Zero Trust for Sustainable Data Discovery

THE CHALLENGE

Former Forrester analyst John Kindervag introduced us to "zero trust" in 2010,and since then, it has become one of the more popular frameworks in cybersecurity. **Massive data breaches, regulatory fines and growing risk associated with data protection have proven that companies need to be more proactive about cybersecurity, particularly around data discovery for security, privacy, and governance,** and a zero trust model might be the right approach.

THE SOLUTION

Zero trust is based on the premise that not even users behind the firewall can be trusted. User error and insider threats continue to be a significant risk for organizations.

To ensure data security in the face of both internal and external threats, data discovery and control should be at the heart of organizational risk management. Organizations need complete visibility into their data - where it is saved, how many copies exist, and where the data has moved over time - in order to identify any unusual patterns or unauthorized activities that may point to the existence of an internal - or external - security risk.

Companies need to be proactive about cybersecurity, particularly around data discovery.

Organizations need complete visibility into their data - where it is saved, how many copies exist, and where it has moved.

IBM Security Discover and Classify Zero Trust Model

Zero Trust People

Zero Trust Network

Zero Trust Applications

Zero Trust Devices

Implementing a Zero Trust Framework can protect companies from advanced cybersecurity threats, data breaches, and regulatory risk while helping achieve compliance with CPRA, CCPA, GDPR, HIPAA, and any future requirements.

Data privacy and security are at the center of zero trust – and data discovery & monitoring are the most crucial steps to ensuring privacy, security, and governance.

AUTHENTICATION & VERIFICATION

The first principle of zero trust is to authenticate and verify existing data discovery processes:

- What kind of sensitive information does your company have in its network?
- Do you have a complete and updated knowledge of different networks, repositories, and applications where sensitive information is saved?
- Do you have a robust process to respond to DSAR requests as part of regulatory requirements - and can you ensure that the process is secure and private?
- Do you have a vetting process that only allows authorized personnel to access sensitive data?
- Do you have a comprehensive process to determine if/when data can be shared with a third party?
- Can you monitor data transfer and identify where and when copies of sensitive information are moved and saved?

The underlying assumption is that every attempt to access data is a threat, and every instance of data transfer and copying is a risk - regardless of the location of access or hosting model.

Building a Zero Trust Security Model

DISCOVERY & MAINTENANCE

Zero trust principles require inspection and verification of every bit and byte of data in your organizational network: discovering and monitoring data at rest and at motion, logging every network call, file access, and email for malicious activity, and identifying the location of every data instance in every repository. This is not something a human or an entire team of humans can accomplish - and certainly not in the continuous, ongoing manner required to keep up with the mutable datascape of a large organization.

Traditional data discovery tools are no more than data mapping solutions that require the customer to point them towards the location and type of sensitive data they wish to discover: they cannot locate or identify sensitive information in unknown locations across unstructured and structured files, databases, and repositories - or discover data beyond standard data.

They cannot monitor the transfer of all sensitive data records - or provide a detailed breakdown of the location of every record instance. Their limited classification capabilities make it impossible to build a full and sustainable picture of data usage.

Continuous discovery, monitoring, and cataloging are the most critical capabilities for maintaining a zero trust security model.

The right system will offer fully automated, continuous data discovery for sustainable insights.

SUSTAINABLE DISCOVERY

Continuous discovery, monitoring, and cataloging are the most critical capabilities for maintaining a zero trust security model. With robust discovery, monitoring, cataloging, and data analytics in place, you can identify sensitive data stored in different repositories, pinpoint the source and target locations of sensitive record transfer processes, and use this information to make informed decisions regarding security, privacy, and governance mandates.

Implementing a Zero Trust Model

Zero trust starts with data discovery. Here are some key recommendations for effective data discovery, monitoring, and cataloging.

DATA DISCOVERY

Figure out where your sensitive data lives, how many copies of the data exist, and who has access to it.

You have to know where your sensitive data lives and who has access to your data before you can protect it.

DATA PATTERNS

Analyze the movement of data in your organization: who is making copies, and where are those copies located? How much data is being moved around, what kind of data is transferred, at what volumes - and who is doing most of the moving?

You need to understand the patterns of data movement in your organization - and to be able to identify unusual data activity in order to identify risks and threats.

NETWORK MAPPING

You need to understand the topology of your network: which nodes are connected? Which elements can and do communicate with one another? Which elements have traffic between them - and when and how does that traffic start and stop? You have to understand communication within your network to identify potential leaks and breaches.

Achieving Zero Trust with IBM Security Discover and Classify

IBM Security Discover and Classify's network- first approach offers:

- **Sustainable Automated Discovery**:Locate sensitive data at rest/motion (transit), structured/ unstructured, and known/unknown
- **Fully Updated Catalog**: Rationalize sensitive data saved in different formats and files and create a smart catalog of all the sensitive data
- **Accurate Data Lineage**: Continuous and full visibility in the data life cycle, including data origin and where it moves over time and identifies how many copies of that data, exist
- **Transfer Logging**: Accurate breakdown of data transfer activities, including identification of which sensitive data records have been transferred, where from - and where to
- **Automatic Mapping**: Continuous mapping of network topology and communications

Organizations need complete visibility into their data: location, copies, and transactions.

IBM Security and Classify provides an accurate view of data so companies can make informed decisions.

IBM Security Discover and Classify's network- first approach offers:

- **Far less operational overhead** and is much easier to manage
- Provides business leaders with an **accurate view of their data** to make informed decisions for security, privacy, and governance
- **Fully supports any kind of operational topology**: fully on-premises, hybrid, or 100% cloud

ABOUT IBM SECURITY DISCOVER AND CLASSIFY

IBM Security Discover and Classify offers a unique and proprietary passive network packet capture process, identifying repositories and network transactions containing sensitive data throughout the organizational network. This process allows ISDC to discover any data, on-prem or in the cloud, structured or unstructured, in motion or at rest, to create a master catalog of sensitive data.

IBM Security Discover and Classify leverages artificial intelligence and machine learning to consolidate and normalize identities to provide a unified view of sensitive data across disparate repositories, data sources, applications & use cases.

To learn more about how our zero trust approach to discovery can help your business, **contact** IBM Security™ for a consultation.

IBM Security Discover and Classify consolidates sensitive data in a catalog that allows user to see data lineage, respond to subject access requests, identify production data in non-production locations, and many other security, privacy, and data governance tasks.