The Zero Trust eXtended Ecosystem: Data

Landscape: The Data Security And Privacy Playbook

by Heidi Shey and Chase Cunningham

August 11, 2020

Why Read This Report

Data security is a key pillar of Zero Trust. Security leaders must use standalone data security technologies as well as data security capabilities within adjacent security technologies and technology platforms to enforce data security and privacy policies. This report highlights key categories of tools and controls for data security and intersections with technologies that support the ecosystem of adjacent pillars of Zero Trust: workloads, networks, devices, and people.

Key Takeaways

Data Isn't "Data" Anymore

The old paradigm in Zero Trust — discover the data, categorize it, and secure it — doesn't cover the entirety of data security in today's Zero Trust eXtended (ZTX) world. Instead, you must first understand what this new "data" is.

The Who And The What Both Matter For Securing Data

Questions about who, what, where, and how all matter. Who's accessing that data and what they're doing with it matter most. If you don't know those things, you're essentially guaranteeing a future security breach.

Behavior Is The Key

Data loss prevention (DLP) and overt "blocking" of data usage isn't the solution. Accept that you must use behavioral monitoring to gain insight into the potential problems with data inside your organization — and then address the anomalies.

The Zero Trust eXtended Ecosystem: Data

Landscape: The Data Security And Privacy Playbook

by Heidi Shey and Chase Cunningham
with Amy DeMartine, Kate Pesa, and Diane Lynch

August 11, 2020

Table Of Contents

Related Research Documents

A Practical Guide To A Zero Trust Implementation

The Zero Trust eXtended (ZTX) Ecosystem

Zero Trust For Compliance

FORRESTER®

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

“Data” For Zero Trust Isn’t What It Used To Be

In early iterations of Zero Trust (circa 2010), the idea was to find the data, categorize it, and then segment networks and access to that data. Today, data is no longer just an entry in a database, a field in a spreadsheet, or a file on a network share. Security professionals must dial in on the totality of what’s critical to the business and consider that as their data.

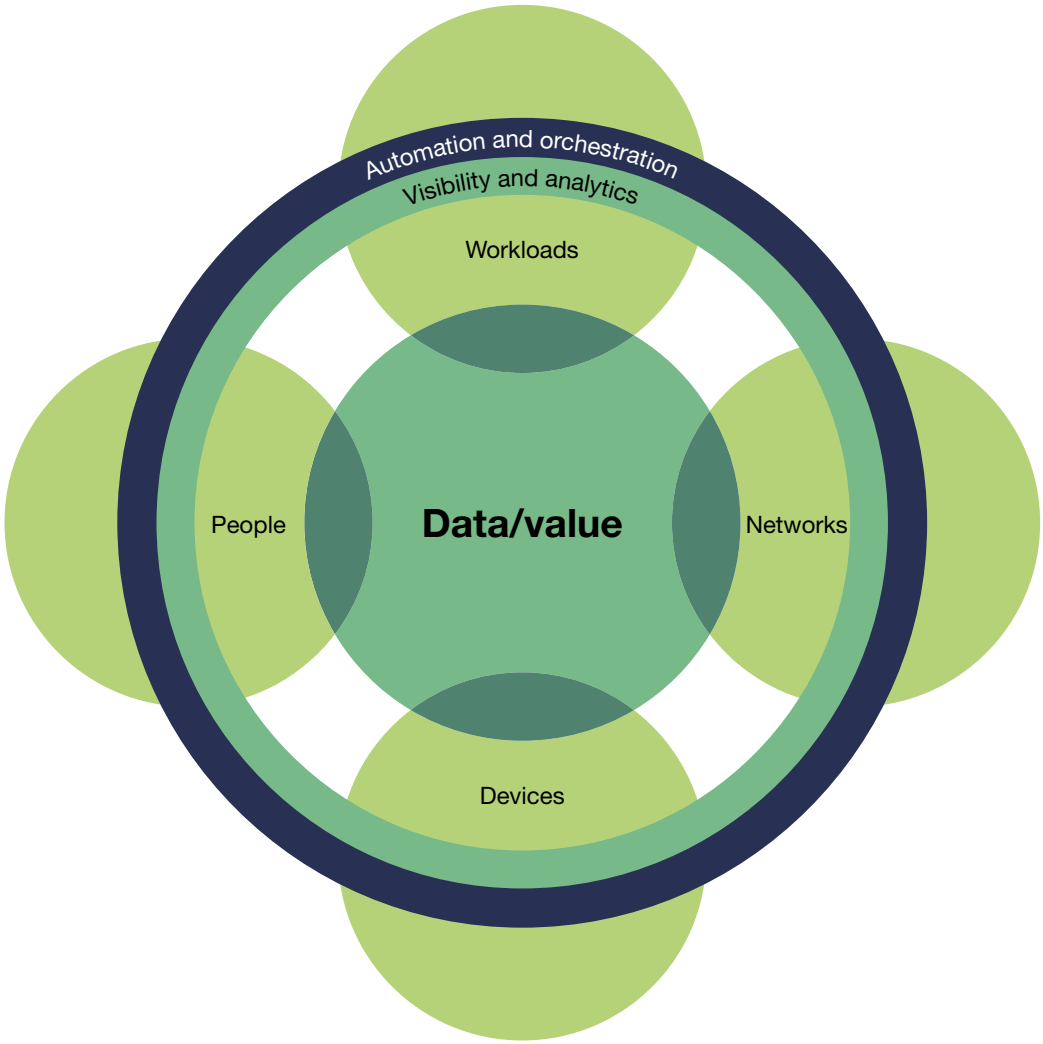
- **What remains unchanged: The usual view of sensitive data still applies.** This includes regulated data (personal data, personal cardholder data, and personal healthcare information) and intellectual property. This data exists in many forms: in real time via voice and video communications or in a database, a file, an email, or an SMS.
- **What’s different: You must defend your additional sources of value.** In truth, what we considered solely as “data” is now really “value.” Whatever is of value to your business is the most critical asset to focus your defenses around, and you should defend that value at all costs. If ransomware struck today and locked portions of the infrastructure down, what pieces of that infrastructure contain critical information that would harm your business? There’s operational data, data about your data, business processes, and more — that’s the value you must protect.

Securing Data In A Silo Is A Failed Approach To Zero Trust

A siloed approach is a failed approach that misses out on broader context and signals from your environment and the individuals who access and use value-centric data. The value you get from your data doesn’t live in a single silo; it’s transitory and dynamic.[1] Trying to enable Zero Trust and ignoring that fact is a surefire way to fail. Instead, consider that:

- **Data controls intersect with the other pillars of Zero Trust.** Data is one of several pillars to enable a Zero Trust approach (see Figure 1). Your controls for data security need to intersect, and interoperate, with other pillars — workloads, networks, devices, and people — to make Zero Trust capabilities useful for the business. These intersections may be native features of a technology offering, or you may achieve them via integration. Without visibility into the interaction between users, apps, and data across a multitude of devices, you can’t set and enforce one set of policies, regardless of whether the user is connected to the corporate network.
- **Data controls cause friction and hinder value creation when they lack context.** This is why traditional DLP failed: There was no context to provide confidence for blocking data movement. Behavioral monitoring gives valuable insight into user activity, potentially malicious actions, and indicators of account compromise. This insight is context to enable tools, whether modern DLP or others, to take smarter actions in response. To be truly Zero Trust, you need to monitor what’s taking place and who’s doing what on your infrastructure.

FIGURE 1 The Zero Trust eXtended Ecosystem



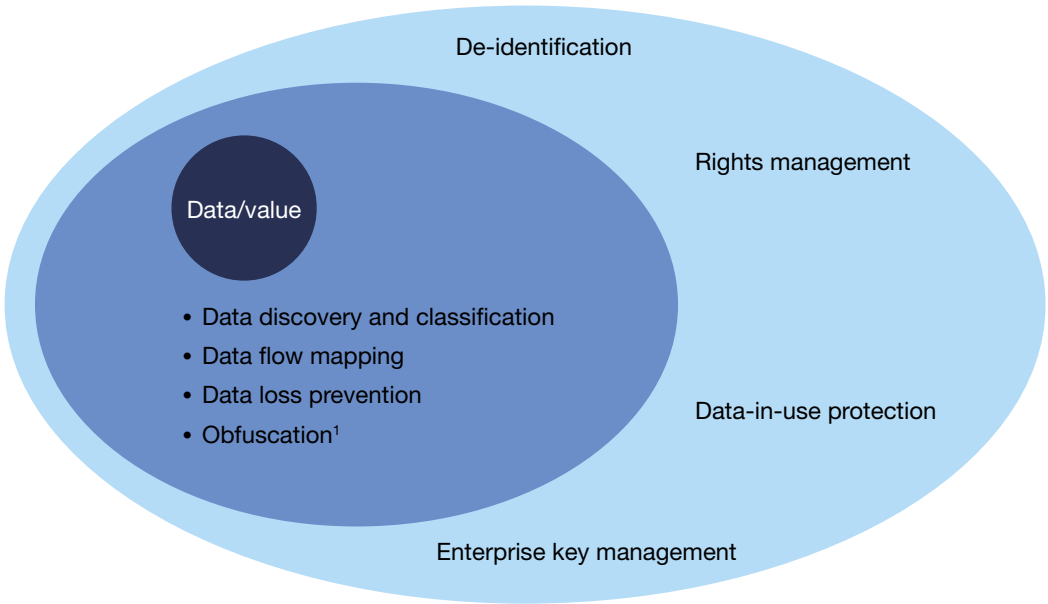
Essential Technologies And Capabilities To Enable ZTX Data Security

There are two types of essential data security capabilities for Zero Trust: core and peripheral (see Figure 2). Core data security capabilities are foundational — they apply to all firms, from multinational corporations to three-person accounting firms to companies that sell fighter jets or lemonade — and they exist in the data pillar of Zero Trust as well as the intersection points between each pillar. Peripheral capabilities are still important and in use for specific use cases or in certain types of organizations, such as large firms that are more likely to have a need for enterprise key management,

while healthcare or insurance firms that deal with lot of personal data will need de-identification to do analytics on or share that data. Peripheral capabilities aren't for data security neophytes; don't prioritize them over implementing core capabilities. For ZTX data security, firms must:

- **Establish a data control foundation with core capabilities.** These include data discovery and classification, data flow mapping, data loss prevention, and obfuscation (see Figure 3). Building up your core enables you to understand what data you must protect, gain visibility into how you use and move it across your organization's environment, and implement a key data-centric security control — obfuscation.
- **Enable the data security capabilities that sit at ZTX intersection points.** For example, as a core capability, obfuscation is typically a key capability available from a variety of technologies that sit at the intersection of securing infrastructure and data (see Figure 4). These intersections matter; secure the infrastructure and enable Zero Trust at every point you can, and the data becomes more secure by default.
- **Expand on a foundation as they continue to improve data security maturity.** Examples of additional capabilities and controls can include, but aren't limited to, de-identification, data-in-use protection, and rights management. These capabilities support specific use cases and functions, such as de-identification for privacy and data analytics, as well as further strengthening your data security posture in particular areas, such as data-in-use protection for secure data sharing.

FIGURE 2 Core Controls And Peripheral Controls Based On Zero Trust Maturity



1. Includes encryption, tokenization, data masking, and redaction

FIGURE 3 ZTX Data Capabilities And Example Vendors

Capabilities of Zero Trust data	Example vendors
Core	
Data discovery and classification	Big ID; Boldon James; Spirion; Titus; Varonis
Data flow mapping	1Touch.io; Io-Tahoe; IOR Analytics
Data loss prevention	Digital Guardian; Forcepoint; Geolang; GTB Technologies; McAfee; Microsoft; Symantec
Obfuscation[1]	Adlib Software; Comforte; PreVeil; PKWare; Thales eSecurity; TokenEx; Utimaco; Virtru; WinMagic
Peripheral	
Data-in-use protection	Baffle; Duality Technologies; Enveil; Inpher; Sharemind
De-identification	Anonos; Nullafi; Privacy Analytics; Privitar; Statice; Truata
Enterprise key management	Micro Focus; Thales eSecurity; Unbound Technologies
Enterprise rights management	Intralinks; Microsoft; NEXTLABS; Seclore

1. Includes encryption, tokenization, data masking, and redaction

FIGURE 4 Examples Of Vendors Supporting ZTX Intersections

Vendor	Capabilities
Examples of vendors supporting ZTX devices and data	
Absolute Software	Endpoint protection; data discovery
Digital Guardian	Endpoint visibility; DLP
Trend Micro	XDR; ESS; DLP; endpoint encryption
Examples of vendors supporting ZTX networks and data	
ColorTokens	Microsegmentation; asset discovery and flow mapping
Forcepoint	NGFW; secure web gateway; DLP
Illumio	Microsegmentation; encrypt data in motion
Unisys	Microsegmentation; encrypt data in motion; cryptographically cloak data assets
Examples of vendors supporting ZTX people and data	
Ionic Security	Data access policy enforcement; access visibility; key management
Micro Focus	Identity and access management; unified endpoint management; encryption/tokenization; data masking
MobileIron	Unified endpoint management
NextLabs	Entitlement management; rights management
Ping Identity	SSO; MFA; data access governance
Thales eSecurity	Access management and authentication; encryption/tokenization; key management
Varonis	Data access governance; data discovery and classification

FIGURE 4 Examples Of Vendors Supporting ZTX Intersections (Cont.)

Vendor	Capabilities
Examples of vendors supporting ZTX workloads and data	
Cyber Armor	Cloud workload protection; transparent encryption
IBM	Database security
Imperva	Web app firewall; API security; database security
Koolspan	Encrypted voice calls and messaging
McAfee	CASB; cloud workload security; container security; DLP
Mimecast	Email security; archiving; email DLP; secure messaging
Proofpoint	Email security; archiving; email encryption; email DLP
Wire	Encrypted group messaging, voice and video calling, and file sharing
Zscaler	Secure web gateway; CASB; cloud DLP

Broaden Your Landscape When Choosing Data Security Technologies

You'll find a dizzying array of standalone best-of-breed technologies, capabilities within a broader platform/portfolio of offerings (e.g., information protection features in O365), and features included in other security technologies (e.g., DLP capability from a cloud access security broker) to choose from. No surprise — there will be tradeoffs and benefits with each approach, ranging from interoperability to depth of control. Don't think you can pick a ZTX ecosystem vendor and be done, either. Major ZTX ecosystem vendors are typically starting from a position of strength in network security or identity, with data security as a less developed capability.[2] As you select your data security technologies:

- **Budget around an overarching data-centric strategy, not a narrow priority.** Most of the time, when we talk to security and risk leaders, they speak about trying to budget for everything at once. For example, in 2019, global security decision makers told us their firms allocated, on average, nearly 9% of their security budgets to data security; they allocated similar amounts to other major areas like network and cloud security.[3] This is really a hedge-your-bets approach to security strategy, not a focused, strategic budgeting plan. If you accept the reality that "value" is what's most important in the context of a Zero Trust strategy, you must align your budget around procuring technology that enables the strategy, with a focus on protecting what matters most all along the way.

› **Pick different technologies to support the full spectrum of data types you have.** Today, you'll see different market offerings to support controls for unstructured data versus structured data, different tools to support other types of "data" like voice calls, and emerging technologies to secure your data lakes. Despite major security vendors and tech titans like Google and Microsoft offering a comprehensive portfolio of capabilities (sometimes overlapping in functionality) to support data security broadly, organizations will need to rely on multiple vendors for different data security capabilities.

› **Consider new approaches to data security.** On the technology front, the time is ripe for innovation for data security (see Figure 5). Roughly 25% of the startups exhibiting in the Early Stage Expo at RSA Conference in 2020 focused on new data security approaches.[4] Startups are innovating in this space. Look to your existing vendors for innovation as well. For example, Code42 has a DLP-like capability that enables data tracking and constant knowledge of who's doing what with your data, but it's not a traditional DLP offering in the sense of blocking data movement.[5] Ionic Security has technology that can help isolate data from hackers on the fly.[6]

FIGURE 5 Examples Of Data Security Startups To Watch

Who	What
Concentric	Discovers sensitive data, categorizes it, and monitors for data risks via deep learning; provides a thematic, category-oriented view of your sensitive data
Cyberhaven	Discovers and monitors trade secrets in real time using data behavior analytics; traces data as it moves across your organization
Immuta	Enables automated data governance, combining purpose-based, role-based, and attribute-based controls to enforce who uses what data and why; provides data science teams with self-serve data access for data lakes
Nullafi	Secures structured data with aliases, enabling you to selectively anonymize, monitor, and sanitize your data; automates data hygiene and controls outbound customer communications
SecureCircle	Enables persistent data protection for data and derivatives of content; protects all the data and lets users decide what is unimportant; makes that decision an auditable event
ShardSecure	Breaks data into bits and distributes it to multiple local and cloud storage locations, unknown to each other; uses pointers in its appliance to reassemble data for authorized parties; secures cloud backups and enables file sharing
Statice	Generates a statistically similar, but synthetic and anonymized, data set based on your data; enables data sharing and analytics, data monetization, protection of data in the cloud, and training of machine learning algorithms

Assess Current Capabilities To Identify Gaps And Next Steps For Data

Zero Trust implementation isn't an immediate rip-and-replace strategy; it's a gradual process. Develop your Zero Trust roadmap to support your strategy.[7] Data isn't its own discrete and isolated part of Zero Trust. It's highly likely that you've already implemented many of these core data security capabilities for key control points in your organization to meet existing regulatory compliance (discovery and classification to support GDPR efforts, for example) or contractual requirements with third-party partners.[8] Understand where your gaps lie and why existing controls or technologies are insufficient to help justify additional measures to close the gaps. Take it a step further and evaluate all the Zero Trust pillars together in the context of your critical applications, data, and assets. Assess where you've currently established controls and processes (see Figure 6). As you take steps to reduce your gaps, align these efforts with your Zero Trust roadmap. At every step of the way for Zero Trust, consider the impact on data protection. This is in terms of how a process or technology is directly improving data control or providing context for making decisions for data security.

FIGURE 6 Questions To Help Identify Gaps In Data Security Controls And Processes

Oversight and capabilities for risk and compliance	
Compliance management	Do you have a function that supports the business by identifying all applicable laws, standards, and other requirements; translating those requirements into practical policies and controls; enforcing those policies and controls in a way that enables the business to operate; and measuring and reporting on the business' adherence to the requirements?
Data lifecycle management	Do you have processes and supporting technology to ensure that data is protected appropriately throughout its useful lifecycle, from acquisition/creation, during use, and through disposal (e.g., defensible deletion/ROT reduction)? This includes secure disposal/decommissioning of assets like servers and laptops.
Risk management	Do you have a set of distinct processes by which the organization identifies, measures, controls, and reports on relevant risks and reports this information to all necessary stakeholders to support better-informed decisions for protecting data?
Third-party risk management	Do you have processes to set requirements and assess vendors, suppliers, outsources, service partners, cloud providers, and other partners to ensure they maintain desired levels of security? Do you understand what data your third parties have access to, what data your organization shares with third parties, and why?
Understanding of data and data threats	
Investigations and reporting	Do you have processes to store, aggregate, synthesize, and report on historical IT and security data for legal, compliance, and risk management requirements?
Threat and vulnerability management	Do you have capabilities to assess and analyze threats to your data, identify vulnerabilities, and take appropriate action to reduce relevant risks to your data?

FIGURE 6 Questions To Help Identify Gaps In Data Security Controls And Processes (Cont.)

Controls and processes	
Access control	Do you have capabilities for data access governance, enforcing privileged user access, and enabling least privilege to data?
Cloud	Do you have capabilities to identify and protect data in cloud applications and workloads?
Data discovery and classification	Do you have processes and supporting technology capabilities to discover where your data (structured and unstructured) is located, identify what data is sensitive, and appropriately tag or label data?
Data lakes	Do you have capabilities to provide governance, protection, and enforcement of access controls for data stored within your data lake environments?
Databases	Do you have capabilities to identify, audit activity on, and protect data stored within your databases?
Endpoints/devices	Do you have capabilities to maintain the confidentiality, integrity, and availability of user endpoint devices (including desktops, laptops, and mobile), IoT devices, servers, and storage infrastructure (including backups)?
Messaging	Do you have capabilities to maintain the confidentiality and integrity of data through email, instant messaging, and other communications (e.g., text or voice)?
Network	Do you have capabilities to maintain the confidentiality of data, control data, and prevent data loss or exposure through network channels?
Secure development	Do you have processes and capabilities to ensure that the development environment is well protected against threats such as unauthorized access or IP theft?
Social media	Do you have capabilities to manage, control, monitor, and archive internal and public social media activity for security and risk management purposes?

Recommendations

Approach ZTX Data With An Ecosystem Mindset

Security professionals must use systems thinking — understanding the data lifecycle, how data flows, and what it touches — and enable controls that work together across the entire ecosystem. The other pillars of Zero Trust are not only enforcement points but also points of intelligence that provide added context to better inform your data security policies and controls, such as a login at a particular time; a specific source location; or a specific device that's missing a patch, putting it out of compliance with your device management policy. Once you've assessed the data controls you already have in place and your gaps:

- **Define your data, its value to your organization, and its interdependencies.** Data security is one of the hardest things to accomplish in a Zero Trust journey.[9] Data is so transitory, ethereal, and key to the business that impacting it can be a big problem. It's imperative to understand the value of your data so you can build security as a priority around it.
- **Augment with behavioral data to create better controls.** If your aim is to protect what's valuable to your organization, you must understand what's happening within your environment. This is the visibility and analytics ring of the ZTX ecosystem. Pull together the signals and context from a variety of sources available to you. This situational awareness will help you enable the controls and responses that matter.
- **Integrate your data approach in your journey instead of treating it as its own initiative.** By securing everything else intelligently, you're making your valuable assets more secure. Data touches everything, but focusing on this extremely difficult problem too early in the journey slows your progress toward a Zero Trust end state and leaves the data vulnerable anyway. Focus on the intersection points of each ZT pillar; data is in all of them.
- **Prioritize segmentation and least privilege as a part of the data control journey.** Plan for the worst-case scenario. If all else fails and the entirety of the infrastructure is compromised, you must have granular and vectored segmentation in place. Think of this as your Alamo — defend it now, or it's all over. If you don't have very specific and very controlled access and least privilege in place around your value-based data, you really don't have control of anything.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Endnotes

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

[2] See the Forrester report "The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019."

[3] Source: Forrester Analytics Global Business Technographics® Security Survey, 2019.

[4] Source: "Early Stage Expo," RSA Conference, February 24, 2020 (https://www.rsaconference.com/usa/expo-and-sponsors/early-stage-expo).

[5] Source: "What is Data Loss Prevention?" Code42 (https://www.code42.com/go/data-loss-prevention/).

[6] Source: Ionic (https://ionic.com/).

[7] See the Forrester report "A Practical Guide To A Zero Trust Implementation."

[8] GDPR is the European Union General Data Protection Regulation.

[9] See the Forrester report "A Practical Guide To A Zero Trust Implementation."

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

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.