Technical Manager's Guide to Zero Trust - Data

May 09, 2023

Cybersecurity Research Analyst

Alex is a cyber security research analyst at Stratascale. His background in both research and practical security gives him a unique perspective on providing security with a risk-based approach. He focuses his expertise on emerging technologies, data-driven IT strategy, and tactical solutions to large security problems.

Submitted by Alex Banghart on 9, May 2023
Technical Manager's Guide to Zero Trust - Data

Zero trust (ZT) is an approach to cybersecurity that aligns organization-wide capabilities around defense of key assets. ZT is organized around six “pillars” – identity, devices, network, infrastructure, applications, and data. Each pillar’s security team needs to both establish ZT principles within their area and work effectively with other pillars to support enterprise wide ZT strategic objectives.

Data Security is fundamental for ZT. Because most attacks ultimately target data, security leaders should prioritize data security in their ZT strategies.

The managers responsible for developing a ZT data strategy must achieve a balance. CISOs wish to have data policies enable the business and support organizational objectives, while data managers will need to develop plans to align their investments and activities all while trying to view their data from the perspective of a threat actor.

Four current trends are driving investment in ZT data strategy:

- Data sprawl.
- The death of the perimeter.
- Historical under-investment in data programs.
- Increased targeting of data by threat actors.

Given these current trends, ZT data managers must undertake the following tasks to support their organizations:

- Plan for all data sources, including data in legacy systems, and third party and external data sources.
- Ensure smooth, reliable operations throughout ZT data projects.
- Develop and communicate an evolving ZT data roadmap.
- Continually reduce data sprawl.
- Drive cultural change and adoption of novel practices.

By aligning their ZT data policies to business objectives, ZT data managers can enable the business to produce, safely process, and store more valuable data, allowing the business to improve decision making and gain competitive advantage. By effectively implementing a ZT data strategy, “ZT data managers can help drive business agility while securing against not only today’s threats but also the threats of tomorrow.”

Data Security as the Foundation of Zero Trust.

Although there are six zero trust pillars, data (along with identity) forms a foundational pillar. To quote a Stratascale SME:

“The whole goal of zero trust is to ensure that critical and sensitive data doesn’t get exposed, doesn’t get out, doesn’t create operational issues [and] doesn’t create problems for the company.”

Although some attacks simply aim to bring down services—denial of service attacks—the biggest payoff attacks and the most frightening attacks against enterprises target their data.

Ransomware can not only take down services that run on top of the compromised data, but could permanently destroy intellectual property that the organization requires to function, such as data necessary to pay employees, contact and sell to customers, produce products, or deliver core customer-facing services.

Furthermore, breaches that lead to leaks of data such as customers' personal information or payment information can result in massive damages in the form of lawsuits, fines, and reputational harm. Threats against data pose direct risk to concerns of senior executives, board members, and shareholders.

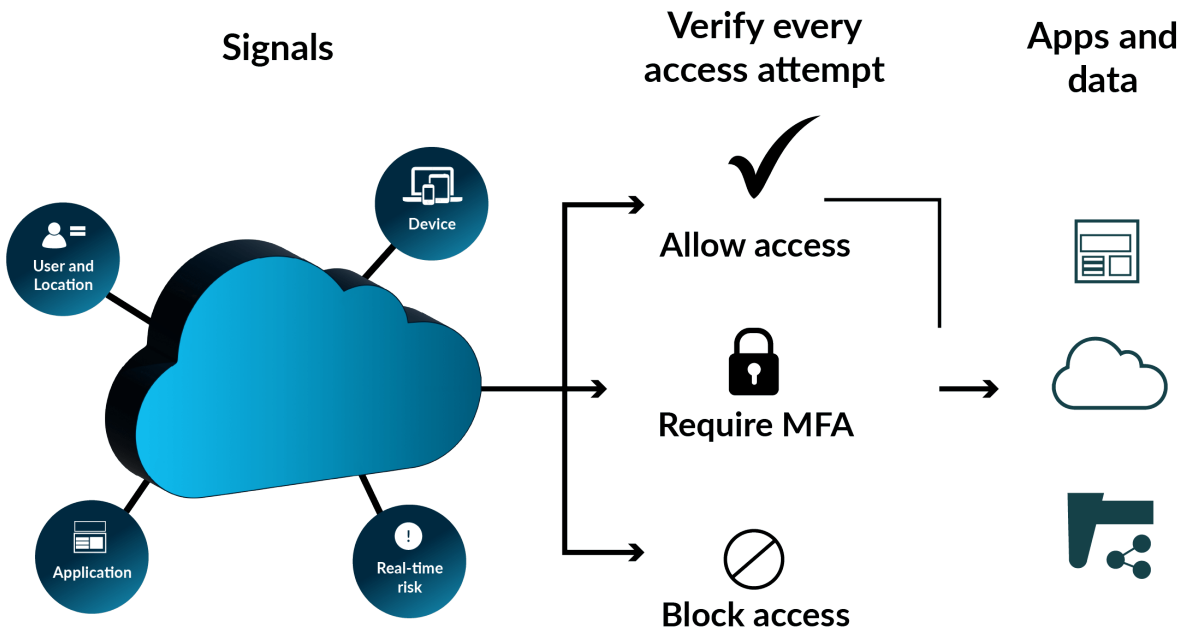
Zero trust focuses on placing the most protection around the most critical assets—the crown jewels. For modern businesses, the crown jewels are in the data.

Data Security: Context Matters

The traditional approach to data access relies on verification of the appropriate credentials. The system checks that the entity requesting the data has the right credentials, and then grants access. But credentials can easily be compromised.

In the modern world, organizations will want to consider other factors beyond credentials in making a data access decision. The decision about whether to grant access should include factors such as the following:

- What time of day is the entity attempting to access the data?
- How much data is the entity attempting to access?
- Is the data access in line with historical trends for the identity associated with the entity?
- What device is the entity accessing the data from? Is it a device they typically use?
- What level of sensitivity is the data?



Zero Trust Data Security Investment Drivers:

SMEs who contributed to our research identified three investment drivers for ZT data security:

- Data program immaturity.
- Data sprawl and the death of the perimeter.
- Increase in threat actor activity targeting data.

Data Program immaturity

Data is often the weakest link in a fledgling zero trust program. As one contributor mentioned, “If we look at the maturity of organizations, the maturity of the data tends to lag behind.” Organizations have simply not done the work to collaborate effectively across silos in developing secure and effective architectures and controls. Our SMEs developed a series of questions to ask when looking at catching up your data security program:

- Does security have a hand in designing your data labeling process?
- How are you doing data discovery?

- How do you deal with data rot (data becoming expired or no longer useful)?
- Do you have a full backup and recovery plan that works in sync with your data team?
- Are you encrypting data and what data are you encrypting or not encrypting?

Digging into these questions and understanding your data is fundamental to being able to secure it. Planning for data is no longer just about ensuring you have a large enough volume of performant enough storage. Teams should think not only about the storage infrastructure, but also about the processes and tools they will use to manage the data. A successful ZT data program requires capabilities to ensure data hygiene, labeling, and discovery.

Data Sprawl and the Death of the Perimeter

As the way we work has changed, the way we deal with data has also changed. In the old days, nearly all the important data was housed within an organization’s on premises data centers. Now, data may be kept locally or on a variety of cloud infrastructure or SaaS platforms. Data is at a greater risk because of the complex, widespread, and dynamic nature of modern IT environments, which results in "data sprawl."

Specifically, SaaS provides a unique set of challenges with managing data. The use of hundreds or even thousands of SaaS applications by tens of thousands of employees can lead to the potential for hundreds of thousands of different classifications of data. The way in which data is collected, analyzed, and shared among these apps and users is not consistent, leading to mismatches and inefficiencies. This mash-up can result in sales teams using a variety of scripts, marketing teams implementing inconsistent messaging in different regions, or analytics teams spending excessive time on data organization. As more data is generated through the use of multiple SaaS applications, teams within organizations risk working with different "languages" of data, which can lead to silos and inefficiencies, rather than fostering collaboration and amplifying insights.

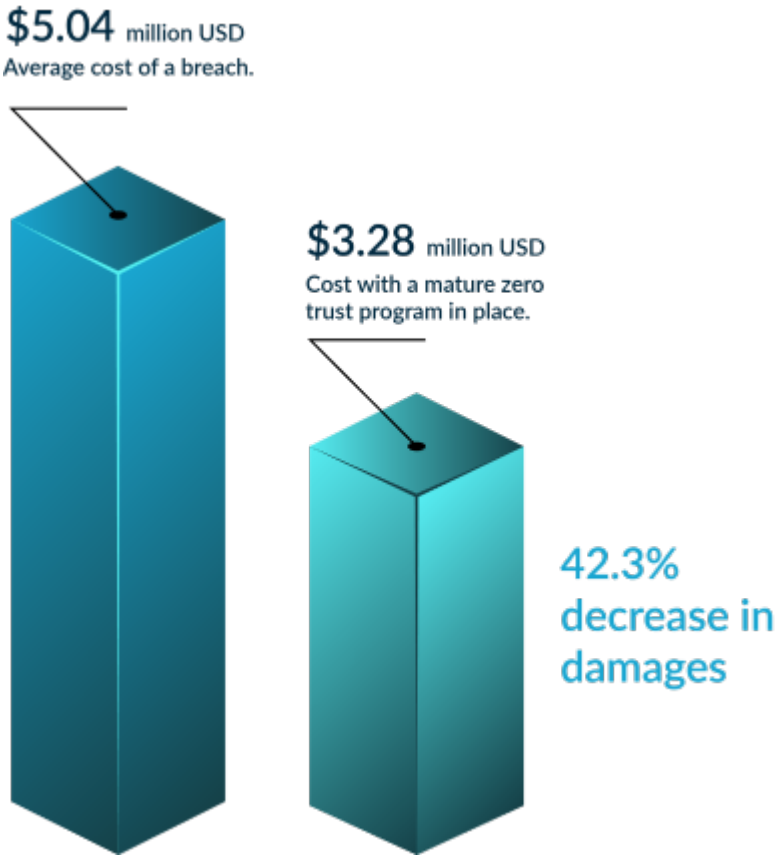
When we combine SaaS with the proliferation of public cloud environments, along with the rise of hybrid work and bring-your-own-device (BYOD), it’s clear that the concept of the perimeter has become obsolete. One SME put it,

“We’re not worried about the perimeter and being able to stop everything that is going out there. We’re worried about the data itself, where the data is going and how it’s going.”

The sprawl and complexity can lead to a great deal of risk, as organizations can lose visibility into where data is and which entities are accessing it.

> To quote a SME: “data sprawl has taken us over, **data sprawl will kill us all.**”

Increase in threat actor activity targeting data



Modern-day attackers have been focusing their efforts on data pieces, driving organizations to demand more robust data security programs. It’s no longer just about ransomware. A contributor explains, “you're starting to see [attackers threaten to publish] lists of names or lists of information, [rather than just leave the data] encrypted and unusable. Because the threat landscape is targeting data more, you're now starting to see the cyber security controls and requirements focused more on what data is.”

An effective zero trust data program can not only reduce the risk of a breach, but also reduce the impact if and when a breach does occur. For an organization without a zero trust program, the average cost of a breach is $5.04 million USD, whereas someone with a mature zero trust program faces an average cost of $3.28 million USD, a 42.3% decrease in damages.

Key ZT Data Security Priorities

Working on a ZT data security program may seem overwhelming. To facilitate incremental progress, Stratascale recommends breaking down your ZT data security priorities into two streams: legacy data management, and managing new and external data sources.

Legacy Data Security Priorities

Defining the data you have

If they don’t have it in place already, organizations must begin by implementing data classification. Classifying data effectively requires understanding the data, how that data is being used, and then developing and implementing a classification scheme that lines up with regulatory and compliance requirements and the organization’s risk tolerance and business strategy.

Set up a data hygiene program

A data hygiene program puts in place continuous processes for cleaning datasets or groups of data to ensure they’re accurate and organized. “Clean” data is error-free, simple to understand, organized, and easy to duplicate. Your data hygiene program will require a cross-disciplinary approach to be successful, including input from lines of business, cybersecurity, legal, risk, data/analytics, and marketing.

Data forms the basis for decision-making. Making decisions based on bad data increases your risk of decision contamination. In a survey by Experion, 77% of respondents claimed that dirty data “hurt their ability to respond to market changes.”

Our SMEs identified several types of dirty data which a data hygiene program ought to address:

- Incorrect data.
- Conflicting data.
- Expired data.
- Rotted Data.

Data Mapping

Few organizations would be able to provide a confident answer if asked “Where are all your data pools (related set of values obtained from a centralized database)?” . A Stratascale SME gave an example: “We've got SharePoint over here. We've got some file store over here. We got some Boxes over there. We got some S3 over here. We've got some Azure buckets over here. We've got our EMC arrays back there that have stuff—and developers putting stuff everywhere and everybody's doing it. It's the Wild West for a lot of organizations when it comes to data.”

Organizations perform data mapping to gain understanding of where data should be located and how it should move along different data pools as it is used by users and applications.

The project team should follow six steps to create and implement data maps:

1. Determine the data fields to be included.
2. Determine standard naming conventions.
3. Define schema logic or transformation rules.
4. Test the logic on a small data sample.
5. Implement the data map.
6. Set up automation and monitoring documentation.

Data maps allow organizations to secure their data more easily, by capturing exactly the types of controls that are needed for the data in their data sources and the methods of encryption, such as whether certain data is encrypted at rest or in transit. For data maps to remain useful, they must grow and evolve over time as the business changes.

Automated Data Discovery

Many organizations have so many moving parts in their environments, that it can be easy for certain types of data to go overlooked. As a contributing SME pointed out, an organization might assume that they won't have any credit card data simply because they don't process any credit card transactions—"But lo and behold, there might be some file [somewhere in their environment] that has credit card numbers."

Organizations can address this risk using automated data discovery—setting up a tool that looks out for certain patterns and/or types of data, with the aim of finding what's sensitive. For example, a discovery tool might seek out PII by looking for data patterns such as names, dates of birth, addresses, phone numbers, financial information, health information, and social security numbers.

Stratascale recommends buying, rather than building, a data discovery tool. Most organizations will get the best return on investment by deploying a commercial-off-the-shelf (COTS) tool, which comes out of the box with existing patterns for the most common types of sensitive data.

Here are some key features to consider when looking for an automated data discovery tool.

- Prebuilt and industry-specific data classification types.
- Content-aware data scanning to suggest classification types.
- Automatic classification of security level based on analysis of the content.
- Classification lifecycle policy enforcement (automatically preventing user action unless files are classified and preventing unauthorized classification changes).

Considerations when bringing on new data sources

ZT data managers must be able to adapt to the speed of business. When a company launches new services, or onboards new external partners, there is business pressure to get integrations running quickly. But data is high risk, so ZT data teams need to enable speedy integrations not by cutting corners, but by putting in place a repeatable and scalable processes that allow for the firm to move both quickly and safely.

ZT data managers need to work with stakeholders to create a checklist based on internal business needs and ensure everything is addressed when adding new or external data sources. Stratascale suggests the following questions as a starting point for your own personalized classification program:

1. How are you tracking new data sources?
2. How will you audit your new data source?
3. How critical is the data?
4. What controls do you need to place on it?
5. Where does it live?
6. Where do the controls for the data live?
7. Where will it flow?
8. How will it flow?
9. What data silos/data lakes will the data live in?

All too often, the security and/or data teams might not be involved until the decision(s) have been made and the project is well underway. These questions need to be asked earlier in the process to enable a secure data workflow. Working to change the culture to get these teams involved earlier can enable faster throughput and can allow ZT data security teams to be seen as enablers rather than as blockers. When implementing a ZT data program, Stratascale SMEs recommend that you establish a sound communication plan to ensure that stakeholders are aware of the program and how it operates, so they can partner with the ZT data team early on.

Defining the path to ZT Data Security

Each document in the *Technical Manager's Guide to Zero Trust* series incorporates a roadmap providing practical guidance to readers looking to implement ZT within their areas.

1. Understand Data, Data Subsets, and Data Policies.

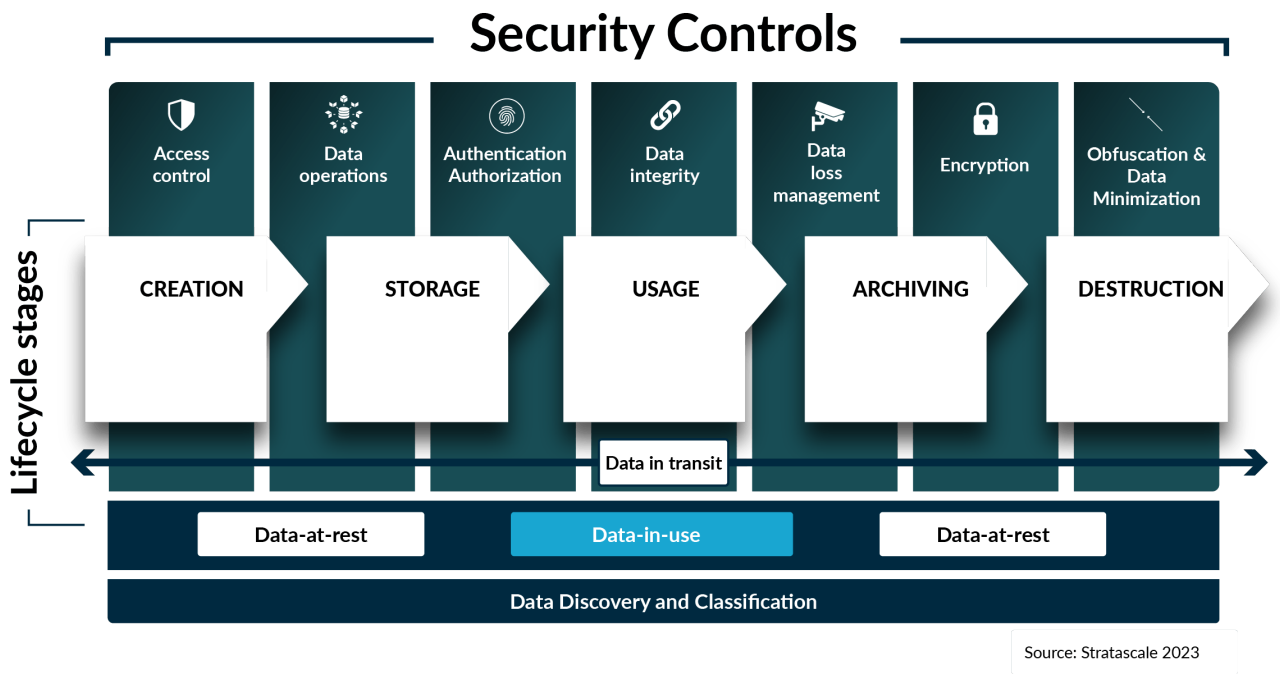
   Organizations should start their path to ZT Data security by defining their data, data subsets (a smaller sized – referential intact – set of data from a 'production' database to a non-production environment), and data policies.

   Some points to consider as you develop an understanding of your data:

   - How are we tagging the data?
   - How are we doing the policies?
     - What policies do we actually need?
     - Who develops and communicates those policies?

        - How do we enforce the policies?
    - How are we doing the procedures?
    - Do our policies follow our data mapping?
    - What is the criticality of the data based on business use and industry requirements?
    - How do we audit policies and procedure compliance?
    - How are we updating the policies with changing business and regulatory requirements?

The following graphic describes the data lifecycle and can help you plan your data policies and understanding of your data.



2. Implement Least Privilege Data Access

Implementing a ZT data strategy means putting in place least privilege access to data at scale, which requires an understanding of which entities actually need access to which data, and then implementing the appropriate controls. Data managers need to have role-based and device-based access rules to data and make sure to have these access roles both monitored and updated as time goes on. Too often people just collect access and make their credentials have more and more access to data as they move between roles in the organization or work on different projects.

A key takeaway for this section is the golden rule of zero trust. Least privilege access, giving people exactly the access they need when they need it, and being sure to **remove** that access when it is no longer needed.

To introduce this program Stratascale recommends the following steps:

1. Conduct a privilege audit.
2. Start all accounts with least privilege.
3. Enforce privilege separation.
4. Utilize just in time privileges.
5. Ensure actions are traceable.
6. Regularly audit and update privileges.

3. Complete the circle, ensure congruence with corporate governance and policies and implement continuous monitoring

Policies must have teeth in order to be effective and to prevent data sprawl. ZT data teams must drive adherence to the policies through continual enforcement and consistent communication of their importance, to instill a culture of data compliance throughout the organization. And as technologies and regulations change, the team must update the policies and effectively communicate the changes.

As noted above, automated data discovery through continuous monitoring and scanning is critical to completing the circle, because it allows you to find data that escapes the areas it is supposed to be in, allowing you not only to move that data back but also to educate the people who are moving the data in unintended ways.

To wrap it all up, a contributor said: “You've got to [monitor] because technologies are changing, because the threats are changing. There has to be this continued monitoring of the zero trust program, not just the devices but of the data as well.”

ZT Data Roadblocks and challenges

ZT data security offers compelling benefits, but no strategy is immune to real-world challenges. Where are these most likely to arise, on the path to establishing ZT in data security? Stratascale SMEs contributing to this document identified potential impediments that ZT data managers may need to overcome.

Getting tunnel vision on technical security controls and losing sight of the business context

Cybersecurity professionals often fall into the trap of deploying and implementing policies and technologies that focus on security objectives that may not line up with business objectives.

Ensuring that a ZT plan involves a variety of different stakeholders throughout the business is critical to ensure your policies enable the business rather than making life more complicated for them.

For example, if the company is deploying a new technology, the security team might want to ensure they have a perfect configuration for the solution, so they can have 100% of the controls it enables when they deploy that solution into production. From the security team's perspective, getting that solution "ready" means getting in place everything that the solution can provide, so the business gets the maximum protection from the product.

But trying to get all those controls absolutely perfect takes time. Provided that the solution can go through change control and is unlikely to disrupt services in production, it's better for the business to deploy that solution as soon as possible. The better way to run that project is to launch the solution with minimal configuration, and get 80% of its controls in place immediately, phasing in the remaining 20% of the controls through enhancements over time.

Technically-focused security staff may need coaching that the business would rather implement controls that are 80% efficient today than 100% a year from now.

Along similar lines, technically-focused personnel may advocate buying the latest and greatest and/or best-of-breed products to fill gaps in your controls. Buying best of breed seems like a no-brainer when you're focused on speeds and feeds. But when you consider the business perspective, ZT data teams would do better by starting with an inventory of their existing tools. In many cases, the team will find they can fill these gaps with unused or poorly implemented features in their current technology stack. Filling gaps in controls will existing technologies enables the security program to deliver value earlier and more cost-effectively.

Lack of resources

Implementing a ZT data program takes a good deal of time and money. And the program stretches across the entire organization—since it doesn't tie to a specific line of business or revenue-generating initiative, ZT data champions may struggle to get buy-in for the necessary investment.

ZT data managers should take the time to work with stakeholders, nurture champions within the organization, and put together a business case showing how setting up a ZT data ecosystem will allow for risk reduction, cost-savings, and increased business agility. By putting together a clear picture of the business benefits of establishing a ZT data ecosystem, ZT data managers greatly increase their chance of getting stakeholder buy-in, as well as the success of the program after launch.

> *To quote our Stratascale SME: "You can't just throw money at it; you need a plan"*

ZT Data Metrics

As part of its zero-trust research program, the Stratascale team has developed the Stratascale Zero Trust Metrics in Context and Action (Stratascale ZT-MICA) tool, which embeds a robust set of metrics that combine to provide strategic insights to executives, operational perspectives to IT and security management, and tactical data to managers responsible for ZT within each of the six pillars

Metrics contained within Stratascale ZT-MICA for ZT data security management include:

- % of all data classified/tagged.
- % of data classified/tagged as sensitive/critical.
- % of data classified as stale.
- % of data with open access.
- % of sensitive/critical data encrypted (at rest/in motion).
- % of all data encrypted (at rest/in motion).
- % of development system enrolled in TDM (Obfuscated/Generic data).
- % of systems enrolled in data discovery.
- % of systems enrolled in backup.
- % of backups encrypted.

- Total # of users with access to critical/sensitive data.
- Total # of 3rd Party users with access to critical/sensitive data.

Collectively, these measurements help data security managers to assess readiness and progress over time, and to identify and respond to areas of need before they are exploited.

Readers looking for a downloadable version of Stratascale ZT-MICA can follow this link to register for notification of release (no cost).

Zero Trust Data recommendations:

At the end of the research discussion, contributing SMEs were asked to propose recommendations that will help Stratascale client managers to succeed in establishing zero trust data security. These recommendations included:

Leverage Automation:

Utilizing automated tools allows for better coverage, faster implementation, and, most importantly, constant maintenance of your data mapping. Think carefully about the data schema you will use to implement these automated tools, and ensure these schemas are updated and maintained regularly to ensure your automated tools are keeping up to date with new technologies and threats.

Some types of automation tools and features to look out for:

- Sensitive data discovery, both at rest and in motion.
- Detection of structured and unstructured data.
- Automatic data catalog generation.
- Data lineage generation (including origin, motion, and number of copies).
- Accurate transfer logging (where is your sensitive data being transferred from and to and who is transferring it?).
- Automatic mapping of data movement and use.

Take an incremental approach to data security:

Clearly, organizations need to safeguard their data, and that requires controls. But while the drivers for a ZT program are straightforward, developing this program and

ensuring it enables the business can be challenging.

ZT data managers may feel overwhelmed by the large scope of attempting to discover, classify, and secure all the organization’s data, especially when facing a lack of data program maturity and heaps of technical debt.

The best way to tackle this issue is to take an incremental approach and be realistic in planning your timelines and goals. Present an initial program plan that focuses on the high-level business outcomes, then break those down into achievable milestones for planning the program. As you proceed with the program, ensure that the timelines you develop match the resources you have, and adjust these timelines as you gain or lose resources. Ensure that stakeholders have visibility into status, and continually keep them abreast of changes and new developments.

Taking a disciplined approach and being careful and thoughtful about your resource planning will help to drive the long-term success of the ZT data program.

Continuously review your data security

A successful data security plan requires feedback loops and regular reviews. Data lives forever and controls need to evolve as technology and threats evolve. In addition to reviewing your program regularly (e.g., annually), Stratascale recommends triggering a review in situations such as the following:

1. Major changes in the organization’s leadership.
2. Major legal or regulatory changes.
3. Major incident or policy violation both internally or externally.
4. Major technology changes.
5. Before any major merger and acquisition activity.

It is also important to look ahead for future problems during your reviews. For example, a contributor proposed, “it's five years from now, seven years or 10 years from now—my personal data is still there. My Social Security number is still the same. My date of birth, still the same. So, if I get that date and I get to quantum [computing], is my encryption good enough? So, I have to keep that continuous [threat] in that eye.”

Important ZT Data Technologies

As part of its *Executive Guide to Zero Trust* research series, Stratascale published the report, Key Zero Trust Technologies and Management Imperatives. The ZT Data section of this report highlights the following as technologies that managers should understand as they plot their ZT data strategies:

Data

Data is seen as the "focal point" or objective of zero trust strategies, which makes data protection a primary objective. The notion that data is the objective that drives both attackers and ZT defenses permeated all discussions that fed into this *Executive Guide to Zero Trust* research series. Many of the technologies and management practices used in ZT data overlap to some extent with measures taken in other pillars (or with each other), but after considering the issue, Stratascale SMEs highlighted 10 ZT data areas that require attention from security leaders.

Data governance

Data governance functions as a capstone consideration for ZT data. Broadly speaking, enterprise data governance policies have been stretched to breaking point by the exponential growth in data, data sources, data users, and data use cases: it is increasingly difficult to maintain governance policies that mandate effective data protection practices across all possible scenarios.

ZT data leaders, though, should view data governance as a means of connecting the many ZT data technologies and practices – and related technologies and practices from other pillars – with corporate business objectives and regulatory requirements. This is (or should be) a symbiotic relationship. ZT data initiatives gain credibility from their connection to governance mandates; at the same time, as one CISO contributing to this research observed, a clear and measured implementation of ZT "speaks to the maturity" of the security practice as a whole and helps reduce the time needed for review and audit.

Data discovery and classification

Research contributors saw the data inventory as essential to an effective ZT program. Organizations beginning on their ZT journey must create a data inventory as a foundational step: You "can't do ZT without that." In this pillar, though, building inventories is predicated on multiple capabilities. One is that this process starts with

data discovery. With data not fully captured in existing registries, but instead, accumulated within organizational silos, in cloud-based (SaaS) applications, or on individual hard drives, effective and automated discovery tools are essential to creating a data inventory.

The second key capability concerns data classification. Data requires stewardship and governance. Sensitive personal data needs to be managed according to policies that will stand up to regulatory scrutiny and protect the organization from fines or reputational damage. Corporate IP needs to be defended against commercially (or in some cases, politically) motivated intrusions. Other data – including outputs from applications based in various locations, which may be accessing or synthesizing sensitive records – needs to be appropriately classified and monitored on an ongoing basis.

One member of the zero-trust thought leadership group positioned the data inventory challenges in the context of inventories in other ZT pillars. User inventories or identity inventories, the contributor stated, can be assembled from existing tools. “Device inventories are a little harder, but still kind of easy,” as “enterprises have device management platforms that enable staff to identify devices, their posture, and how they relate to identities.” But there isn’t an analogous source for insight into where data is, and which data is most critical from a confidentiality (and security) perspective. “Data inventories are always the hardest,” the contributor believed – and as a result, there is a tendency to “put all these roadblocks and bubbles and firewalls and access control rules around the data.”

Absent a current and detailed data inventory, security leaders may default to these generalized controls. This approach is the antithesis of the zero-trust intention: CISOs need to identify the locations and criticality of corporate IP in order to implement data access control and focus protection on data assets.

Data inventory/catalog

This category is intrinsically linked to discovery and classification: discovery finds data, classification defines its significance, and then inventory and catalog add a centralized organization of the data, enabling it to be understood, consumed, and managed.

Data lineage

Data lineage enables understanding of the data lifecycle, including the point at which data must be archived or destroyed. Organizations tend to be far better at creating and aggregating data than deleting data that should no longer be stored – but data destruction is an important aspect of data security. Data lineage is critical to guiding decisions about data management, including data archiving and destruction.

Data access control

Data access control isn't a technology category *per se* but is one of several phrases that could be applied to systems and practices that align data access and authorization with policy and governance. The objective is to ensure that access to data is gated based on identity and is informed by the sensitivity and criticality of the data, which assumes a necessary prerequisite focus on data classification.

This seems an appropriate juncture to emphasize that access requests may come from human or non-human (e.g., IoT) users. The ability to classify these identities and devices, which relies on success in the identity and access pillars, is important to successfully managing access to data. Within the data pillar, information on identities and devices is mapped to the data inventory and used to limit data access, reducing the potential for a compromised device to harvest data that isn't logically connected to the user or device function.

Data encryption

Data encryption is (or ought to be) standard practice for security teams. It is fundamental to ZT data – protecting data that resides in storage or is "in flight" from one device, application, or user to another is a hygiene-level step in the ZT process.

Surprisingly, there are environments where security professionals eschew encryption of data in motion. Such practitioners believe that VLANs, segmentation, and other measures provide adequate protection for unencrypted data, rendering encryption in motion superfluous. SMEs contributing to this report vehemently disagree. There are many attacks (including router compromise, spam forwards, attacks on load balancers or application servers, etc.) that can open a window into traffic – and if that traffic is unencrypted, it provides a clear view of the data itself. Data

encryption, including encryption in transit, is critical to ZT data success.

Test data management

“Test data management” doesn’t generally leap to mind when data security is raised as an issue. But as one CISO contributing to this document noted, “test data is a critical, thorny issue. You need data isolation. You can have a good [test] strategy and good tools with an ecosystem comprised of knowledgeable people that can manage the process – DBAs and business professionals. But who can manage the data obfuscation?”

Again, “data obfuscation” is rarely priority #1 for security leaders. But in some contexts – notably, when the ultimate system will deal with PCI or other regulated data – it is very important. “You're not going live with the system that's never been production tested, right?”

In many corporations, there will be multiple systems under development that will process sensitive, confidential, and/or regulated data when they are in production – which means that there is a need to support multiple test environments. The CISO concluded by saying that this is “a very solvable problem on paper, but it's challenging to build up to that level of maturity.”

Data loss prevention

Data loss prevention (DLP) is a mature technology – meaning that it is likely deployed in most organizations that are pursuing a zero-trust strategy – but there is a need to ensure that DLP products and policies are consistent and integrated with ZT data and organizational ZT framework priorities. Key attributes of DLP, including visibility into the data and the ability to deploy consistent policies that map data access to device posture, are important to overall ZT data capabilities. Other ZT functions and technologies may ingest DLP outputs, such as warnings about potential exposure of sensitive data. By providing visibility into how data is used and moves and enforcing security policies that respond to content and context, DLP supports the overall ZT data strategy.

Data backup and recovery

With the huge increase in the use of cloud-based resources adding to the strains imposed by business unit data stores and files resident on local hard drives, IT organizations have needed to revamp backup and recovery approaches and tooling. The security team plays a critical role in shaping this strategy, since security issues – ransomware protection, support for audit, and compliance – feed into the backup and recovery strategy. Security leaders may also be accountable (to some degree) for Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO), which further connect data backup and recovery to the ZT framework.

Data privacy

Data privacy is more an imperative than a defined toolkit, but it is “becoming a nightmare” for security leaders and can’t be overlooked. Data privacy builds off discovery and classification and the data catalog, referencing the need to govern how sensitive data is collected, tracked, used, and shared. Data privacy ensures the confidentiality of sensitive data (such as personally identifiable information (PII) or protected health information (PHI)) – objectives that are intrinsic to data governance mandates.