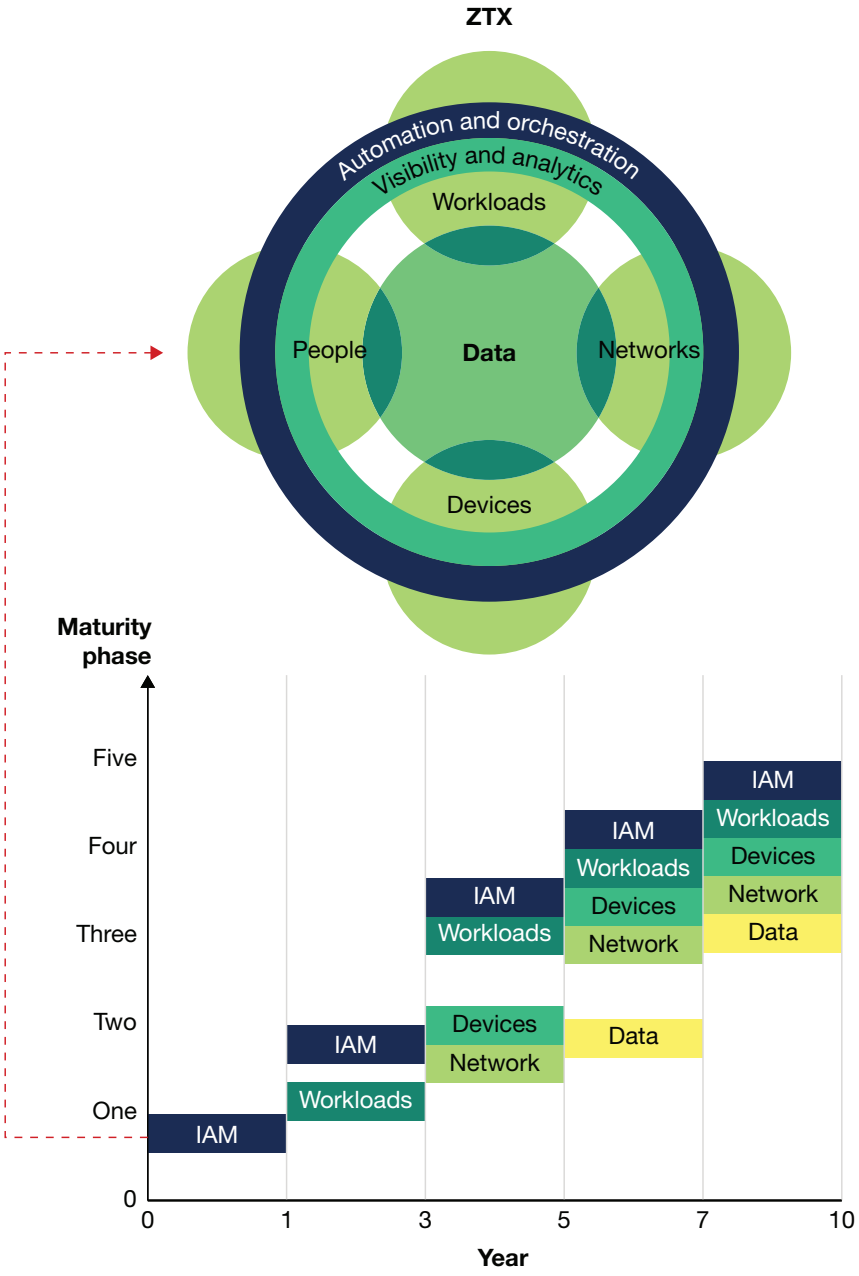


Plot Your Maturity To Discover Your Zero Trust Starting Point

Start building a Zero Trust roadmap by: 1) assessing the maturity of your current Zero Trust state; 2) understanding current business initiatives and security projects; 3) documenting where you can reuse existing capabilities; and 4) setting goals for your future maturity state and time frame to achieve it. Understanding your current maturity level and where you want to be in a given time frame will help you focus your projects and initiatives. For example, if you have a mature identity and access management (IAM) capability and have already implemented many of the necessary technologies from multifactor authentication to privileged identity management, you may wish to start with an area such as cloud workload security that is less mature. To begin creating your detailed roadmap:

- **Establish your current baseline.** Assess your current Zero Trust maturity and establish a baseline of capabilities. For example, a government client we work with in Europe conducted a maturity assessment to understand their current state. The assessment highlighted that they required a large improvement of their IAM capabilities to enable Zero Trust. Use Forrester's short Zero Trust maturity assessment to assess your current capabilities to implement the Zero Trust model.[3]
- **Identify current business initiatives and existing security capabilities.** Before starting a Zero Trust initiative, learn what other business initiatives are in play. In Forrester's experience, public cloud migrations and other disruptive IT changes have often acted as a good vehicle for achieving a Zero Trust security model.[4] For example, an Irish Bank we worked with leveraged a move to Microsoft Azure to implement many Zero Trust tenets, making use of embedded cloud capabilities that were already being implemented to accelerate the journey. Security leaders should take advantage of these changes that the business has already sanctioned to deliver Zero Trust more effectively in their organization.
- **Set your desired maturity state and time frames to achieve it.** Once you have conducted a maturity assessment, set the desired future state maturity and time frame (see Figure 2). Use the familiar 0-5 scale from the Forrester ZTX maturity assessment to target your next stage of maturity.[5] Forrester recommends a two- to three-year horizon as a typical time frame to plan a detailed Zero Trust program roadmap. Most of the clients we work with plan their Zero Trust roadmaps in this time frame to get a meaningful advance in maturity without necessarily expecting to achieve perfection. For example, an Australian financial services organization determined its future state maturity for Zero Trust and security and decided to implement this strategy over a three-year period.

FIGURE 2 Zero Trust Maturity Phases



Roadmap Considerations: Zero Trust For People

Digital businesses require platforms that are secure but also intuitive enough for users to adopt without hurting customer experience (CX) or employee experience (EX). With consumers, employees, business partners, and bots all using unique identities with differing access privileges, IAM requirements have grown increasingly complex. ZT for people, the component of our framework that focuses heavily on IAM, is often one of the least mature areas (and one of the top three vectors for external attacks). And being the least mature, it is often the easiest to quickly improve with some essential capabilities and supporting technologies. As you develop your roadmap:

- **Invest in IAM technologies that solve the most critical business or audit problems.** To justify the monetary costs and potential disruption caused by adopting Zero Trust IAM, security professionals must show how these new technologies solve the organization's most pressing people and access problems. When developing IAM improvements as an augmentation of an organization's larger digital evolution, the chances of project approval, funding, and completion skyrocket. For example, when a US health sciences company implemented multifactor authentication (MFA) and single sign-on (SSO), the implementation helped fix other issues related to compliance, security, and productivity.[6]
- **Apply least privilege.** Don't provide more access to data and apps than users need. This is one of the most important principles of solid ZTX IAM practices.[7] You need an annual attestation/access review process whereby managers and app/data owners review user entitlements and grant or revoke them in an identity management and governance (IMG) platform. Similarly, you must ensure that privileged users don't have access to admin functions on systems they don't need to do their job. As users move from job to job and project to project, be sure to retire their access to assets. Overprivileged users — employees, contingent workers, business partners, and customers — and dated access credentials lead to breaches.
- **Retire the password.** While entrenched in apps, passwords are snoopable, crackable, and stuffable, representing a significant weakness. Ensure, at a minimum, that MFA protects critical apps and data assets. Using passwordless authentication methods such as biometrics, tokens, keys, or Auth0-related solutions greatly reduces the surface of man-in-the-middle attacks. Vendors such as Google, Ivanti, Microsoft, Okta, Secret Double Octopus, Yubico, and others deliver solutions to help kill the password.

Roadmap Considerations: Zero Trust For Workloads

After you have started your IAM projects and initiatives, you need to determine the next Zero Trust pillar on which to focus. The maturity model that you completed in phase one will help you choose your next Zero Trust initiative. For many organizations, devices or workloads will be the next initiative. The rapid adoption of cloud and the new models of computing that support rapid application development have made workload security an urgent area to mature. As you develop your roadmap:

- **Establish a robust cloud governance process and structure.** Build a repeatable process to ensure that governance is an ongoing benefit to security, not a one-time checkbox compliance exercise. Documenting the process and establishing a formal organizational structure ensures: 1) proper coverage and scope, as your organization may have many different areas and infrastructure components that it wishes to cover, including on-premises, private, and public clouds, and 2) executive support. Cloud governance should also cover cost optimization, budgets, regulatory compliance, and threat detection.[8]
- **Inventory and monitor workload configurations — before it's too late.** Because of the ease of creation, cloud workloads proliferate very quickly, often without any oversight or formal governance of cloud platform credentials, configuration settings (i.e., not leaving AWS S3 buckets world writable, etc.), and even instance creation.[9] Manual processes or IaaS-specific tools won't cut it: You need a true cross-cloud workload security solution. Vendors like CloudPassage, Qualys, and Trend Micro can help.[10]
- **Focus on cloud-native security and management solutions.** Cloud washing and dumb lift-and-shift of data and workloads to the cloud without a proper governance structure and oversight lead to data sprawl, inadequate data protection, high costs, and audit findings. The configurations and protection appropriate for an on-premises workload are rarely appropriate in a public cloud. Forrester interviewees tell us that cloud migrations are a great opportunity to replatform, reconfigure, or refactor applications to use cloud-native storage, databases, containerization, and logging.[11]

Roadmap Considerations: Zero Trust For Devices

To fully adopt a ZTX framework, security pros must be able to monitor, isolate, secure, control, and remove every device that is connected to the network at any given moment.[12] Most security teams still find securing laptops and mobile devices to be a challenge. IoT devices will make it exponentially more difficult. In the past few years, numerous compromises against a wide range of connected devices have emerged.[13] These threats rely on a range of known and unknown vulnerabilities ranging from botnets to insecure software, weak or nonexistent encryption, default plain-text passwords, and insecure communication protocols. Security pros must create a flexible architecture that can adapt to the evolving threat landscape quickly and effectively.[14] As you develop your roadmap:

- **Apply Zero Trust network segmentation to manage devices.** IoT network segmentation solutions take an existing network of IoT devices and create zones or microperimeters to help isolate IoT devices from other IT devices or networks, including the ability to quarantine potentially infected or compromised devices from propagating malware. Segmenting user and device traffic away from the rest of the network can significantly reduce the risk of cybersecurity incidents.
- **Harden IoT devices.** IoT device hardening solutions enable IoT device and data integrity through capabilities such as secure firmware, trusted execution environments obfuscation, or binary modification to help minimize the risk of device/data tampering and unauthorized access and use of the IoT device and its data. When implemented, device hardening can support secure

communications, signed software delivery, and secure patches and application updates. This category can include scenarios such as device-based lockdown and application sandboxing. Vendors in this space include Cisco, Infineon, Intel, and Thales.

- **Curtail user risk created by BYOD policies.** Endpoints are not "yours" anymore. BYOD and the increasingly mobile workforce have eliminated the control IT used to have over endpoints that connect to enterprise networks and access data. Minimize issues by negating the overt threats that endpoints present such as malicious software infections, ransomware events, and malware. Conduct health checks on endpoints before allowing them to connect to your network or access systems. Cisco (Duo), Ivanti, Microsoft, and Unisys have device health checking that can be applied in this use case. Use application allowlisting to shut down all the non-used and possibly threat-riddled apps your users want to run on their BYOD devices. Act prescriptively to gain some control by using software-defined networking (SDN) solutions that push the fabric of your enterprise security out to the endpoint. It may not be "your" endpoint, but it is your network, and you can enforce your security policies on those endpoints if you do it right.

Roadmap Considerations: Zero Trust For Networks

Contrary to vendor marketing, the perimeter did not disappear: Our perception of the network perimeter has evolved. The perimeter is now "the edge" of your network, whereby users touch or connect to the enterprise. Activate a core principle of Zero Trust by redrawing logical segmentation boundaries around network assets and increasing isolation between segmentations. Authorize and log all access at segmentation boundaries and inspect and log all activity within each network segmentation. As you develop your roadmap:

- **Redraw the boundaries.** Draw boundaries to protect resources, not networks. For most organizations, that means *segmenting around an application and its associated hosts, peers, and services*. The segmentation policy defines the access that each group has with another group. For example, the application tier can talk to middleware, which can talk to databases, but the application tier (where most exploits will happen) cannot access the database tier (where the crown jewels are) directly. The baseline, if generated by sensors, will often include the suggested segmentation policy. Review it for anomalies before enforcement. Enforcement of the segmentation policy can be done at each host (via an agent) or via virtual network routing. Host-based agents are the most common, but some users shy away from them for fear of having to deploy those agents on tens of thousands of endpoints. In fully virtualized environments like VMware, a hypervisor component enforces the policy.
- **Push controls to the "edge" of the enterprise.** There are multiple approaches to leveraging the existing north-south perimeter as an inspection zone for all human-generated traffic. Web gateways operating in explicit-proxy and transparent modes can detect and block risky clicks and stop malware. DNS-based solutions can achieve a majority of your border security goals while being incredibly simple to deploy. Akamai has lightweight DNS solutions for the enterprise, and Webroot for SMB.

- **Use modern enterprise firewalls to augment cloud security controls.** The next-generation firewall (NGFW) was the original poster child for Zero Trust, and it is even better today.[15] Today, these appliances are stuffed with crypto chips to decrypt and inspect all traffic transiting a boundary, but virtualized use cases are finally becoming common, too. In the cloud, you can now insert a layer of autoscaling virtualized firewalls or Trend Micro's IDS/IPS behind a gateway load balancer to inspect your application traffic. Many vendors, including Check Point, Cisco, and Palo Alto Networks, are also integrating the management of container security policies and cloud firewalls into their cloud-delivered or cloud-connected security dashboards, signaling a path forward where third parties manage cloud objects on your behalf.

Roadmap Considerations: Zero Trust For Data

ZTX is a much more data- and identity-centric approach to security than a network-focused one — the historical approach.[16] This involves building capabilities for visibility into the interaction between users, apps, and data across a multitude of devices and the ability to set and enforce one set of policies irrespective of whether the user is connected to the corporate network. This is not easy and is compounded by the challenge of understanding what is sensitive and valuable data for the organization today. Typically, basic data security controls are already established due to compliance requirements; organizations feel they have stopped the bleeding, buying themselves a bit more time. However, you need to evaluate all the Zero Trust pillars together in the context of your critical applications, data, and assets. As you build your roadmap:

- **Define your data to understand what you must protect, where, and how.**[17] This includes building capabilities for data discovery and classification to help identify where data is located, and what is sensitive data. These capabilities are readily available today as a feature of other technology offerings (e.g., Microsoft Information Protection) as well as from specialized offerings like BigID, Boldon James, and Titus. Work with your risk and privacy organizations to help define the policies around this.
- **Dissect your data to understand its value and lifecycle, and threats to it.** This data intelligence provides business and contextual insights about data to help guide policies and controls. It requires processes and technologies to help answer questions about your data, such as: How does this data flow to produce a business outcome? Who is using this data, how often, and for what purpose? Why does the business have this data, how is it collected, and what is its useful lifecycle? What are the consequences if data integrity is compromised? In addition, understand the threats to your data collected from other security tools in your environment, such as DLP and EDR, to help guide decision-making.
- **Defend your data through four core measures and enabling technologies.** These include controlling access, inspecting data usage patterns, defensible disposal of data, and obfuscation. There are many key technologies to support data security and privacy.[18] Encryption alone

encompasses a variety of separate offerings from email encryption to database encryption, to support protecting data in its various states (at rest, in transit, and in use), as well as innovations like homomorphic encryption and quantum-safe offerings.[19]

Recommendations

Bring Your ZT Strategy And Roadmap Right To The Board

CISOs have become common fixtures in boardrooms, communicating complex issues and engaging board members' and executives' hearts and minds on the topic of security. This is shifting the boards from having a vague awareness that security threats are real to having an actual understanding of what these threats are and how to tackle them. They are asking tough questions that increasingly demonstrate they understand that the old way of doing security is no longer sufficient. Courageous CISOs are taking Zero Trust to the boardroom. To do this successfully you must:

- **Be clear that ZT is what will ultimately get you customer trust.** Boards finally understand the importance of customer trust to their overall strategy, and this has allowed many CISOs to show how security engenders trust. To some boards, the concept of Zero Trust seems at odds with engendering trust. Don't get caught up in unhelpful nomenclature debates, and work with your board to: 1) determine the best language to use (a CISO told us that his organization decided that its board didn't want the strategy to be called Zero Trust, but CompanyXYZ Trust, to reflect that this is a strategy which ensures trust) and 2) communicate that regardless of the name, ZT is an architectural concept designed to ultimately protect your most valuable asset, hence protecting your employees, customers, and society.
- **Build engaging ZT content and meet your board's expectations of you as a leader.** Board members expect a partnership with their CISO in which they can have regular and clear conversations about security. They also expect a security team that manages cybersecurity like any other risk.[20] What they get instead is a siloed cost center that uses its own language, one-way overly manufactured security presentations, and a whole bunch of tech speak. Close that gap by building engaging content, via gamification, for example, focus on impact and likelihood rather than fear, uncertainty, and doubt, and get executive coaching on the ever-important skill of communication.[21]
- **Translate technology needs to business benefits.** A thoroughly prepared budget is always a must when implementing a new strategy, and a Zero Trust transformation is no different. Don't focus your budget on validating more technology just to acquire more technology. The goal of security is to make business better and better protect your customers' data, not have more cool security tools. If you are doing this right, you should be culling technologies that don't align with business needs and removing solutions that aren't optimal for your strategy. Demonstrate how your Zero Trust initiative enables business initiatives like digital transformation, cloud migration, and enabling a remote workforce. This will allow you to shine as a business leader, not just the "security person."

Endnotes

[1] See the Forrester report "The Zero Trust eXtended (ZTX) Ecosystem" and see the Forrester report "No More Chewy Centers: The Zero Trust Model Of Information Security."

[2] See the Forrester report "The Zero Trust eXtended (ZTX) Ecosystem."

[3] See the Forrester report "Gauge Your ZTX Security Maturity."

[4] Several Forrester reports summarize the rate of public cloud adoption in the European and Asia Pacific regions. See the Forrester report "Adoption Profile: Public Cloud In North America, Q2 2020" and see the Forrester report "Adoption Profile: Public Cloud In Europe, Q2 2019."

[5] See the Forrester report "Gauge Your ZTX Security Maturity."

[6] See the Forrester report "Build Your Identity And Access Management Roadmap."

[7] See the Forrester report "The Future Of Identity And Access Management."

[8] See the Forrester report "Hybrid Cloud Security Best Practices."

[9] See the Forrester report "Best Practices: Cloud Workload Security."

[10] See the Forrester report "The Forrester Wave™: Cloud Workload Security, Q4 2019."

[11] See the Forrester report "Best Practices: Cloud Governance."

[12] See the Forrester report "The Zero Trust eXtended (ZTX) Ecosystem."

[13] See the Forrester report "The State Of Endpoint Security, 2019."

[14] See the Forrester report "The Future Of Endpoint Protection, 2019 To 2024."

[15] See the Forrester report "Build Security Into Your Network's DNA: The Zero Trust Network Architecture."

[16] See the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[17] See the Forrester report "A Five-Step Strategy For Data Discovery And Classification."

[18] See the Forrester report "The Forrester Tech Tide™: Data Security And Privacy, Q3 2019."

[19] See the Forrester report "Use Advanced Encryption For Data Security."

[20] See the Forrester report "How To Talk To Your Board About Cybersecurity."

[21] See the Forrester report "Harden Your Human Firewall."

FORRESTER®

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.