SYMMETRY SYSTEMS

WHITEPAPER

How Dataguard Empowers Zero Trust

What is Zero Trust?

Zero Trust is a philosophy that perceives all connected hosts, applications, and identities as untrusted; therefore requiring users to be explicitly authenticated and authorized, before granting them just the right amount of access to the applications and data they need (implicit trust). This philosophy requires significant investment in a Zero Trust architecture.

Figure 1: Zero Trust Access

Why are organizations adopting Zero Trust?

As organizations adopt cloud-based technology and enable greater mobility, they are scrambling to understand their expanded and often unknown attack surface. In the cloud, organizations must assume that everything is internet facing. As a result, organizations can no longer rely on their traditional perimeter based defense solutions to secure them in the current threat environment and are turning to Zero Trust strategies and architecture to secure their data and systems.

Zero Trust at a glance

"The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible. Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time"

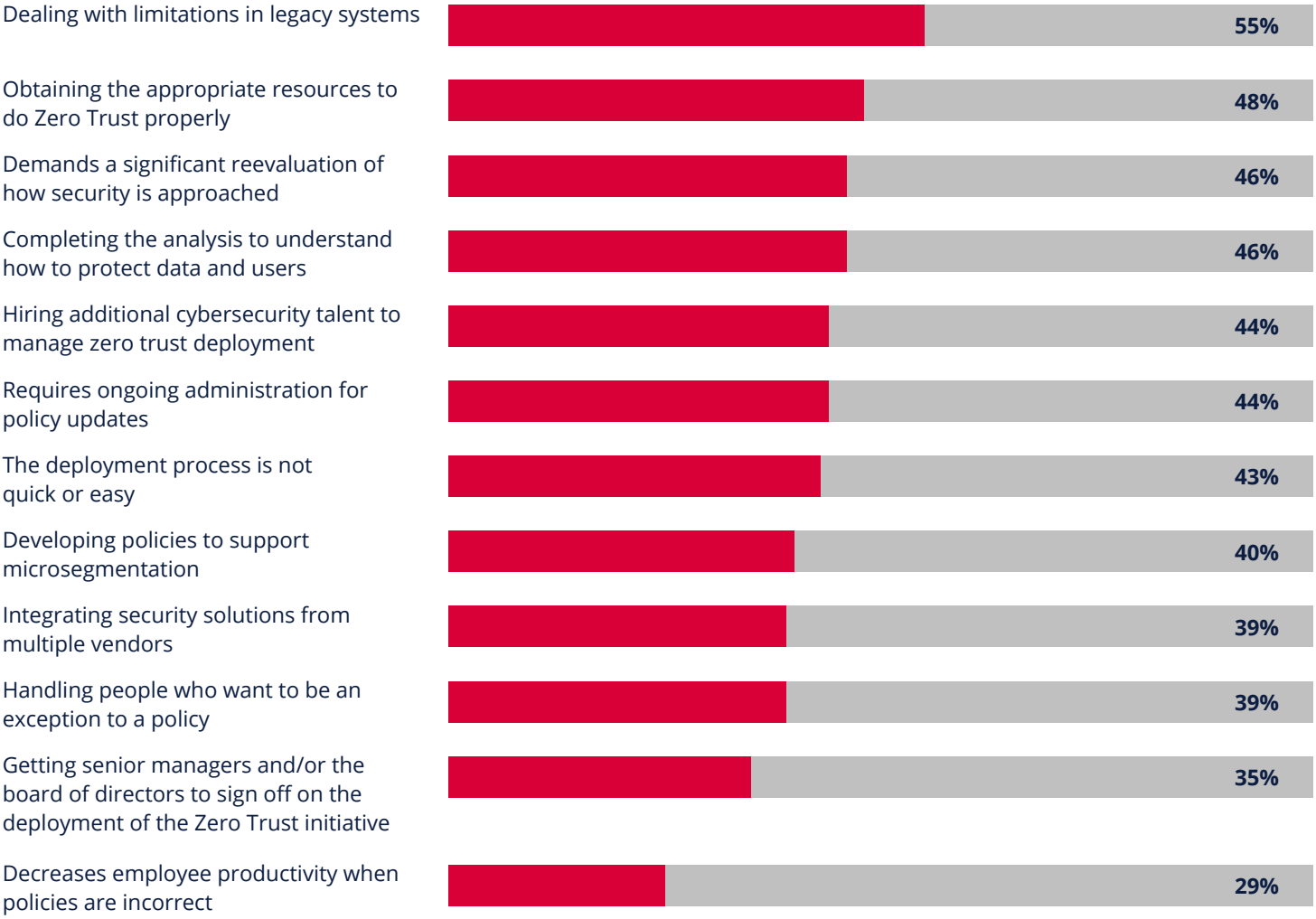
https://www.cisa.gov/zero-trust-maturity-model

Zero Trust in the cloud

Successful management of cloud environments is drastically different from our traditional approach to managing on-premise networks. Organizations not only have to adapt to the ephemeral nature of the cloud, the complexity and scale of the applications, the identities being used, but also the petabytes of data being created, processed and stored on a daily basis. These increased levels of complexity can enable greater security at a finer granularity, but too often result in misconfigurations and non-configured controls that circumvent Zero Trust controls.

A significant Zero Trust problem that remains for organizations, even when they can reliably enforce secure configuration of their cloud infrastructure, is excessive privileges. Historically organizations have had their IT administrators assign access rights to data (including admin rights) based primarily on ease and avoidance of business impact. This historical approach is simply incompatible with Zero Trust, particularly when focused on single data objects. Being able to actively restrict specific data access to specific identities requires an understanding of not, just if a specific identity has access to a given datastore, but the specific operation that identity can and is taking against a single data object within that datastore.

Key Barriers to Embracing Zero Trust



Source: Why Zero Trust is Important, Whitepaper, Osterman Research, November 2021

For successful Zero Trust in the cloud, organizations need to know with precision and accuracy:

- The identity of every given account and device on a continuous basis
- The location and flow of sensitive and critical data
- The permissions they have to access and take action on data and applications are appropriate
- The specific operation that identity is taking against a single data object within that datastore
- The record of how items above have changed over time

In particular, cloud organizations enacting Zero Trust policies to restrict resource access require:

- An accurate assessment and configuration of cloud native bi-directional permissions
- Solutions that provide evidence of operations against data, not just "access" or "permissions" to that data
- The ability to alert and take action on precise operational evidence, through integrations within their own given ecosystem of tools and solutions

How DataGuard helps organizations with implementing and maintaining Zero Trust

Symmetry Systems DataGuard allows security teams to manage their data following Zero Trust principles. With DataGuard security teams can continuously monitor and adjust identity access management (IAM) policies on individual data objects at scale. This way they can make sure that only the right users and technologies have the right access to the right data, and that authentication for those users are in line with Zero Trust requirements. Without clear, immediate, and continuous insights into data access, user permissions, and operations taken against data, security teams leave their doors wide open to data breaches, and other unintended data access.

DataGuard arms security teams with automated capabilities and alerting mechanisms to maintain true Zero Trust at the **data object level**. The capabilities provide organizations with:

Data asset inventory & data flow analysis, including:

- Detecting the presence of sensitive and confidential data
- Identification of dormant data; that may no longer be required

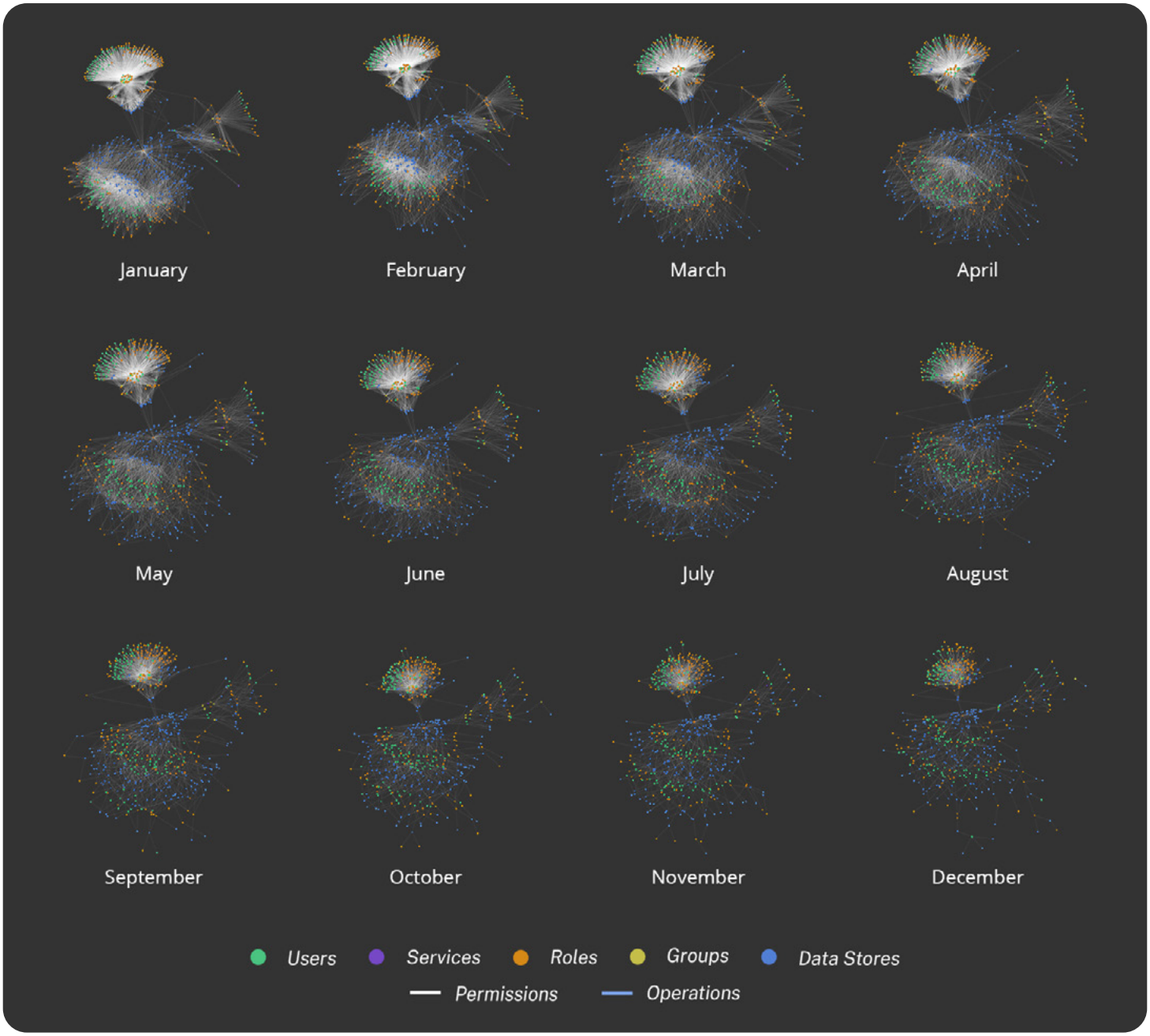
Granular zero trust at the data object level, including:

- Continuous identification and reduction of:
  - » Overprivileged users
  - » Excessive SRE or top-level admin access rights with tighter control
  - » Cross account or cross cloud operations against data
- Reduction of supply chain risk:
  - » Overprivileged vendors, partners, contractors, and third-parties, to ensure that only necessary access permissions have been granted
  - » Improperly offboarded contractors, vendors, and third-parties, so that they can ensure permissions have been completely removed and cyber risk exposure has been reduced

Continuous monitoring, including:

- Visibility and monitoring of admin accounts, break glass accounts, that unnecessarily increase cyber risk exposure
- Identifying gaps in micro-segmentation policies that create vulnerabilities
- Dormant accounts with high levels of privilege, which if activated could have a broad data blast radius
- Derived permissions, to understand how secondary user permissions or toxic permission combinations might increase cyber risk exposure, and take corrective action
- Ensuring data operations are no longer being executed after remediation

Visualize and track changes over time to data flows and operations in the cloud



Conclusion

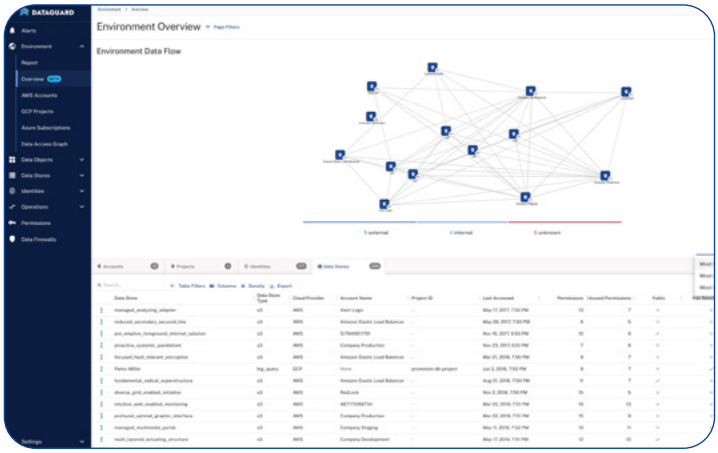
With DataGuard, organizations now have the tools and data needed to prioritize their Zero Trust network initiatives based on the **sensitivity** and **volume** of data at risk. Organizations can identify with precision and accuracy the right amount of access required by authenticated users and continuously monitor the effectiveness of their Zero Trust architectures based on the flow of data within their environment.

About Symmetry Systems DataGuard

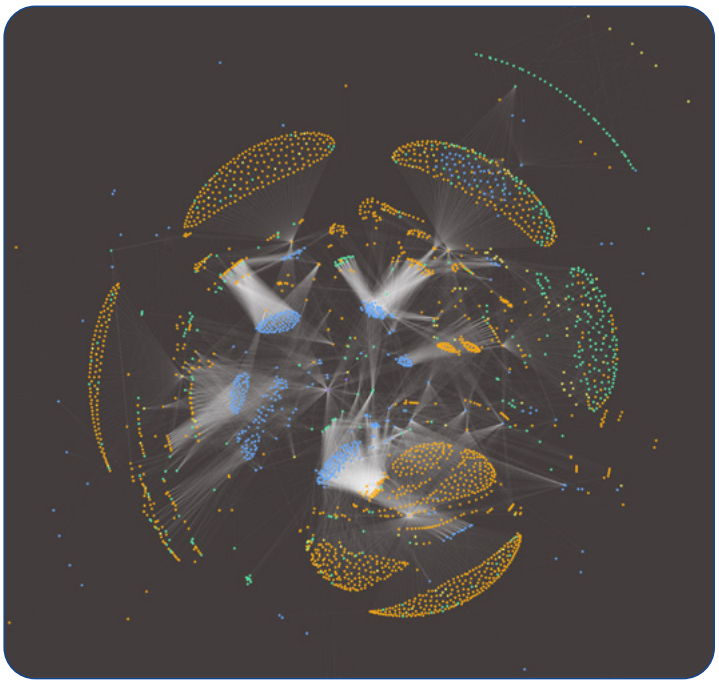
Symmetry's DataGuard is a hybrid cloud data security solution that provides a data-centric approach to enable organizations to map, secure and track identity, permissions, and data flows – **at scale in multi-cloud environments** – while providing unified visibility across these environments for cloud- and information security teams.

DataGuard is a cloud **Data Security Posture Management (DSPM)** solution that unifies visibility into data objects across all data stores, answering data security and compliance questions that **traditional cloud security tools cannot.** For example, what data is affected by a compromised credential, or an exploited web-service, or an off-boarded analyst?

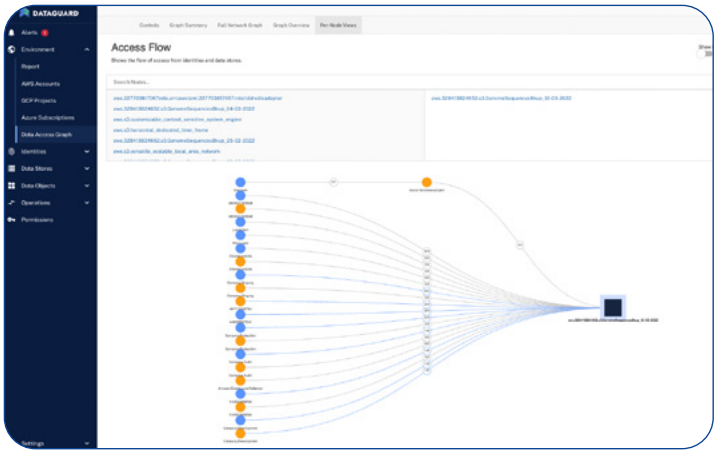
DataGuard enables cloud and security operations to understand and systematically control data risk – **defining the path to zero trust for data** – while baking in compliance and incident response. DataGuard provides actionable insights into your data flow, unlike the traditional, static views offered by legacy technologies.



Top-down view into your data environments: filter by **most data stores, permissions or identities**



Cutting-edge visualizations produced by DataGuard to help you visualise your entire environment, blast radius and more



Easily track data flows: both in and out of your environments with high accuracy

Supports a variety of integrations out of the box, so you can track IAM, Alerts and Evidence

SYMMETRY SYSTEMS
symmetry-systems.com | hello@symmetry-systems.com
LinkedIn / symmetry-systems-inc
Twitter / @SymmetrySystems