COALFIRE

WHITE PAPER

Enabling zero trust for security and privacy with Cyera

Product Applicability Guide

COALFIRE OPINION SERIES – Ver. 1.0

ALISON D. TUTTLE, CSSLP, CISSP, CIPP/US

CYERA

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Executive summary

In today's digital landscape, organizations face increasing challenges in securing vast and dynamic data environments while enabling innovation, cloud transformation, and safe AI adoption. The explosion of data across cloud, SaaS, and on-premises systems has dramatically increased the attack surface, making system design and architecture a mission-critical function which must implement, enable, and support legal and regulatory requirements, as well as, among others, mission and business, security, privacy, and capability requirements.

Security is inherently critical to the design of a system and, ultimately, determines business resilience, response readiness, and operational agility; while privacy is critical to protect business-to-consumer relationships and brand reputation. This white paper is provided as a Product Applicability Guide to present critical perspectives on the security and privacy requirements for system design and how these translate to compliance objectives. Further, this guide reviews how the Cyera Data Security Posture Management platform can support organizational efforts to optimize data and enable visibility into sensitive data, contextualize risk, and automating protection, ultimately promoting a stronger data security and privacy posture while enabling secure AI adoption.

This guide examines both the potential value of organizational data and the critical issues that prevent the realization of that value, including common problems like data sprawl, data hoarding, uncertain data provenance, and poor data visibility. Security and privacy are presented as organizational objectives, and the zero trust methodology is reviewed as a methodical approach to security and privacy that strengthens an organization's defenses and where the adoption of the Cyera Data Security Posture Management platform can promote and enhance data security and privacy.

Coalfire presents a summary of the Cyera Data Security Posture Management platform and its capabilities, including data discovery, classification, and automated risk management, and reviews the technical details surrounding its deployment and implementation into customer environments. These capabilities and features are compared against the following industry best practices for security and privacy and zero trust: *Secure Design Principles*, *Generally Accepted Privacy Principles*, and the *Tenants of Zero Trust*.

Additionally, Coalfire has compared the Cyera Data Security Posture Management platform's capabilities to ISO/IEC 27001, an international standard for designing and implementing an information security management system (ISMS), as well as a sample selection of system security and privacy requirements published by the NIST which are incorporated in its RMF process and make up the baselines for common public sector compliance programs like FedRAMP, FISMA, DoD RMF, and CMMC.

Through this parallel discussion of these foundational system security and privacy concepts, the zero trust methodology, and the technical review of the Cyera Data Security Posture Management platform's capabilities, Coalfire presents a comprehensive analysis of the Cyera Data Security Posture Management platform's specific application to these frameworks, as well as common best practices and compliance requirements. This guide outlines how the Cyera Data Security Posture Management platform can not only support an organization's compliance requirements but can also enhance an organization's efforts toward data optimization, through the ability to directly support the adoption of generative AI and helping accelerate business enablement by helping eliminate data blind spots that can stall innovation.

Coalfire opinion

The Cyera Data Security Posture Management platform introduces a holistic solution to data management that can help resolve many of the industry's most complex problems related to data management, including data security and privacy compliance. The data-centric approach enabled by the capabilities and performance of the Cyera Data Security Posture Management platform can enable organizations to support and implement industry best practices, concepts, and the tenets of security, privacy, and zero trust to help harden their systems and enhance overall compliance posture. Coalfire has determined that the Cyera Data Security Posture Management platform can be effective in the effort to secure data and achieve security and privacy compliance objectives, as well as provide enhancement for implementing zero trust for security and privacy.

Introduction

Cyera US, Inc. (“Cyera”) has engaged Coalfire Systems, Inc., or its subsidiaries (“Coalfire”), a respected thought leader in the cybersecurity compliance industry, to conduct an independent technical review of its Data Security Posture Management solution (“Cyera DSPM” or “Cyera platform”) in the form of a Product Applicability Guide (PAG).

This guide reviews the Cyera platform against data, security, privacy, and zero trust standards and discusses the most significant problems often associated with implementing these standards within information systems. In addition, Coalfire examines a use case for organizations seeking to improve data security and privacy and to begin implementing both with a zero-trust approach.

This paper outlines Coalfire’s methodology for reviewing the Cyera DSPM, its applicability to data, security, privacy, and zero trust standards, the approach used for the review, and the results of the review. This paper also includes further comments on business considerations for implementing the Cyera platform.

Purpose and scope

This guide aims to educate organizations on the critical issues related to data optimization, security, and privacy, as well as the zero trust methodology as an approach for meeting these objectives. This guide emphasizes the importance of holistic data compliance in the evolving digital landscape and will provide a review of the business drivers for data optimization and the most critical issues related to organizational data management and compliance. Further, this guide will introduce the Cyera platform, its capabilities, and how the product application can support these foundational concepts to enable data optimization.

The scope of this guide is limited to the domains identified here and to the opinion of Coalfire regarding the application of the Cyera platform as a solution for enabling maturity in data optimization and compliance.

Target audience

This guide is written for Cyera customers and may be appropriate for professionals and decision-makers involved in data security, privacy, and compliance, including C-suite executives and officers; network and security teams; compliance, privacy and legal teams; and risk management professionals.

References note

This guide uses endnote citations. Reference citations within the text correlate to the listed references in the rear of the publication.

System security and privacy: data-centric objectives

The sheer volume of data in current IT ecosystems, and the velocity at which it's being created, have outpaced the ability of most organizations to secure it. According to researcher and author Pedro Palandrani, "The world produces 2.5 quintillion bytes of data daily, but that figure should grow at an accelerating rate as more people and devices are connected to the internet."[15]

On the one hand, organizations are embracing data as a barely tapped reservoir of potential revenue streams, consumer insights, and business intelligence. Emerging adoption of AI, data science and analytics, machine learning, and data modeling all help organizations optimize and monetize their data.

On the other hand, data requires devices to store it and systems to process it, which means funding, people, and space are required for its upkeep. Data also introduces increased risk. Data-rich environments make more attractive targets for attackers and can make ransomware events more destructive. In many ways, data introduces as much potential cost to an organization as it does potential value.

Optimizing value requires organizations to minimize the costs and risks associated with their data while maximizing its value. To that end, organizations have begun to recognize the importance of implementing modern data security and privacy, but few are achieving the bare minimum of holistic data management necessary to support this effort.

Why is data optimization so hard to solve? Due to the sheer amount of data they must manage, organizations are struggling to confront and resolve complex data issues, including:

- **Data sprawl:** The rapid creation and broad sharing of data within and between organizations means data is finding its way into applications or environments where it does not belong.
- **Data hoarding:** There is no benefit to the business in retaining data that cannot or will not be used for the business, and every benefit to potential attackers since this retention increases the attack surface and potential payout in the event of a breach. But the mere idea that data may turn out to be useful, or that it cannot be safely deleted, encourages this unnecessary saving.
- **Data provenance:** Data provenance is difficult to trace, making it difficult to and accurately identify applicable compliance requirements and legal restrictions across the compliance landscape.
- **Data visibility:** Lack of data visibility, traditionally poor classification methods, and the improper documentation and mapping of data means that there is no accurate data inventory to support business efforts or compliance activities. AI has only exacerbated this challenge.

These critical issues can seem an insurmountable challenge for many organizations; however, a data-centric approach can help businesses optimize their data while fulfilling the traditional cybersecurity imperatives of data security and data privacy. Data is an asset; as such, it must be managed and protected. Organizations must face the reality that while data my provide for new and innovative business strategies and products, it comes with a multitude of obligations – to the data subject, the data owners, the customers, the business and mission, the shareholders, and more.

Examining data and data management

What is data? How do we define data to ensure understanding of the full scope and nature of what must be protected to the extent that, from this understanding, appropriate and effective protections can be designed and implemented?

National Institute of Standards and Technology (NIST) defines data as “pieces of information from which ‘understandable information’ is derived,”[11] and in another publication as a “[r]epresentation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.”[12]

If data is merely a collection of bits, then it seemingly has no meaning or value. Daniel Keys Moran, fiction writer and computer programmer, said, “You can have data without information, but you cannot have information without data.”[1] For the purposes of this guide, data is information and, therefore, must be understood so that it may be identified, inventoried, and adequately protected to ensure minimum risk to the business while also promoting maximum business value from its use.

The objectives and goals of data management involve technical, administrative, operational, security, and organizational domains. Just as data has become an ever-growing, pervasive thing, the business requirements, legal rules and regulations, and industry best practices that dictate the how of its management continue to evolve and introduce burdens for organizations.

Compliance as an objective is often a complete derailment for an organization. Compliance is concerned with the governance of data and the adherence to applicable laws, regulations, and industry requirements. Security and privacy both play a large role in data-related compliance but are frequently in opposition or conflict due to their divergent objectives. Security aims to protect the confidentiality, integrity, and availability of data, while privacy aims to protect the data subject and their rights to the data. While closely related, these are not the same – privacy cannot exist without security but security may exist without privacy. Compliance activities are made more difficult by the complexity of jurisdiction and application of various security and privacy laws, rules, and frameworks.

Security and its application to data

Security as a concept applied to data is fairly straightforward and has been the focus of the information technology industry for long enough that most are familiar with its basic principles, the CIA triad. Security is concerned with making sure information is protected from unauthorized disclosure (confidentiality), unauthorized alteration (integrity), and unauthorized disruption of access to the information by authorized individuals (availability). Central to these concepts is the establishment of a secure system to hold and process an organization’s data.

Security is also concerned with authentication, authorization, and nonrepudiation. These concepts are data-focused but have historically been implemented at the system level. Authentication ensures the individual is who they say they are (e.g., through passwords and tokens). Authorization ensures the individual is allowed to perform the activity they are attempting on the object they are targeting (e.g., through file permissions). And finally, nonrepudiation ensures no individual can perform an activity and later deny that action (e.g., through logging).

This is a basic summation of these concepts, and there are additional nuances and intricacies in the implementation and enforcement of these within information systems, but for the purposes of this guide it is sufficient to know these concepts are foundational to the security of data and systems. Noticeably, what is *not* required for security is privacy.

Privacy and its application to data

To understand the privacy requirements as related to data security and, more specifically, the less familiar ones related directly to data privacy, we must first understand what privacy means for data.

Privacy is best and most famously explained as the “right to be let alone.” Justice Louis Brandeis is considered to be the “father of privacy” and is credited with the original idea of personal privacy as a basic and fundamental human right. His essay *The Right to Privacy* was published in the *Harvard Law Review* in 1890 and, along with some of his work as an Associate Justice of the Supreme Court, serves as the foundation for all of the United States’ privacy laws[8], as well as some laws from other countries. Brandeis defended the position that privacy is actually a constitutional right by directly aligning the right to privacy and the ‘right to be let alone’ with the Fourth Amendment, which protects people from unreasonable searches and seizures by the government.

Brandeis laid the foundation for our modern interpretation and application of individual privacy by introducing and defending the position that it is an individual’s right to determine the manner in which information about them is shared and used:

> “The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music. Neither does the existence of the right depend upon the nature or value of the thought or emotion, nor upon the excellence of the means of expression.”[17]

This argument is as applicable today as it was in 1890, and businesses that collect, ingest, process, and produce data that directly or indirectly identifies individual persons have a responsibility, both legal and moral, to protect that data and abide by the purpose for and use of data that the data subject agreed to at the time of creation.

Businesses collect personal data to perform and provide services, and, therefore, there is a business purpose aligned with the data collected. However, many organizations view data in their keeping as an asset to use as they see fit even if that use is outside the scope and limits of the original collection purpose. Even if organizations are cognizant and diligent about limiting date use to the purpose for which it was collected, and the data may be reserved for a specific purpose or service fulfillment, data can often sprawl across organizations and business partners and end up in systems and places for which it was never intended.

There are a great number of data privacy laws and frameworks in place that apply across various industries and locations, and the compliance requirements they introduce can be difficult to navigate because the rules can vary depending on multiple criteria, including:

- **Jurisdiction:** This is the area over which the law applies – sometimes geographical area depending on the authority of the court or enforcing entity and sometimes subject matter area depending on the authority of the court. An infamous example from the headlines is the dramatic back-and-forth between the European Union and various U.S.-based companies, where the E.U. attempted to fine them for violations of the General Data Protection Regulation (GDPR) and those companies argued against that jurisdictional authority and refused to pay the fines.
- **Scope and applicability:** Even within the jurisdiction of the court or enforcing entity of a particular law, there are often limitations in the authority of that law due to its established scope and application. For instance, HIPAA does not apply to all medical records or health data collection – it is specifically scoped to apply to covered entities and their business associates involved with health insurance, health clearinghouses, and healthcare providers.
- **Notice and consent:** Many laws and compliance frameworks related to privacy require organizations to provide notice to data subjects of the privacy policies and practices of the organization and to acquire the consent of the data subject to collect their personal data and use it for specific purposes, including the consent of the individual for that information to be shared with third parties and partners. Additionally, an organization is obligated to adhere to any privacy notice it publishes that states its privacy practices, even if those practices are stricter than the requirements of applicable law.

- **Breach notifications:** The term “breach” is defined separately by each applicable law and framework and can vary; however, depending on its definition in and the jurisdiction and applicability of the authoritative reference, organizations must include breach notifications as part of their incident response plan. In addition, they must ensure to meet the varying requirements across applicable laws and frameworks for the timing of the breach notification, the extent of information required within the notification, and any required legal and law enforcement notifications on top of the individual breach notifications. Disparate breach notification requirements across multiple federal and state laws mean organizations must navigate maintaining compliance with the law while also not over-extending and causing unnecessary damage to the business’ reputation.
- **Subject rights:** Many – but not all – privacy laws have data subject rights. Organizations must be cognizant of when and where there is a legal obligation to provide the data subject with information or response to requests, like the “right to be forgotten” included in the GDPR or the “right to delete” included in the California Privacy Rights Act (CPRA).

When organizations do not know where their data came from, the purpose for which it was collected, where it been store or used, or how it has been altered during its lifetime, these compliance requirements are impossible to meet.

In 2021, an internal memo from a prominent social media company was leaked to the press due to its scandalous assertion that data sprawl across the organization – due to a “lack of closed systems” – meant that there was no possible way to determine data lineage and ensure compliance with emerging legal requirements. This situation was likened to spilling a bottle of ink in the ocean and later trying to get it back into the bottle.[6]

Sadly, while this situation is just the most prominent example of this kind of gross negligence with data throughout its life cycle, it is all too common for organizations to be completely unable to identify data provenance or lineage – where the data originally came from as well as the path it has traveled across the organization and its systems – thus making privacy an objective they cannot truly achieve.

Implementing zero trust for security and privacy

As previously stated, security can exist without privacy, but privacy cannot exist without security. Thus, there is a disconnect between these two primary objectives of organizational data management which can, and does, introduce complexity for the data owners and stewards tasked with ensuring compliance. However, the two concepts can be congruous, and frameworks and methodologies have been developed to support the seamless integration of controls to enforce both security and privacy for data and systems. Principal among these is the zero trust model.

Zero trust is a common buzz word but is often misunderstood in its intent and implementation. Zero trust is not a specific model, framework, or design so much as it is a methodical and strategic approach to implementing specific information system objectives, like security and privacy.

Originally developed to address information system security, zero trust as a methodology was introduced by John Kindervag with the intention to alter the mindset of every network and system architect. In *No More Chewy Centers: The Zero Trust Model of Information Security* [7], Kindervag introduced a new perspective to the phrase “trust but verify.” Zero trust does not, as is occasionally thought, mean “trust nothing and no one,” rather it encourages movement away from *inherent trust*. As summarized in the “Key Takeaways” of Kindervag’s original paper zero trust means:

- Move away from perimeter-based defense.
- Don’t allow inherent trust.
- Keep investing in the journey.

While originally designed for security, zero trust has since been adopted in support of privacy. According to *Fehrer in Zero Trust Privacy: A new strategy for protecting your company's data*, "The Zero Trust [M]odel, which originated in the field of cybersecurity, has begun to be seen as a promising solution to modern privacy challenges. The zero trust approach represents a paradigmatic shift in how organizations perceive and approach security and privacy."[3]

This PAG aims to further define and defend zero trust as the data-centric solution implementation for data security and privacy, as well as to discuss and provide an opinion on how Cyera's DSPM solution can help organizations achieve security and privacy goals.

Cyera enables data-centricity

The most foundational requirement for the successful implementation of zero-trust security and privacy is an organization to identify and understand its data. The Cyera platform is designed to help organizations meet this objective, regardless of organizational maturity in this space, from just beginning to achieving and maintaining compliance for data security and privacy.

Philosophy and mission

Beginning from the philosophy that data a valuable organizational asset that is also high risk and introduces complex issues related to compliance, Cyera aims to support organizations in managing and protecting of their data. Cyera DSPM is a cloud-native platform for data identification, classification, protection, and overall management that is designed to help enable data security in a non-invasive manner so that organizations can maximize the value of their data to support development, growth, and innovation through secure AI adoption, set out to develop a solution to.

Services

Cyera DSPM is designed to manage data across a diverse landscape of modern systems, including cloud, on-premises, and hybrid infrastructures, as well as all manner of storage solutions. The Cyera platform's data discovery and management capabilities work to provide organizations with a complete picture of their data inventory across disparate data stores and in a dynamic capacity. The Cyera platform minimizes human involvement, enables customization in data type and classification schemes, and implements ML to learn and adapt to an organization's specific data discovery and classification needs. Cyera DSPM includes the services below:

- **Data Analysis Service (DAS):** The DAS is a security-hardened Kubernetes cluster performing data discovery and classification, connecting to the environment using cloud-native APIs.
- **Data Insights Service (DIS):** The DIS is hosted in Amazon Web Services (AWS) and is managed and operated by Cyera's cloud engineering team.

Deployment models

Cyera DSPM can be deployed in a SaaS model or as an "Outpost" model.

- **SaaS:** Cyera DSPM is deployed in AWS with Kubernetes clusters in the Cyera Cloud Environment. Connection between Cyera DSPM and the Customer Cloud Environment is via a "cross-account assume role" trust policy, granting the Cyera platform temporary, read-only access to data stores, environment logs, and monitoring infrastructure. In this deployment model, both the DAS and DIS are hosted in the Cyera Cloud Environment.
- **Outpost.** Cyera DSPM is deployed in AWS with Kubernetes clusters in customer's leader account in the Customer Cloud Environment. Connection between Cyera DSPM and the Customer Cloud Environment is via an encrypted private link. In this deployment model, the DAS is hosted on a Cyera Kubernetes Cluster in the Customer Cloud Environment and the DIS is hosted in the Cyera Cloud Environment. This enables the service while limiting the information that is transferred outside of the Customer Cloud Environment.

While this guide describes the deployment models via AWS, Cyera can also be deployed via Microsoft Azure and Google Cloud Platform (GCP).

Security considerations

Cyera DSPM was developed with security and compliance inherent to its operational design:

- **Data location:** All customer data analysis is performed in the same region where the data was originally discovered.
- **Data minimization:** All customer data analysis is performed inside the DAS and then immediately deleted.
- **Privilege limitation:** Because Cyera DSPM uses read-only access credentials, the Cyera platform cannot make any changes to customer workloads or data stores and won't make any changes to or impact customer runtime environments.
- **Secure connection:** Cyera DSPM connects to customer systems via safe, encrypted links and secure API endpoints.

Data discovery and classification

Cyera DSPM works by performing dynamic data discovery via the DAS and returning results from across an organization's entire system, including disparate storage locations and all data structures, with minimal impact to system performance. This data store inventory is generated across structured and unstructured data in buckets, blob storage, unmanaged, semi-managed, or DBaaS stores, data lakes, and other data platforms.

Cyera DSMP then "reads" the data, metadata, or schema, and categorizes the data as Personal, Financial, Health-related, Business & IP, or IT & Security. Cyera DSPM also has hundreds of data classifications built-in and will also automatically discover Customer- and environment-specific data types. The Cyera platform is able to learn the customer data and data classification and can identify types of encrypted, masked, and tokenized data.

Cyera DSPM provides contextualized data classification that gives users insight into the data, incorporating data classes such as data subject role, data subject residency, data-level encryption, identifiable data, and synthetic data. The Cyera platform can also enable organizations to minimize human interaction as there is no manual tagging or correlation or de-duplication required.

Automated risk management

Cyera DSPM can also enable automated security and compliance policy enforcement. The DIS assesses exposure and risk by reviewing sensitive data identified by the DAS, incorporating its knowledge of the environment and compliance frameworks, and identifying security posture gaps against specific security and regulatory frameworks. DIS also provides intelligence that helps to prioritize risk based on data impact, which is critical for both traditional incident response and secure AI deployment. The Cyera platform also presents customers with remediation guidance and an option to implement automated remediations.

Cyera DSPM allows customers to implement custom policies to further meet their specific industry and compliance needs. Built-in policies are focused on concepts of external exposure, access, logging, encryption, privacy, data sprawl, and backup.

Impact-driven alerting and incident prioritization

Security teams can incorporate data intelligence provided by Cyera DSPM with existing DLP, SIEM, or SOAR capabilities to add impact-based prioritization to security events. This allows alerts tied to systems storing sensitive or regulated data to be automatically elevated, leading to faster and more informed responses. By layering data context into traditional event metadata, the Cyera platform can help enable smarter triage, reduce alert fatigue, and focus analyst attention on the risks that matter most to the business.

Secure AI adoption and business enablement

AI is only as secure as the data it consumes. Cyera DSPM provides visibility into sensitive data assets across an organization, including those feeding LLMs, ML pipelines, or custom AI tools, to help with safe, responsible AI adoption. With contextual classification, data tagging, and policy enforcement, Cyera DSPM helps organization implement AI without exposing regulated, proprietary, or high-risk data to misuse.

Cyera DSPM can also help improve business enablement. Through use of accurate, real-time data intelligence, security controls can be surgically applied, helping enable quick access for trusted users while minimizing operational friction. This shifts the posture of security teams from blockers to enablers, helping developers, analysts, and data teams to move fast while staying secure.

Cyera DSPM for zero trust for security and privacy

Cyera DSPM helps enable data-centricity, which is integral to implementing the zero-trust methodology to achieve the objectives of data security and data privacy. Organizations cannot protect what they do not know they have, and, since not all data is created equal, unknown or unclassified data cannot be protected appropriately. Cyera DSPM is designed to solve both of these problems for organizations facing big data issues like data sprawl, data hoarding, data provenance, and data visibility.

Product application scope and approach for review

Cyera engaged Coalfire to conduct an independent review of the Cyera platform in application to security and privacy, including the context of zero trust. Due to the large target of applicability and the abstract nature of zero trust, Coalfire began by identifying industry best practices for security and privacy and analyzing Cyera DSPM's capabilities to support them: *Generally Accepted Privacy Principles (GAPP)*[2] and Saltzer and Schroeder's *Secure Design Principles*.[16] Coalfire also reviewed Cyera against the *Tenets of Zero Trust*[14] and then identified two specific and common compliance frameworks:

- **ISO/IEC 27001:** ISO/IEC 27001 is an internationally respected standard for information security management systems (ISMS). This framework is widely adopted and commonly accepted by the majority of organizations, stakeholders, and customers as an indicator of the security health and posture of a system. Coalfire analyzed the Cyera platform against several groupings of controls within ISO/IEC 27001.
- **NIST Risk Management Framework (RMF):** The NIST RMF serves as a foundational risk management life cycle framework and is leveraged by several U.S.-specific public sector compliance programs, including FedRAMP, FISMA, DoD RMF, and CMMC. Coalfire analyzed the Cyera platform against several groupings of controls taken from the NIST Special Publication (SP) 800-53[10] and NIST SP 800-171[13].

Generally Accepted Privacy Principles

Cyera DSPM: GAPP		
Principle	**Description**	**Applicability to Cyera DSPM**
Management	*The entity defines, documents, communicates, and assigns accountability for all of its privacy policies and procedures.*	This principle addresses ensuring policies and procedures are appropriate for the target of their application. Cyera DSPM's discovery and ability to learn and categorize data automatically can enable organizations to identify and understand their data and the compliance requirements of that data, which is essential to ensuring policies and procedures are appropriate and support compliance.
Notice	*The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.*	This principle addresses notice, which is generally implemented at the point of collection but may be necessary later in the data life cycle when an organization wishes to utilize the data for purposes outside the scope of the original collection notice or for when policies change. In order to manage these scenarios appropriately, organizations must know what data was collected when, and for what reason. Cyera DSPM enables this granular level of data understanding and lineage tracing.

Cyera DSPM: GAPP		
Choice and Consent	*The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, or disclosure of personal information.*	This principle also addresses a change to the planned utilization of personal data, where the organization must understand and respect the original point and purpose of collection to ensure compliance and appropriate updates to consent where necessary. The full suite of data management capabilities offered by the Cyera DSPM enables organizations to maintain awareness of the provenance of personal data and therefore tie it back to its original collection purpose.
Collection	*The entity collects personal information only for the purposes identified in the notice.*	This principle addresses transparency in the original collection of data, which Cyera DSPM does not directly address. However, in the instance an organization collects this information from a third party, Cyera DSPM can enable the organization to identify the type of data and review whether it is fair and lawful.
Use, Retention, and Disposal	*The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.*	This principle addresses a large part of the data life cycle, including data use limitation, data minimization, and data retention. Cyera DSPM can help organization meet this requirement through its abilities to discover, classify, categorize, and track data across the life cycle, which inherently supports the objectives of this principle.
Access	*The entity provides individuals with access to their personal information for review and update.*	This principle requires that organizations identify data related to a specific data subject, which assumes data is properly managed and inventoried. Cyera DSPM can support this effort; organizations leveraging the data discovery and classification capabilities to organizations to quickly and efficiently respond to these types of requests.
Disclosure to Third Parties	*The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.*	This principle addresses data sharing and relies heavily on the terms of notice and consent acquired at collection. Cyera DSPM can enable organizations to trace data lineage and review these terms prior to data sharing to help ensure the activity is in accordance with the same.
Security for Privacy	*The entity protects personal information against unauthorized access (both physical and logical).*	This principle addresses data protection. Cyera DSPM can directly enable organizations to implement this principle through its dynamic capability to apply security and compliance policies, including automated remediation.
Quality	*The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.*	This principle addresses data quality in terms of accuracy and completeness. Cyera DSPM can support this principle by enabling organizations to discover and classify data, which directly supports organizational efforts to maintain data quality. While Cyera DSPM cannot specifically ensure accurate or complete data, it can help organizations identify these gaps.
Monitoring and Enforcement	*The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy*	This principle addresses monitoring and enforcement, which can be directly fulfilled by utilization of the security

Cyera DSPM: GAPP		
	related inquiries, complaints, and disputes.	and compliance policy enforcement capabilities included in the Cyera DSPM platform.

Secure Design Principles

Cyera DSPM: Secure Design Principles		
Principle	**Description**	**Applicability to Cyera DSPM**
Economy of mechanism	*Keep the design as simple and small as possible. This well-known principle applies to any aspect of a system, but it deserves emphasis for protection mechanisms for this reason: design and implementation errors that result in unwanted access paths will not be noticed during normal use (since normal use usually does not include attempts to exercise improper access paths). As a result, techniques such as line-by-line inspection of software and physical examination of hardware that implements protection mechanisms are necessary. For such techniques to be successful, a small and simple design is essential.*	This principle is not directly supported by Cyera DSPM, but it is worth noting that the use of the Cyera platform can help identify where this principle is not being implemented sufficiently. Mapping the organization's data with Cyera DSPM can enable the organization to develop a truthful representation of the economy or complexity of their system designs.
Fail-safe defaults	*Base access decisions on permission rather than exclusion. This principle, suggested by E. Glaser in 1965, means that the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted. The alternative, in which mechanisms attempt to identify conditions under which access should be refused, presents the wrong psychological base for secure system design. A conservative design must be based on arguments why objects should be accessible, rather than why they should not. In a large system some objects will be inadequately considered, so a default of lack of permission is safer. A design or implementation mistake in a mechanism that gives explicit permission tends to fail by refusing permission, a safe situation, since it will be quickly detected. On the other hand, a design or implementation mistake in a mechanism that explicitly excludes access tends to fail by allowing access, a failure which may go unnoticed in normal use. This principle applies both*	This principle essentially takes the long way to assert deny-by-default, allow-by-exception, a common secure tenet and best practice. While Cyera DSPM cannot directly influence this implementation, the use of the Cyera platform can help organizations identify appropriate access policies based on the nature of the data in the objects attempting to be accessed. Additionally, Cyera DSPM's automated security and compliance policy enforcement can help reinforce this implementation.

Cyera DSPM: Secure Design Principles		
	to the outward appearance of the protection mechanism and to its underlying implementation.	
Complete mediation	*Every access to every object must be checked for authority. This principle, when systematically applied, is the primary underpinning of the protection system. It forces a system-wide view of access control, which in addition to normal operation includes initialization, recovery, shutdown, and maintenance. It implies that a foolproof method of identifying the source of every request must be devised. It also requires that proposals to gain performance by remembering the result of an authority check be examined skeptically. If a change in authority occurs, such remembered results must be systematically updated.*	This principle addresses the practice of inherent trust and continual access verification. Cyera DSPM can support this implementation by assisting the organization in determining appropriate access schemes based on the sensitivity of the data in the object attempting to be accessed, and through its automated security and compliance policy enforcement capabilities.
Open design	*The design should not be secret. The mechanisms should not depend on the ignorance of potential attackers, but rather on the possession of specific, more easily protected, keys or passwords. This decoupling of protection mechanisms from protection keys permits the mechanisms to be examined by many reviewers without concern that the review may itself compromise the safeguards. In addition, any skeptical user may be allowed to convince himself that the system he is about to use is adequate for his purpose. Finally, it is simply not realistic to attempt to maintain secrecy for any system which receives wide distribution.*	This principle states that security shouldn't rely on an inability to figure out how the system works but on the strength of the encryption and associated keys. Cyera DSPM can assist in the implementation and maturity of this implementation by helping organizations to identify where this sensitive data is located and adjust the system design according to that location and sensitive contents, supporting efforts to continue to protect these secrets.
Separation of privilege	*Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key. The relevance of this observation to computer systems was pointed out by R. Needham in 1973. The reason is that, once the mechanism is locked, the two keys can be physically separated and distinct programs, organizations, or individuals made responsible for them. From then on, no single accident, deception, or breach of trust is sufficient to compromise the protected information. This principle is*	This principle addresses the concept of a weak link along with dual integrity. The separation of privilege described ensures that no accident or force can, by itself, result in a breach of policy. Cyera DSPM cannot directly provide this implementation but can support the organization in identifying where this implementation is most critical and appropriate when leveraged to inform the organization of the location of this data, as well as supporting the policy enforcement and protection of the keys.

Cyera DSPM: Secure Design Principles

	often used in bank safe-deposit boxes. It is also at work in the defense system that fires a nuclear weapon only if two different people both give the correct command. In a computer system, separated keys apply to any situation in which two or more conditions must be met before access should be permitted. For example, systems providing user-extendible protected data types usually depend on separation of privilege for their implementation.	
Least privilege	*Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur. Thus, if a question arises related to misuse of a privilege, the number of programs that must be audited is minimized. Put another way, if a mechanism can provide "firewalls," the principle of least privilege provides a rationale for where to install the firewalls. The military security rule of "need-to-know" is an example of this principle.*	This principle addresses limiting privileges to the bare minimum required for personnel to perform their duties, thus reducing the risk and potential impact of the misuse of these privileges. Cyera DSPM can support organizations in its implementation through the automated security and policy enforcement capability where the system, environment, data type, user and role access, and more are considered, and the Cyera platform can provide insights and alerts on the security posture and compliance state of the system.
Least common mechanism	*Minimize the amount of mechanism common to more than one user and depended on by all users. Every shared mechanism (especially one involving shared variables) represents a potential information path between users and must be designed with great care to be sure it does not unintentionally compromise security. Further, any mechanism serving all users must be certified to the satisfaction of every user, a job presumably harder than satisfying only one or a few users. For example, given the choice of implementing a new function as a supervisor procedure shared by all users or as a library procedure that can be handled as though it were the user's own, choose the latter course. Then, if one or a few users are not satisfied with the level of certification of the function, they can*	This principle addresses the inadvertent sharing of information. Cyera DSPM can support the implementation of this principle since it provides organizations with the capability to discover data and identify where accidental or inappropriate information transfer has occurred.

Cyera DSPM: Secure Design Principles

	provide a substitute or not use it at all. Either way, they can avoid being harmed by a mistake in it.	
Psychological acceptability	*It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.*	This principle addresses the need for security to not be seen, heard, or impact the user, as the user will circumvent the security mechanism if it is obstructing their activities. Cyera DSPM can support this principle through its capability for automated security and compliance policy enforcement.

Tenets of Zero Trust

Cyera DSPM: Tenets of Zero Trust

Tenet	Description	Applicability to Cyera DSPM
All data sources and computing services are considered resources.	*A network may be composed of multiple classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service (SaaS), systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.*	Cyera DSPM can support this tenet through its incorporation of the entire cloud estate as well as on-premises system components in its data discovery and classification processes.
All communication is secured regardless of network location.	*Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise-owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.*	Cyera DSPM can support this tenet through its automated security and compliance policy enforcement capabilities.
Access to individual enterprise resources is granted on a per-session basis.	*Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.*	Cyera DSPM can support this tenet through its automated security and compliance policy enforcement capabilities.

Cyera DSPM: Tenets of Zero Trust		
	This could mean only "sometime recently" for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.	
Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.	*An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need. For zero trust, client identity can include the user account (or service identity) and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks. Requesting asset state can include device characteristics such as software version installed, network location, time/date of request, previously observed behavior, and installed credentials. Behavioral attributes include, but not limited to, automated subject analytics, device analytics, and measured deviations from observed usage patterns. Policy is the set of access rules based on attributes that an organization assigns to a subject, data asset, or application. Environmental attributes may include such factors as requestor network location, time, reported active attacks, etc. These rules and attributes are based on the needs of the business process and acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. Least privilege principles are applied to restrict both visibility and accessibility.*	Cyera DSPM can support this tenet through its abilities to enable organizations both to gather an accurate inventory of their resources (data) and help to define, categorize, classify, and protect that data according to organizational policy and security/risk posture.
The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	*No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing ZTA should establish a continuous diagnostics and mitigation (CDM) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed. Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently*	Cyera DSPM can support this tenet by providing the organization with identified risks and security posture gaps based on a dynamic review of the environment, the data, and associated activities, all against the organization's identified risk tolerance and compliance requirements. This is further supported by Cyera DSPM's automatic policy enforcement capability.

Cyera DSPM: Tenets of Zero Trust		
	(including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associate devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise resources.	
All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	*This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.*	Cyera DSPM can support this tenet through its ability to provide the organization with context around the sensitivity of objects and the ability to adapt dynamically to requests to those objects. While Cyera DSPM cannot implement the ICAM aspect, the information and insights provided by the DAS and DIS services, as well as the capability to automatically enforce compliance remediation based on the organization's policies and risk tolerance can support this effort.
The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.	*An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.*	Cyera can support this tenet with its ability to provide the organization with a dynamic inventory of its data assets as well as providing dynamic assessments on the risk level and security posture of the system based on its observations and return remediation recommendations and policy improvement recommendations.

ISO/IEC 27001

Cyera DSPM: ISO/IEC 27001		
Category	**Description**	**Applicability to Cyera DSPM**
Asset Management	*Organizations maintain inventories of data assets and asset owners, correctly classify and label data assets, and*	Cyera DSPM can support this requirement thorough its ability to discover all of an organization's data across

Cyera DSPM: ISO/IEC 27001		
	securely dispose of data on media assets to prevent unauthorized access or breaches.	SaaS, IaaS, PaaS, DBaaS, and on-prem resources, and classifies this data with over 95 percent precision. Cyera DSPM also builds an inventory of all data owners and any other identities with access to an organization's data. The Cyera platform sends notifications and alerts directly to data owners when policy violations are detected, along with instructions for remediation. Cyera DSPM can also discover orphaned, stale, or ghost data stores that should be securely disposed of and can validate disposal efforts.
Access Control	*Organizations define access control policies, register and provision user accounts, manage access rights and authentication information, and regularly review and adjust user access rights.*	Cyera DSPM can support this requirement through its ability to identify excessive permissions and overly broad access to sensitive data, recommending least privilege policies. Cyera DSPM can also identify stale identities such as ghost accounts or users who have left the organization or switched roles within the organization. Cyera DSPM automates access certification for sensitive data, helping to review and update user access rights. The Cyera platform can also detect and automatically mask sensitive data such as login credentials that have been discovered in plain text.
Compliance	*Organizations ensure compliance with applicable data privacy regulations such as GDPR, HIPAA, or CCPA.*	Cyera DSPM can support this requirement by coming pre-trained with classifiers (e.g., PII, PHI) aligned to major data privacy and data security frameworks.
Cryptography	*Organizations use cryptographic techniques to protect the confidentiality, integrity, and availability of information assets.*	Cyera DSPM can support this requirement by detecting unencrypted sensitive data and recommending encryption and tokenization, mapping to cryptographic policies.
Operations Security	*Organizations separate development, testing, and production environments, maintain secure backups, and monitor and log network and data events to support incident response, remediation, and compliance audits.*	Cyera DSPM can support this requirement by continuously monitoring organizations' entire data estates, logging data events, and generating alerts for remediation. Cyera DSPM can also detect and help remediate data drift between environments. Through its partnership with backup provider Cohesity, Cyera DSPM can also help organizations manage backups and verify their completeness, which can be helpful when assessing the impact of, and recovering from, a ransomware attack.
Organizational Controls	*Organizations define information security roles and responsibilities, include information security requirements in third-party supplier relationships, and identify critical third-party suppliers as part of their business continuity planning.*	Cyera DSPM can support this requirement by leveraging its asset discovery and classification capabilities to help identify data owners and their access privileges, helping organizations align access configurations to defined roles and responsibilities. Cyera DSPM also identifies and monitors access to organizational data by external actors or services, which can be used to create an inventory of third-party applications and services in use in the organization's IT ecosystem. By mapping data flows to these applications and services, organizations can leverage Cyera DSPM's insights to identify their most business-critical information assets.

Cyera DSPM: ISO/IEC 27001		
People Controls	*Organizations screen personnel before providing access to sensitive data and engage in regular information security awareness and training campaigns.*	Cyera DSPM can support this requirement by leveraging its asset discovery and classification capabilities to help ensure least-privilege access. Cyera DSPM also helps organizations raise awareness about data security by directly notifying data owners when policy violations occur. By providing data owners with notice and instructions for remediation, the Cyera platform helps to democratize data security responsibility across the organization.

NIST RMF

Cyera DSPM: NIST RMF		
Control/Practice Family	**Description**	**Applicability to Cyera DSPM**
Access Control (AC)	*Organizations must implement controls to control access to critical information resources. This access includes user- and system-access and is data-centric, meaning the objective is not focused on the user or the account but on the data itself and what is allowed to happen to it and where it is allowed to move within the system.*	Cyera DSPM can support this control by not only identifying and categorizing the data used to support the categorization of the system itself and the development of information flow control policies but also identifying and reporting on excessive permissions and inappropriate or malicious accounts and helping to automate access control.
Assessment, Authorization, and Monitoring (CA)	*Organizations must undergo an assessment of their information system in order to receive an authorization for it to operate at the identified impact level appropriate to the data it processes and stores. Organizations must also implement continuous monitoring in order to ensure the security posture identified in the assessment and which that authorization was granted upon has not been altered or compromised.*	Cyera DSPM comes pre-trained with classifiers aligning to major categories of data and includes the capability to introduce new categories, thereby supporting organizations in determining what the appropriate impact level is for the system containing the data. Leveraging Cyera DSPM in this manner can help remove some level of effort from the original determination of system categorization prior to assessment (where appropriate and not already dictated by the data owner) and helps ensure the organization is aware if data outside that impact level or data that does not belong on the system is detected.
Incident Response (IR)	*Organizations must detect and respond to system occurrences which actually or potentially jeopardize the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.*	Cyera DSPM can support incident response procedures innately through the detailed insight it provides about what data, what type of data, the criticality of that data, and associated data requirements are impacted by any given incident. Cyera DSPM continuously monitors organizations' entire data estates, logs data events, and generates alerts for remediation. Cyera DSPM can also detect and help remediate data drift between environments.
Risk Assessment (RA)	*Organizations must undergo a process of identifying risks to organizational operations (including mission, functions, image, reputation),*	Cyera DSPM can support organizations in the assessment and remediation of risk to their systems and data through asset discovery and classification, data owner reporting and access authorization automation

Cyera DSPM: NIST RMF		
	organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.	capabilities, and by generally providing the organization with an exact and precise report on the impact level of the system based on the data it detects and helps categorize. Through the use of Cyera DSPM and the capabilities listed throughout this guide, organizations have an accurate understanding of the risk to the system based on the inherent risk of the data itself and can leverage that consistently to support risk remediation throughout the system.
System and Communications Protection (SC)	*Organizations must protect the system and all communications within by implementing strong network security policies and tools, including system design and architecture to support communications protection and tools or components to support data loss prevention (DLP), antivirus malware protection, boundary protection, cryptographic protections, and more.*	Cyera DSPM can be leveraged to support these requirements by providing a mapping of what data exists within the system, including encrypted data and its level of sensitivity or classification, and providing recommendations for appropriately protecting any data that it detects is not currently sufficiently protected. Additionally, Cyera DSPM and its data learning capabilities can be leveraged for DLP: Cyera DSPM connects to an organizations' current tooling to understand the context behind alerts and to enhance its remediation recommendations. Cyera DSPM "learns" the data within the system and adapting to customize its operations to those defined and desired by the organization.

Further considerations

This section documents additional considerations related to the business impact of implementing the Cyera platform to support data security and privacy.

Trust relationships between the business and consumers

Arguably one of the most interesting aspects of the data privacy discussion is the lack of reactivity from the data subjects. Most people are grossly unaware of the amount of data collected on them and spread across cyberspace for the perusal and unfettered use of whoever happens upon it. Indeed, it is nearly impossible to avoid the spam calls, texts, and emails which are a direct result of data dumps on the dark web, especially with the constant alerts from mobile operating systems prompting yet another password change due to a detected compromise or leak. And still, there is very little change in the behavior of consumers – they hand over their data willingly.

Kevin Mitnick, the famous Blackhat-turned-Whitehat hacker, and prolific author of publications on both data security and privacy, said, “You would think, given the constant news about data breaches and surveillance campaigns by the government, that we’d be much more outraged. You would think that given how fast this happened – in just a handful of years – we’d be reeling from the shock and marching in the streets. Actually, the opposite is true. Many of us, even many readers in this book, now accept to at least some degree the fact that everything we do – all our phone calls, our texts, our e-mails, our social media – can be seen by others. And that’s disappointing.”[9]

This was addressed in a special series published by the Harvard Business Review as well, where the term privacy paradox was used to describe the duality of consumers simultaneously trusting businesses with their personal data and not trusting businesses with their personal data.

Across the board, the conclusion is that this behavior is best explained by a feeling of powerlessness among consumers – what choice is there but to continue to let it happen? The services we want and need require that we hand over our data and the businesses hold the power to either handle it appropriately or continue to disappoint all of us.

This concept leads to one very important business insight, which is that there is a significant advantage to building consumer trust, and ensuring consumer privacy can be a major differentiator. “Companies that are trusted can gather more personal data and use that data to enhance their services, giving them a competitive advantage over less trusted firms. And trusted companies are more readily forgiven when things inevitably go wrong.”[4]

The consumers may not be refusing to interact and share their data, but they are taking great strides to try to protect themselves on the other side – it is not uncommon for individuals to keep multiple email addresses to collect spam, pay for “robo-killer” apps to block spam calls, and subscribe to data scrubbing services. Consumers do care, they just generally lack the power to directly defend themselves from the actual collection and must live with the consequences of the spills.

While this argument can be taken as just further exploitation of consumers for monetary gain, responsible organizations with a service-oriented mission should receive this as a strategic opportunity to turn the hassle of compliance into business growth and maturity, ultimately leading to increased brand respect and revenue.

Implementing Cyera DSPM to support data security and privacy objectives and compliance requirements can help to not only make GRC activities less painful and introduce automation and optimization into the process, but it can also inherently lead to an increase in consumer trust and enhance the B2C relationship.

Cyera DSPM as a third-party data processor

A tenet central to both security and privacy is the minimization of data, including its processing, transmission, and sharing with third parties. While the use of the Cyera platform should not significantly increase the risk associated with data sharing, as it has designed its deployment models to help ensure that the risk is negligible, the use of any third-party tool should be reviewed against an organization's existing privacy notice to ensure this specific type of sharing is covered appropriately, and an organization's legal team should be consulted; however, especially if other SaaS tools are already used within the system, acquisition contracts usually account for and mitigate such risks.

Cyera's architecture is flexible, and its Outpost deployment serves to limit the information transferred outside of the customer's cloud environment and communicates via a secure private link. This deployment model enables customers to adhere to their risk tolerance levels as well as other requirements restricting the movement of data. In either of its deployment models – Outpost or SaaS – the data does not cross regional boundaries.

Diverse uses and benefits

Cyera DSPM is a data inventory and data security platform with a diverse range of capabilities. Because of this, organizations are able implement Cyera DSPM for several purposes including data discovery, data classification, data security, and data privacy. Organizations should also consider the manual activities which Cyera DSPM can automate and the long-term benefits that can arise from the increase in security posture and data security and privacy compliance enabled by its use. Cyera DSPM's capabilities can help accelerate digital transformation initiatives, secure AI adoption, and cloud migrations by resolving uncertainty around sensitive data.

Conclusion

Cyera DSPM is a data security platform designed for the challenges of modern security operations, such as cloud-related risk, secure AI adoption, and rapid incident response. Cyera DSPM is also able to drive privacy compliance, a critical outcome achieved through enhancing security posture by providing data-driven risk context and enabling zero trust implementation across the enterprise. The Cyera platform offers a holistic solution to data management and can help resolve many organizational problems related to data management while providing a data-centric approach with its capabilities and performance. Cyera DSPM can be used by organizations to support and implement industry best practices, concepts, and tenets of security, privacy, and zero trust to harden their systems and enhance overall compliance posture. Coalfire has determined that the Cyera platform can be effective in the effort to secure data, achieve security and privacy compliance objectives, and implement zero trust for security and privacy due to its dynamic, adaptive capabilities.

A comment regarding regulatory compliance

Coalfire disclaims the generic suitability of any technology or service to establish regulatory compliance. Organizations achieve compliance through the implementation and maintenance of a GRC program, not via the use of a specific technology or service. This is true for all entities subject to data security and privacy compliance requirements, as well as all other standards, regulations, or mandates applicable to the entity.

References

1. Adams, J. (2019). Personal Information Security & Systems Architecture: A Systems Architecture Approach to Security and Privacy. Independently published.
2. Clarke, I. (2017). The 10 Generally Accepted Privacy Principles. Linford&Co. LLP. https://linfordco.com/blog/the-10-generally-accepted-privacy-principles/
3. Feher, N. (2023). Zero Trust Privacy: A New Strategy for Protecting Your Company's Data. Independently published.
4. Gartner, J. (2019). Customer Data and Privacy: Insights from Business and Technology Leaders. Harvard Business Review Press.
5. Howard, R. (2023). Cybersecurity First Principles: A Reboot of Strategy & Tactics. Wiley.
6. Ikeda, S. (2022). Leaked Documents From Facebook Indicate Engineers Have Lost Control of User Data, Can't Keep Up With International Privacy Regulations. CPO Magazine. https://www.cpomagazine.com/data-protection/leaked-documents-from-facebook-indicate-engineers-have-lost-control-of-user-data-cant-keep-up-with-international-privacy-regulations/
7. Kindervag, J. (2020). No more chewy centers: The Case for Zero Trust Security. Palo Alto Networks. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf
8. Kramer, I. R. (1990). The Birth of Privacy Law: A Century Since Warren and Brandeis. Catholic University Law Review. Volume 39, Issue 3.
9. Mitnick, K. D. (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company.
10. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (Special Publication 800-53 Revision 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5
11. National Institute of Standards and Technology. (2014). Guidelines for Media Sanitization (Special Publication 800-88 Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-88r1
12. National Institute of Standards and Technology. (2021). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (Special Publication 800-160 Volume 1 Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-160v1r1
13. National Institute of Standards and Technology. (2024). Protecting Unclassified Information in Nonfederal Systems and Organizations (Special Publication 800-171 Revision 3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-171r3
14. National Institute of Standards and Technology. (2020). Zero Trust Architecture (Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207
15. Palandrani, P. (2021, February 9). The Value of Data in a Digital World. Nasdaq. https://www.nasdaq.com/articles/the-value-of-data-in-a-digital-world
16. Saltzer, J., & Schroeder, M. (1975). The Protection of Information in Computer Systems. University of Virginia. https://www.cs.virginia.edu/~evans/cs551/saltzer/
17. Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries ("Coalfire") for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided "as-is" with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the author

Alison D. Tuttle, CSSLP, CISSP, CIPP/US | *Principal, Public Sector Advisory Services*

Alison D. Tuttle is a seasoned professional with experience across the fields of data privacy, information systems and software security, and public sector compliance. Currently serving as a Principal within Coalfire's Public Sector Advisory Services, Alison is passionate about sharing knowledge and driving strategic innovation across her various areas of expertise. As a U.S. Army Veteran and former federal contractor, Alison has a strong foundation in federal compliance and regulation and has experience in applying cybersecurity and privacy best practices to all types of technical products and environments, including AI/ML initiatives, cloud services, and on-prem systems. In addition to her work within the cybersecurity industry, Alison is an active volunteer, former Chapter President and Board Director with the Raleigh Information Systems Security Association (ISSA) where she spends time mentoring young professionals and providing training on data security and privacy. Alison holds a B.S. in English from Drury University and is an (ISC)^2 Certified Software Security Lifecycle Professional (CSSLP), (ISC)^2 Certified Information Systems Security Professional (CISSP), and IAPP Certified Information Privacy Professional – United States (CIPP/US).

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

WP_Enabling zero trust for security and privacy with Cyera_20250808