Datasheet

SYMMETRY SYSTEMS

Data Security Posture Management as a Service

We get it. We understand the monumental challenge–data security–that you are facing today. We also understand that for many organizations rethinking their approach to cybersecurity isn't easy. Pivoting from securing endpoints and the perimeter, to securing the business from the data-out can seem like a daunting task. However, it doesn't have to be.

Symmetry Systems is confident that our short term 60 to 90 day turnkey Data Security Posture Management as a Service offering will enable security organizations to quickly uncover the gaps in their data security posture and what actions to take to remediate them.

During the engagement, the Symmetry Systems data security team will become an extension of your team. They will install DataGuard, our Data Security Posture Management solution, in your chosen cloud environment, configure it, administer it, and test it against success criteria established at the onset of the engagement. Our team will make sure that you can take advantage of all of the possible business outcomes that DataGuard can deliver.

The Engagement Process

At the onset of the engagement, our team will work closely with you to define the full scope of the engagement by developing a Statement of Work (SOW). We will outline goals of the engagement and success criteria to manage expectations. To drive successful collaboration between our teams we will provide weekly updates to showcase our progress against the mutually agreed upon success criteria.

During our 60 to 90 day turnkey Data Security Posture Management as a Service engagement, our data security team will:

- Provide a comprehensive data security posture map of your cloud environment
- Discuss findings and the priority in which any challenges should be addressed
- Suggest remediations to data security challenges (e.g. dormant data stores, over permissioned identities, cross-account data flows, toxic combinations, improperly offboarded vendors, etc.)
- Set up alerts and notifications to abnormal data behaviors, potential insider threats, potential malicious actions, and more
- Stand up simple integrations or automations with third party technologies (as outlined in the SOW)
- Deliver a report along with an executive summary that measures our progress against the success criteria

Next Steps After the Engagement

Once the engagement concludes, and our data security team has met the success criteria, you have three options to continue your data security journey using DataGuard as your source of data security truth.

Annual DataGuard Subscription

You can convert your 60-90 day DSPM as a Service subscription to an annual DataGuard subscription. This way your team will continue to receive advice on how to resolve any new data security challenges, and will continue to receive alerts to abnormal and malicious data behaviors. The Symmetry Systems data security team will work with your team closely to make sure they can operationalize DataGuard. Our customer success team will of course provide ongoing customer support.

Managed Security Services Partner Engagement

Symmetry Systems is closely aligned with Managed Security Service Providers across the United States. In the event that you do not have the internal resources to manage DataGuard, we are more than happy to work with your Managed Security Service Partner of choice, or can introduce you to one of our partners, to continue the DSPM as a Service engagement.

Symmetry Systems DSPM as a Service

As a premium offering, Symmetry Systems can continue the engagement. New success criteria would be set on a quarterly basis.

Engagement Outcomes

Improved security posture of your sensitive data and cloud data stores	→	**Understanding of who has access to which sensitive data in your customers on-prem and multi-cloud data stores**
Identification and locking down of excessive data access permissions and privileges	→	**Discovery of databases, data objects, data operations, and identities**
Hardening of controls around your most valuable asset, your data, with continuous compliance checks	→	**Understanding of the data blast radius of compromised identities and other insider threats**
Discovery of sensitive data, even where you didn't know you had it	→	**Detection and control out of your country data operations & maintain compliance with privacy regulations**
Minimization of the cost and risk of data exposure associated with cloud data stores	→	**Reduction in time to detect and remediate data security issues to minimize data breach cost**
Quick identification of violations of least privilege for data access to simplify zero trust strategies	→	**Executive visibility of cloud data sprawl, identity life-cycle, zero-trust violations and sensitive data access**