PROTEGRITY

COMPLIANCE BY DESIGN: A DATA-CENTRIC APPROACH

TABLE OF CONTENTS

01 The Rising Tide of Compliance Challenges

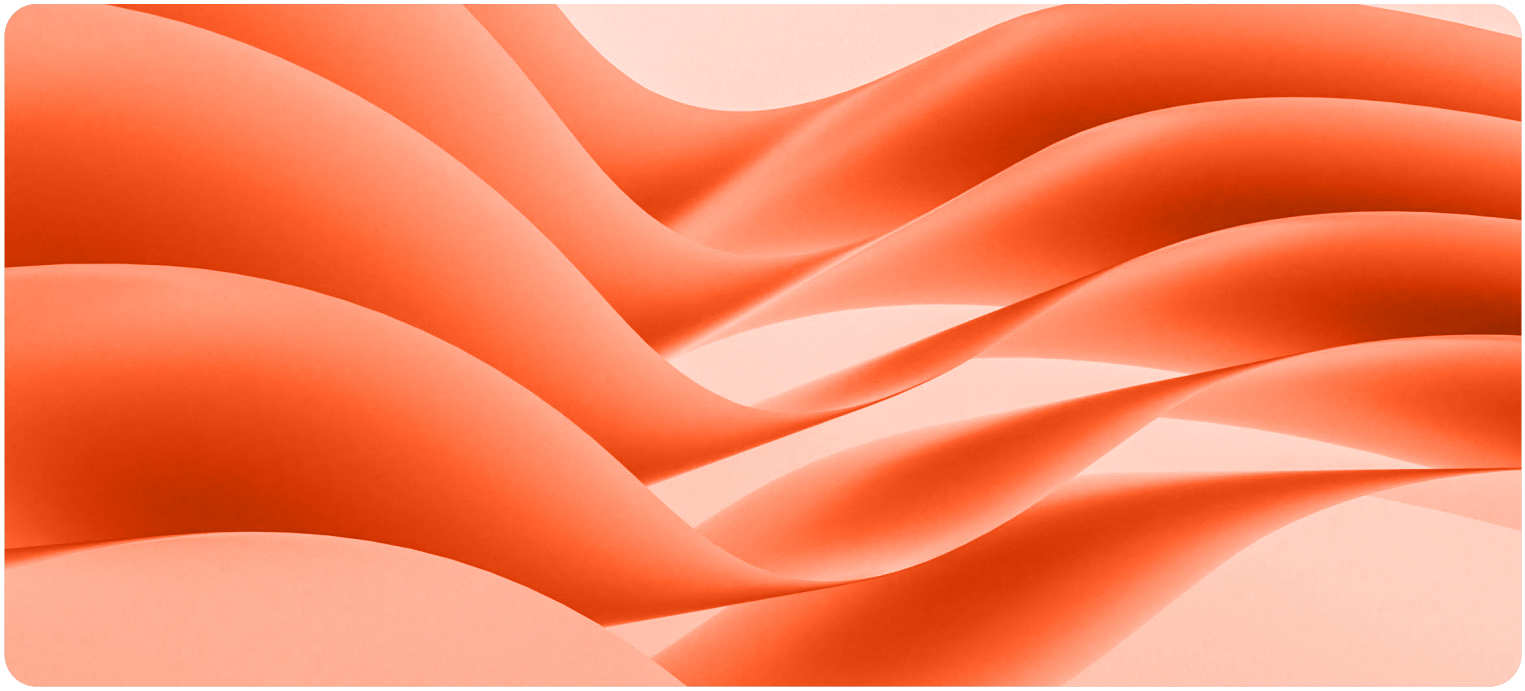
02 The Pitfalls of Traditional Security Methods

03 Navigating the Privacy Landscape

04 The Industry Shift Toward Data-Centric Security

05 Implementing Data-Centric Security Into Your Ecosystem

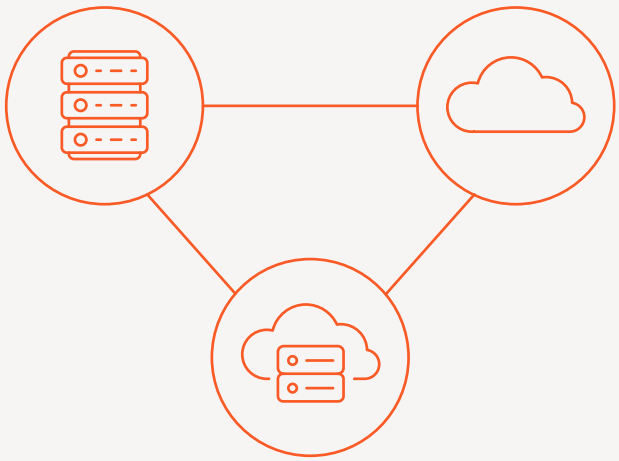
06 Protegrity's Approach to Data-Centric Security



01

The Rising Tide of Compliance Challenges

Compliance with regional privacy like GDPR, DPDP, CPRA, or Law 25 and industry regulations like HIPAA or PCI DSS is not about avoiding fines, it's about safeguarding your organization's data against breaches and cyberattacks. The cybersecurity world has been and continues to change at a rapid speed, thanks to hybrid environments, SaaS applications, and AI innovation—and businesses are scrambling to keep pace. If you're in healthcare, finance, retail, or another highly regulated industry, you've probably felt the pressure firsthand—both customers and regulators are demanding airtight security for personal identifiers, financial records, and sensitive data. By aligning compliance efforts with a solid, data-centric security foundation, you can protect sensitive information and maintain customer trust, ensuring your organization is prepared for the challenges ahead.



THE EXPANDING DATA FOOTPRINT

Imagine you're an IT director at a major financial firm. Your data used to sit safely inside locked-down servers, behind firewalls that felt like castle walls. But today? Your sensitive records flow across multiple environments:

- On-premises infrastructure like IBM Db2, SAP, Microsoft SQL Server, Oracle Database, and traditional mainframes
- Public cloud and SaaS platforms like AWS, Azure, Google Cloud, Salesforce, and ServiceNow
- Hybrid data ecosystems such as Databricks, Snowflake, Cloudera, and Teradata
- Expanding data pipelines powered by AI, Machine Learning (ML), and Large Language Models (LLMs)

The reality is, security perimeters don't work the way they used to. The threats you're up against don't just pound down the walls, they slip inside unnoticed. Insider threats, misconfigured cloud settings, and sophisticated cyberattacks mean that just one vulnerable entry point can compromise everything.

THE SOLARWINDS® WAKE-UP CALL

If you think your organization is immune, consider the 2020 SolarWinds® attack—one of the most alarming security breaches in history. Hackers infiltrated software updates, affecting 18,000 organizations worldwide, including major tech firms and government agencies. The worst part? The attack went undetected for months. It happened because of:

- Untracked credentials left unguarded
- Weak configuration management
- A lack of real-time data visibility

The aftermath was brutal—months of forensic investigations, regulatory scrutiny, and reputational damage. If nothing else, SolarWinds proved one thing: the real target isn't the network, it's the data.

PRIVACY REGULATIONS AND THE "RIGHT TO ERASURE"

In response to growing security concerns, governments worldwide have tightened data privacy laws. You've probably heard of GDPR's "right to be forgotten" (Article 17)—a policy that allows individuals to demand the deletion of their personal data under specific conditions. Sounds simple, right? Except it's not. Businesses are caught in a balancing act between:

- Consumer rights – Individuals demand greater control over their personal data.
- Operational efficiency – Data is needed for analytics, AI, and business insights.
- Regulatory pressure – Non-compliance can lead to fines of €20 million or 4% of annual revenue.

And GDPR isn't alone. Canada's Law 25, the EU's Digital Operational Resilience Act (DORA), and countless emerging regulations across the globe are demanding stricter data minimization and governance.

THE COST OF GETTING IT WRONG

So what happens if your organization falls short?

$1.2 billion in fines issued across Europe in 2023 for non-compliance

Businesses hesitating to use analytics for fear of violating privacy laws

Skyrocketing compliance costs from endless audits and security overhauls

Reputational damage that lasts long after a breach is contained

This is why organizations are ditching outdated security models and embracing data-centric security—where protection is embedded into the data itself, rather than relying on a fragile perimeter or access controls that simply surround data with layers of security.

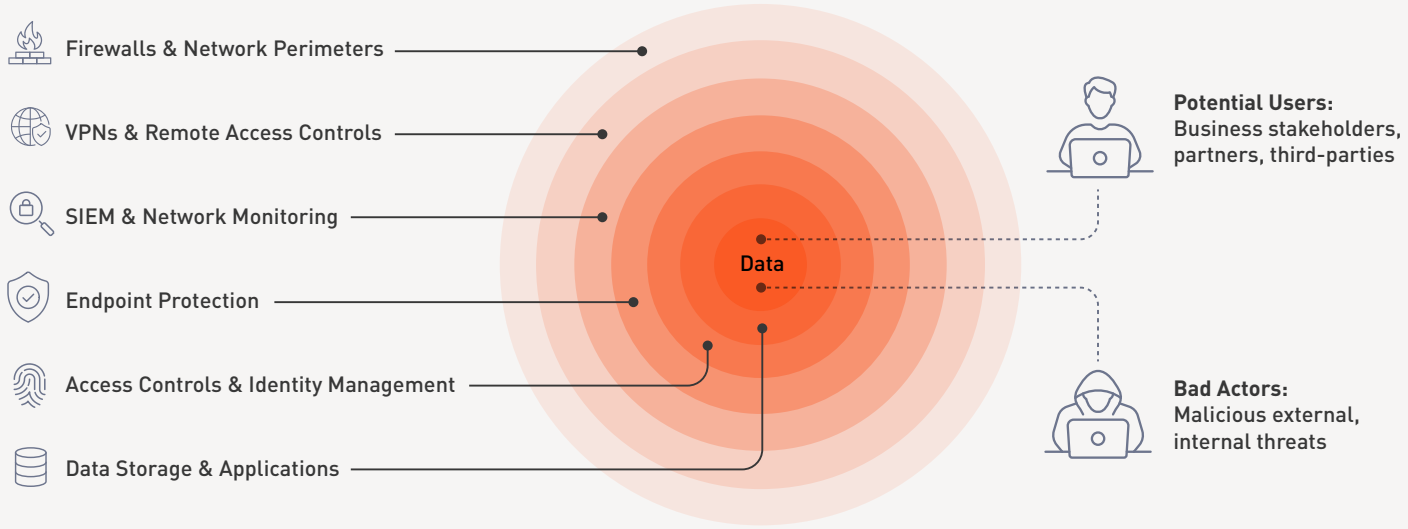
WHAT'S NEXT?

The question isn't *if* you need to rethink your approach to security, it's not even *how soon*, it's *why haven't you already?* In the next chapter, we'll dive into the critical flaws of the legacy security models you are using today and why they're holding your business back. We'll show you how compliance, privacy, and innovation must go hand in hand.

02

The Pitfalls of Traditional Security Methods

You wouldn't leave a vault full of cash unguarded just because your bank's front doors are locked, right? Yet, many organizations rely solely on traditional security methods—like firewalls and even access controls—to protect their data. These legacy methods assume threats only come from outside and focus on infrastructure rather than the data itself. But data no longer stays neatly behind castle walls; it flows across applications, storage systems, and cloud environments. When security doesn't enable a data-centric approach, sensitive information becomes dangerously exposed.



THE SHORTCOMINGS OF PERIMETER-BASED SECURITY

For decades, businesses treated security like building a fortress: Keep the bad guys out, carefully control entry points, and assume everything inside stays safe. Firewalls acted as gatekeepers, blocking unauthorized external traffic, while access controls managed who could reach critical systems, applications, and data. Application controls governed interactions within software to prevent misuse, and DLP tools monitored data flows, flagging suspicious transfers or activities. But today, this traditional perimeter-focused approach alone isn't enough to secure data effectively as it moves freely beyond conventional boundaries.

But here's the problem: Data doesn't sit still. It moves continuously between on-premises data centers (Oracle, Teradata, SQL Server), cloud service providers (AWS, Azure, Google Cloud), data warehouses (Snowflake, Databricks), SaaS applications (Salesforce, ServiceNow), and countless third-party partners. The moment data enters an AI pipeline, the traditional security measures you've built no longer matter. This is when blind spots emerge, leaving sensitive information vulnerable to data exfiltration—enabling attackers to quietly siphon off data without setting off alarms.

THE OPTUM HEALTHCARE BREACH: A COSTLY BLIND SPOT

Imagine you're responsible for securing patient records at a healthcare giant like Optum. You've invested in firewalls, access controls, and endpoint protection. But one day, 1.1 million patient records are exposed because personal health information (PHI) wasn't properly de-identified in a database.

- Regulators demand answers. Compliance violations trigger investigations.
- Patients panic. No one wants their medical history exposed.
- The company scrambles. Weeks of incident response, legal fees, and public relations damage control ensue.

The kicker? This could have been avoided if security focused on the data itself instead of just controlling access to the network, infrastucture, and applications.

THE CHURN EFFECT: SECURITY TEAMS STUCK IN A LOOP

If you ask security professionals what their biggest frustration is, many will say the same thing: They're always reacting instead of preventing.

This churn effect is exhausting and costly. Siloed security tools—SIEMs, firewalls, endpoint protections, access controls, application controls, and network monitoring—fail to work together. Security teams are forced to manually investigate, patch, and document everything. And because compliance audits are relentless, teams are always chasing the next fix rather than addressing the root problem.

MOVEIT'S $10 MILLION MISTAKE: A CASE STUDY IN DISJOINTED SECURITY

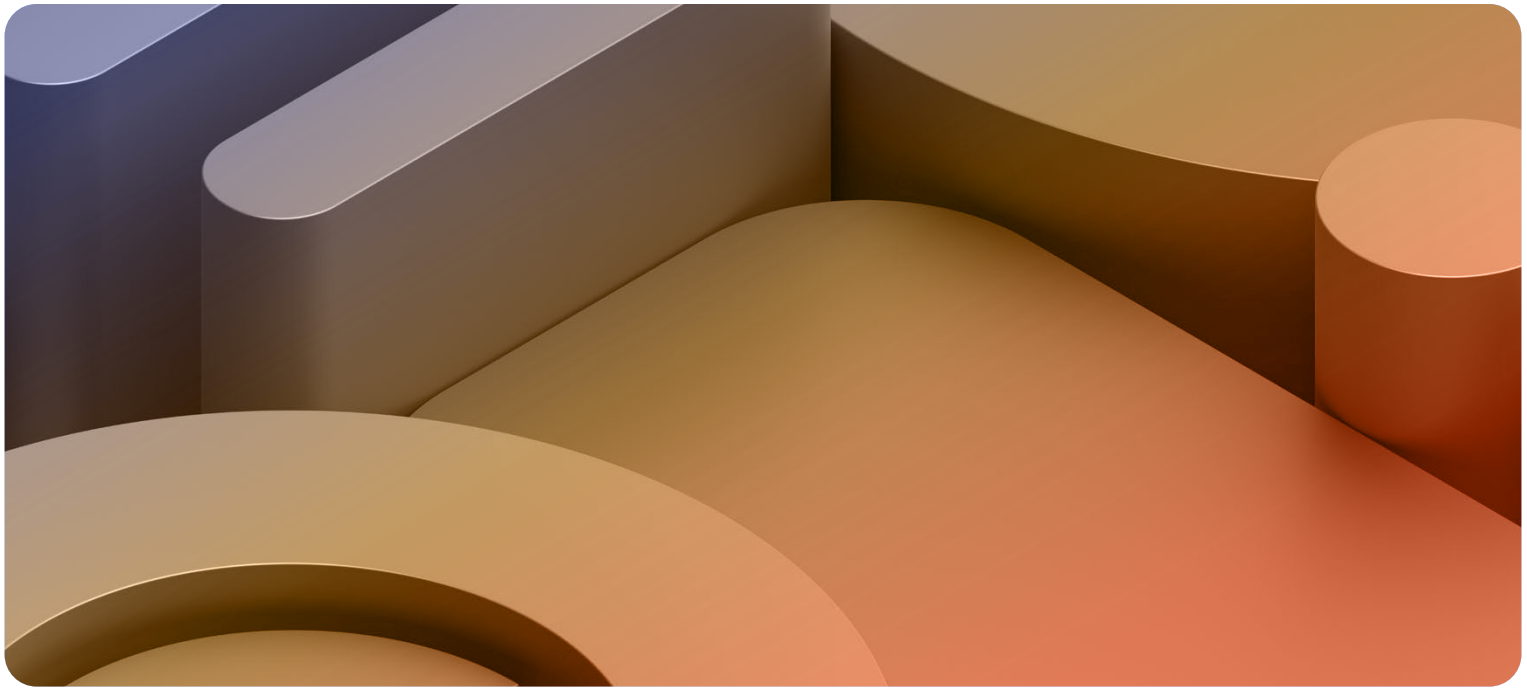
The 2023 MOVEit® breach is a perfect example of what happens when security doesn't follow the data.

- 60 million records were exposed. Why? File transfers weren't properly secured.
- Companies scrambled to contain the breach. Without real-time monitoring, it took too long to detect.
- MOVEit® was fined $10 million. Regulators aren't forgiving when security lapses cost consumers their privacy.

It wasn't just one weak spot. It was an entire system that failed to protect data as it moved.

A BETTER APPROACH: SECURITY THAT'S EMBEDDED INTO THE DATA

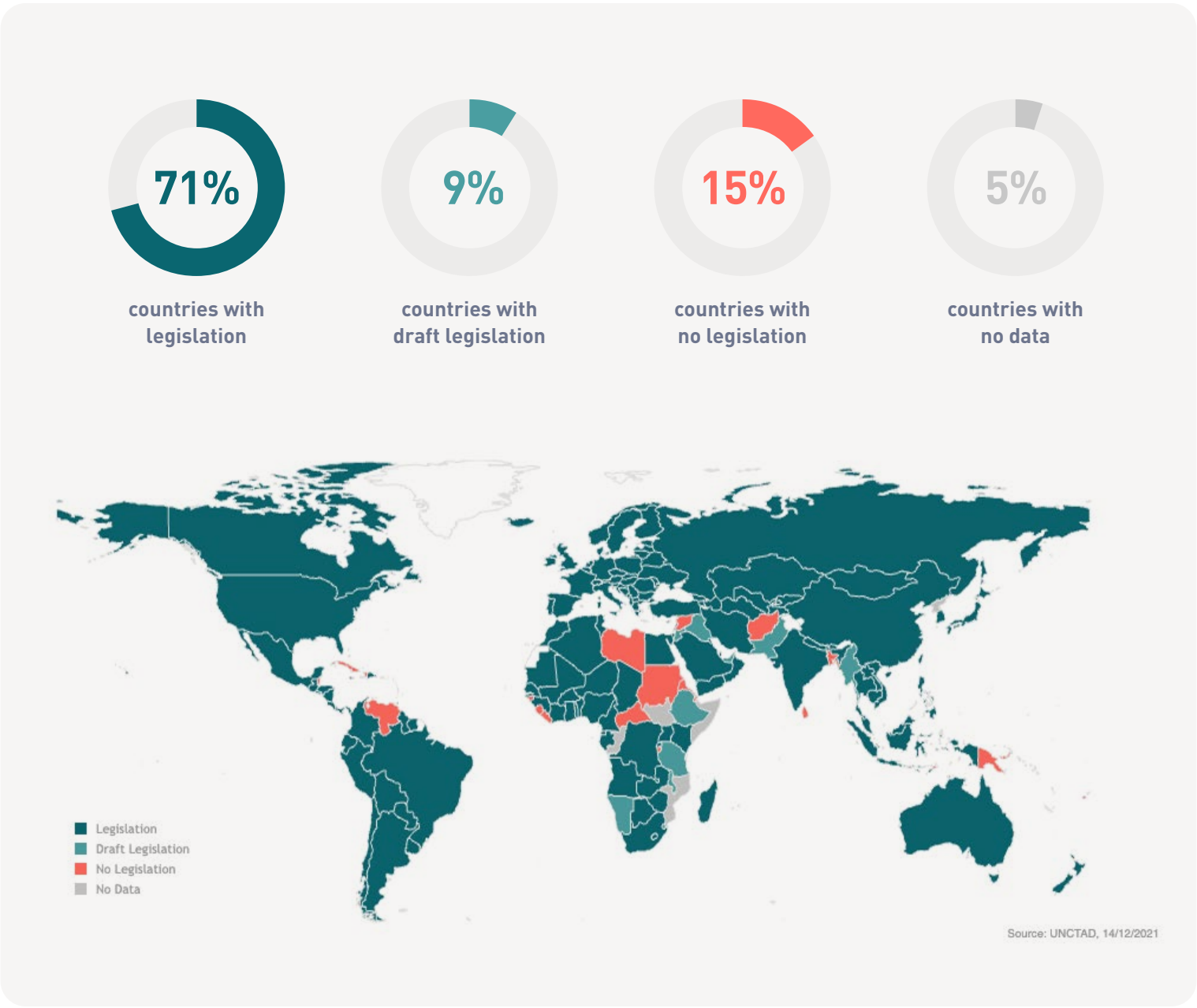
The old way isn't working. The future of security is data-first, where protection stays with the data no matter where it moves. In the next chapter, we'll explore the privacy revolution and why companies should be shifting to data-centric security models to stay compliant and competitive.



03

Navigating the Privacy Landscape

If it feels like privacy laws are coming at you from all directions, it's because they are. Over the last decade, more than 140 countries have introduced regulations designed to put individuals back in control of their data. But for security pros, compliance officers, and IT leaders, this explosion of laws isn't just about protection—it's a complex puzzle of overlapping rules, conflicting requirements, and ever-growing stakes. Get it wrong, and the consequences range from massive fines to legal nightmares and lost trust.



THE GLOBAL PRIVACY SHIFT: WHY IT'S HAPPENING NOW

For years, companies collected, stored, and shared personal data with little oversight. Then came the wake-up calls—breaches exposing millions of customer records, rising public outrage, and lawmakers finally stepping in. Take the 2018 Marriott breach, where 500 million guest records were compromised, leaking travel details, payment info, and passport numbers. That breach alone cost the company $123 million in fines.

The takeaway? Beyond being a security risk, data hoarding without protection is a financial disaster in the making. Governments worldwide are now demanding that companies minimize the data they collect, safeguard it with strong security measures, and prove they're doing it right.

PRIVACY LAWS: A THREE-PART CHALLENGE

Understanding the privacy landscape means breaking it down into three key areas:

1

GLOBAL INFLUENCE: THE HEAVYWEIGHTS

Some regulations set the bar for everyone—whether companies like it or not.

- GDPR (Europe, 2018): The gold standard of data privacy, giving individuals control over their data, enforcing strict security measures, and hitting violators with multi-million-dollar fines.
- APPI (Japan), PDPA (Singapore), DPDP (India, 2023): Strong consent and security rules influencing data-handling standards across the Asia-Pacific region.

Impact? If you operate globally, these laws shape your entire approach to data protection—pushing for encryption, strict access controls, and audit-ready compliance.

2

INDUSTRY-SPECIFIC RULES: HIGH STAKES FOR CERTAIN SECTORS

Some industries deal with data so sensitive that governments impose extra safeguards.

- HIPAA (U.S.): Health data protection that demands ironclad security for patient information.
- PCI DSS: Payment security standards that force businesses to protect credit card data or risk millions in penalties.

Impact? Healthcare, finance, and e-commerce companies face double the compliance burden—meeting both general privacy laws and sector-specific rules.

3

REGIONAL LAWS: THE LOCALIZED MAZE

Different countries tweak privacy laws to fit their unique political and economic priorities.

- Canada's Law 25: Stronger consent requirements and automatic breach notifications.
- Brazil's LGPD: Similar to GDPR but with added data portability rules.
- Australia's Privacy Act: Emphasizes individual access to data and stricter security requirements.

Impact? Businesses handling data across multiple regions must juggle different rules for breach reporting, consent, and retention—making compliance a logistical nightmare when trying to adhere to the lowest common denominator.

THE COLLISION OF PRIVACY LAWS AND DATA SHARING

Let's say your company relies on AWS, Azure, or Snowflake for analytics. What happens when one law says you must delete data, while another requires you to keep it? Consider these regulatory clashes:

GDPR (EU) explicitly grants individuals the "right to erasure," mandating organizations to erase personal data upon request.

("...the right to obtain... the erasure of personal data..." – GDPR, Art.17)

APPI (Japan) emphasizes retaining personal data securely for defined purposes and durations, complicating immediate erasure.

("...Personal data shall not be retained beyond the scope necessary for achieving the purpose..." – APPI, Art.19)

LGPD (Brazil) supports data portability, allowing individuals to request transfer of personal data, which doesn't always neatly align with HIPAA's strict restrictions on data sharing and security requirements.

(LGPD grants users "data portability rights," while HIPAA requires "stringent safeguards against data sharing.")

PCI DSS adds complexity, requiring payment data be protected and stored securely, often constraining flexibility in cloud environments.

("Cardholder data must be retained only as long as necessary..." – PCI DSS Requirement 3.1)

These regulatory contradictions underscore how traditional security measures alone struggle to maintain compliance across today's evolving data landscape.

THE BUSINESS IMPACT: RISK VS. OPPORTUNITY

THE RISKS

FINES & LEGAL TROUBLE

Non-compliance with privacy regulations comes with a hefty price tag. For example, GDPR fines across Europe exceeded $1.2 billion in 2023, and cases like Marriott's 2018 breach resulted in $123 million in penalties. Regulatory scrutiny is unforgiving, and the financial fallout can cripple businesses.

SLOWER INNOVATION

Complex compliance requirements often discourage companies from fully utilizing their data for analytics or AI initiatives. This hesitation stifles innovation and prevents organizations from unlocking the full potential of their data.

LOST CUSTOMER TRUST

A single data breach can damage customer relationships irreparably. Headlines about exposed sensitive information erode confidence, and rebuilding trust can take years—if it's even possible.

THE OPPORTUNITIES

BUILD TRUST

Consumers are more concerned about privacy than ever before. In fact, 80% worry about their online privacy and data security, and 83% say data protection is a key factor in determining trust in a brand. Companies that prioritize privacy can win big—87% of consumers are more likely to stay loyal to businesses that value their privacy, and 94% remain loyal to brands that are fully transparent about how their data is used. Building trust through strong privacy practices demonstrates both good ethics and good business.

UNLOCK NEW MARKETS

Privacy compliance can offer a company a competitive advantage. With 82% of the world's population now covered by privacy laws, companies that meet these requirements can expand into new regions where others can't. On the flip side, 48% of consumers have stopped shopping with companies due to privacy concerns. By investing in compliance and transparency, businesses can unlock new markets and stand out in an increasingly regulated world.

STRONGER SECURITY = BETTER BUSINESS

Investing in stronger security pays off. The average cost of a data breach hit a record $4.88 million in 2024, but companies with proactive measures like AI-driven security automation saved an average of $2.2 million per breach. Organizations with dedicated incident response teams saved even more: $1.76 million per breach. Strong security not only prevents breaches but also ensures long-term business stability, as 60% of small businesses that experience a cyberattack go out of business within six months. The Reality: Privacy Is Now a Core Business Function.

If you work in security or compliance, your job has changed. Privacy laws aren't just an IT issue, they shape how businesses store, share, and analyze data. Every decision about security—from encryption on Oracle to compliance tracking on Azure—is now a balancing act between protecting data and maintaining its utility.

The world is shifting toward a privacy-first mindset, and businesses that adapt will lead the way. The challenge now? Finding a way to make compliance manageable—without drowning in complexity and costs.

In Chapter 4, we'll explore what a future with smarter, simplified privacy protection could look like—and how to get there.

04

The Industry Shift Toward Data-Centric Security

As discussed in previous chapters, businesses have relied on perimeter-based security models—firewalls, endpoint protections, access controls, application controls, and network monitoring—to safeguard their most sensitive information. These traditional defenses, designed to keep bad actors out, have defined enterprise security strategies for decades.

But today, data is no longer confined within organizational perimeters. It moves fluidly between cloud environments, AI models, third-party integrations, and global business networks. Cybercriminals and compliance regulators have shifted their focus—they no longer target just infrastructure; they target data itself.

Organizations that fail to evolve beyond legacy security strategies face growing risks, from data breaches and insider threats to escalating regulatory penalties.

WHY TRADITIONAL SECURITY MODELS ARE FAILING

Historically, enterprise security has centered around defending the perimeter—securing networks, endpoints, and user credentials. The assumption was simple: If you keep attackers out, the data stays safe.

That assumption no longer holds. Today's attackers no longer need to break through firewalls—they bypass traditional defenses entirely by:

- Exploiting stolen credentials or weak authentication.
- Using supply chain attacks to infiltrate systems indirectly.
- Targeting cloud misconfigurations and third-party vendors.

As previously mentioned, this shift has been evident in some of the largest data breaches in recent years:

MARRIOTT

2018

A breach affecting 500 million guests revealed how poor data visibility leads to prolonged security failures.

solarwinds

2020

A supply chain attack compromised thousands of organizations, proving external defenses are no longer enough.

Optum

2023

A healthcare data breach exposed 1.1 million patient records due to inadequate data governance.

Each of these incidents exploited weaknesses in data security, not just infrastructure.

Companies that focus on stopping only external threats often fail to recognize vulnerabilities inside their own environments, such as:

- Unknown or untracked sensitive data, lacking appropriate security controls.
- Overly broad access permissions and access control lists, increasing insider threat risks.
- Compliance blind spots, exposing businesses to regulatory fines and reputational damage.

An infrastructure-based approach simply cannot protect data that moves across cloud applications, AI platforms, and third-party ecosystems. This reality has driven organizations toward data-centric security—a model that secures the data itself, wherever it resides.

INDUSTRY INSIGHTS: WHY TRADITIONAL SECURITY METHODS NO LONGER WORK

Traditional security methods—often referred to as infrastructure-centric or network-based security—include perimeter defenses like firewalls, VPNs, intrusion detection and prevention systems (IDS/IPS), and access controls. These methods rely heavily on protecting network boundaries and infrastructure components rather than safeguarding the data itself.

Security analysts and industry leaders have recognized the urgency of this shift. Static security perimeters are no longer viable in an environment where remote work, cloud transformation, and AI-driven automation have fundamentally changed how organizations operate. Modern environments demand a shift toward data-centric approaches that protect sensitive information directly, regardless of its location or how it's accessed.

Network-based security models

MUST EVOLVE

Gartner's 2024 Strategic Roadmap for Data Security highlights that network-based security models must evolve, particularly as businesses embrace cloud-native applications and hybrid infrastructure.

305%

reduction in breach-related costs for companies investing in data-centric security

Forrester's ROI Study found that companies investing in data-centric security reduce breach-related costs by 305%, primarily due to automated compliance enforcement and proactive risk management.

51%

of breaches occur across multiple cloud environments

IBM's 2023 Cost of a Data Breach Report revealed that the average data breach cost increased to $4.45 million, with 51% of breaches occurring across multiple cloud environments—a clear indicator that traditional security approaches are no longer enough.

These findings reinforce what security leaders have been warning for years: Protecting the network, hardening infrastructure, and controlling application access is no longer enough. Protecting the data itself must be the priority.

This transition toward data-first security models is not just a recommendation—for many organizations, it has become a business necessity.

THE SHIFT TOWARD DATA-CENTRIC SECURITY: KEY INDUSTRY CHALLENGES

Organizations aren't adopting data-centric security simply because it's an emerging trend—they are being forced to.

1. THE VISIBILITY GAP: UNKNOWN, UNTRACKED, AND UNPROTECTED DATA

Modern organizations struggle to locate and classify their sensitive data. Information is spread across on-prem databases, cloud platforms, and SaaS environments, yet many companies lack a unified view of their data assets.

What This Means for Security:

- Shadow IT creates hidden or unsanctioned technology use, making visibility difficult.
- Unstructured data leads to difficulty in tracking sensitive information effectively.
- Expanding AI pipelines introduce new compliance blind spots and vulnerabilities.
- Manual data classification leaves organizations uncertain of sensitive data locations and access permissions.
- Bad actors exploit visibility gaps, frequently targeting unprotected or misconfigured data stores and AI-driven workflows.

The Consequence:

- Data breaches go undetected for months, significantly increasing exposure risks.

2. REGULATORY PRESSURES AND COMPLIANCE BURDENS

Privacy laws like GDPR, DPDP, HIPAA, and PCI DSS are no longer just about IT security—they directly regulate how businesses handle and protect data.

What This Means for Security:

- Organizations must demonstrate real-time data protection and auditing to stay compliant.
- Regulations are evolving faster than most companies can adapt, leading to compliance failures despite good intentions.
- Companies must carefully balance compliance risks with data utility, ensuring data remains protected without sacrificing its value for analytics, innovation, and business growth.

The Consequences:

- Companies lacking automated compliance enforcement struggle to keep pace, leading to regulatory penalties and reputational damage.
- Non-compliance fines are increasing—global penalties exceeded $2.5 billion in 2023 alone.

3. CLOUD & AI: A NEW ATTACK SURFACES FOR DATA EXPOSURE

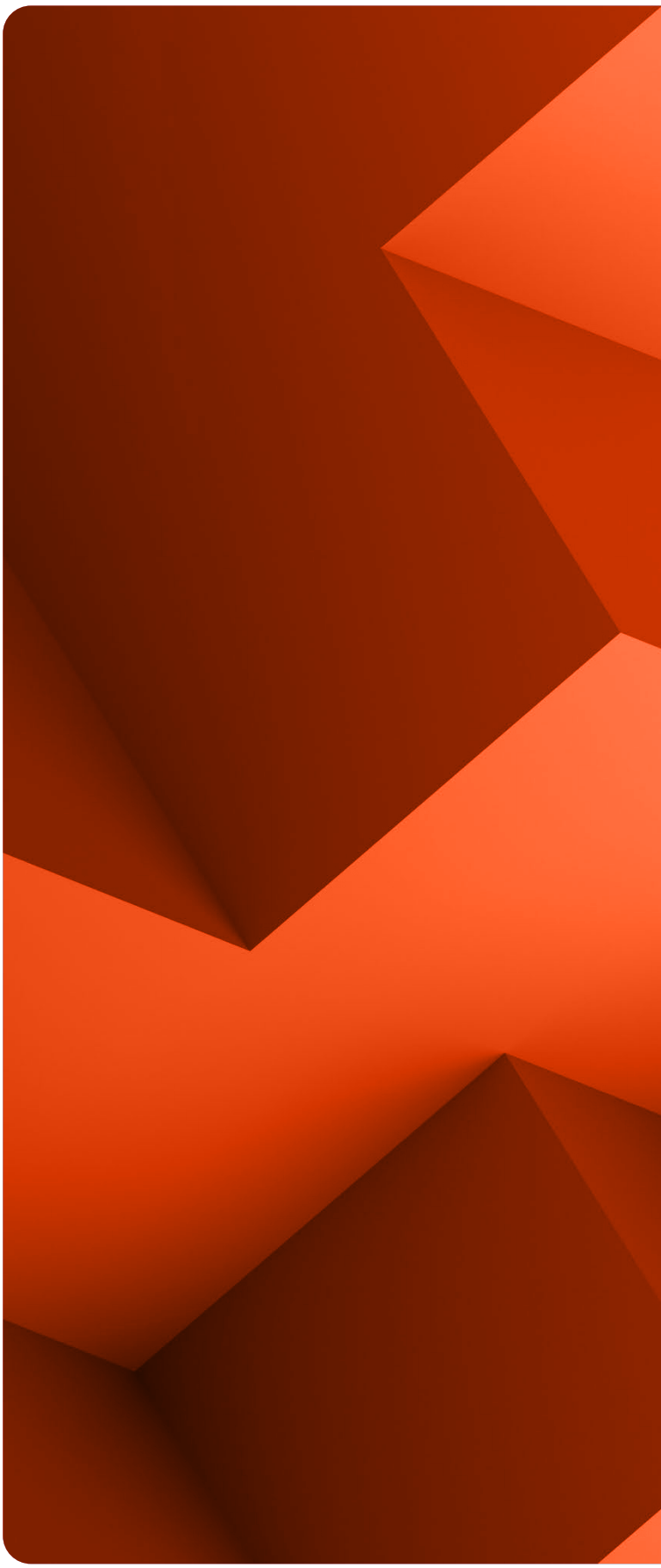
AI-driven analytics, cloud migration, and multi-cloud strategies offer new business opportunities—but also introduce new security risks.

What This Means for Security:

- AI, Machine Learning, and GenAI models—especially Retrieval-Augmented Generation (RAG) pipelines—rely on vast amounts of sensitive structured and unstructured data that must remain secure during training and inference.
- Data continuously flows across hybrid environments and diverse pipelines, where traditional or environment-specific controls (like those in Snowflake or cloud-based services) often fail to provide sufficient protection once data leaves their boundaries.
- Under the cloud-shared responsibility model, infrastructure providers secure their platforms but leave responsibility for protecting the data itself entirely up to your organization. This makes securing data at the data layer critical, especially as it moves across complex AI-driven ecosystems.

The Consequence:

- If security is not embedded into data workflows, sensitive information is at higher risk of exposure, data utility can be compromised, access to valuable data may be blocked, or organizations may be forced to accept increased risk.



THE EVOLUTION TOWARD DATA-CENTRIC SECURITY

Instead of locking down systems, businesses should be shifting their focus to securing the data itself. This transition requires a fundamental shift in strategy:

KEY AREA	TRADITIONAL SECURITY MODEL	DATA-CENTRIC SECURITY MODEL
Primary Focus	Networks, infrastructure, applications, endpoints, and users	Data itself, wherever it moves
Access Control	Protects systems and user accounts	Protects data at the field, column, or row level
Threat Detection	Monitors external attacks	Detects unauthorized data access
Regulatory Compliance	Compliance applied to IT systems	Compliance built into data security
Cloud & AI Protection	Security struggles with multi-cloud and siloed systems	Security is embedded directly into the data itself, ensuring protection travels seamlessly wherever the data goes

Organizations that embrace data-centric security achieve a more resilient, adaptable, and regulation-ready security posture.

PREPARING FOR DATA-CENTRIC SECURITY: WHAT'S NEXT?

Chapter 5 will outline the practical steps organizations must take to:

- Build a structured data-centric security model
- Implement security policies without disrupting operations
- Ensure compliance while enabling AI, cloud, and analytics

05

Implementing Data-Centric Security Into Your Ecosystem

Chapter 4 highlighted the failures of perimeter-based security and the challenges driving businesses toward data-centric security. Now, the focus shifts to how organizations can implement a data-centric security model—one that ensures security follows the data while enabling compliance, efficiency, and growth.

A successful transition to data-centric security requires a phased approach, integrating security at every stage of the data lifecycle while ensuring minimal business disruption.

UNDERSTANDING YOUR ECOSYSTEM: WHERE SECURITY NEEDS TO WORK

Every organization operates within a complex data environment, where information constantly moves between systems, platforms, and partners. Security must be adaptive, following the data without hindering performance or analytics. Here is where you would typically look for common components of a modern data ecosystem.

On-prem databases	IBM Db2, Oracle, SQL Server – Storing legacy records and business-critical structured data.
Cloud platforms	AWS, Azure, Google Cloud – Hosting scalable applications, analytics, and AI/ML workloads.
Data warehouses	Snowflake, Databricks, Cloudera – Powering data-driven initiatives including BI, AI, and ML.
SaaS & enterprise applications	Salesforce, SAP, ServiceNow – Managing customer, financial, and operational data in the cloud.
File systems, extract, transform, and load (ETL) pipelines & integrations	Moving, transforming, and syncing sensitive data across internal systems and third-party providers.

In a data-centric model, security is not applied in isolated layers—it must be embedded across the entire ecosystem, ensuring data remains protected at every stage of its lifecycle.

THE FIVE CORE COMPONENTS OF A DATA-CENTRIC SECURITY STRATEGY

A data-centric approach requires organizations to adopt five key implementation steps, aligned with the challenges identified in Chapter 4:

DATA DISCOVERY & CLASSIFICATION: IDENTIFYING AND UNDERSTANDING YOUR SENSITIVE DATA

Understanding what data you have, where it resides, and how it's used is the first step in protecting it—especially in complex, hybrid environments.

Why It Matters:

- Security begins with visibility—organizations cannot protect what they cannot see.
- Manual data classification processes create compliance blind spots, making it difficult to balance understanding data risk with meeting data consumption needs.

Best Practices:

- Implement automated data discovery tools to locate PII-, PHI-, and PCI-regulated data across on-prem, cloud, and SaaS environments.
- Continuously scan structured and unstructured data—including data used by AI and chatbots—for newly created or modified sensitive information, and update classification policies accordingly.

Action Step: Organizations should deploy centralized data classification engines that scan structured and unstructured data for sensitive elements.

ACCESS CONTROLS & PERMISSIONS: DEFINING WHO CAN ACCESS WHAT DATA

Managing access based on roles, attributes, and business need helps reduce the risk of internal misuse and external compromise.

Why It Matters:

- Overly broad permissions are one of the leading causes of data breaches.
- Insider threats and privileged user abuse continue to rise due to lack of access governance.

Best Practices:

- Enforce Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to restrict permissions based on business need.
- Define field-level access controls to limit the exposure of sensitive records, customer details, or financial transactions.
- Implement Zero Trust policies—requiring identity verification before granting access to sensitive data.

Action Step: Organizations should audit user roles to ensure access is granted on a least-privilege basis, limiting excessive permissions.

DATA PROTECTION MECHANISMS: SECURING DATA ACROSS ITS LIFECYCLE

Effective protection means securing data not just at rest or in transit, but throughout its entire lifecycle—without sacrificing usability.

Why It Matters:

- Once data is compromised, encryption alone can be reversed if keys are exposed—tokenization and masking remove this risk by replacing sensitive data with non-exploitable values. These methods render the data useless to attackers, even in the event of a breach.
- To stay secure and compliant, companies must protect data at rest, in transit, and in use—while preserving its usability for analytics, AI, and business operations.

Best Practices:

- Apply encryption, tokenization, and format-preserving encryption (FPE) at the point of data collection to protect it before it moves downstream.
- Use dynamic data masking to enable secure analytics while keeping PII or financial data hidden from unauthorized users.
- Ensure consistent security policies across databases, file systems, APIs, and SaaS platforms.

Action Step: Organizations should apply tokenization for PCI data, encryption for regulatory compliance, and masking for analytics workflows.

CONTINUOUS MONITORING & COMPLIANCE READINESS

Real-time visibility into data access and movement is essential for detecting threats early and proving compliance when it counts.

Why It Matters:

- Regulations like GDPR, DPDP, HIPAA, and PCI DSS demand real-time tracking of data access and movement.
- Security teams often struggle to detect breaches until long after data has been exfiltrated.

Best Practices:

- Deploy automated monitoring solutions that provide real-time alerts on unauthorized access attempts.
- Maintain an automated audit trail for regulatory compliance reporting and internal security reviews.
- Integrate Security Information and Event Management (SIEM) tools to detect anomalies in data access patterns.

Action Step: Organizations should implement real-time logging tools that track who accessed what data, when, and for what purpose.

DATA GOVERNANCE: ENSURING COMPLIANCE AND POLICY ENFORCEMENT

Centralized governance ensures security and compliance policies are applied consistently across every system, team, and data flow.

Why It Matters:

- Compliance violations can lead to multi-million-dollar fines and irreversible reputational damage.
- Inconsistent security controls across cloud, SaaS, and on-prem environments increase risk.

Best Practices:

- Use centralized policy management platforms to enforce consistent security rules across all environments.
- Automate compliance reporting to reduce manual audit efforts and ensure ongoing adherence to regulations.
- Align security governance with business objectives, ensuring security enables, rather than disrupts, operations.

Action Step: Organizations should automate compliance tracking to proactively manage regulatory requirements without disrupting business workflows.

TRANSITIONING FROM LEGACY SECURITY TO DATA-CENTRIC SECURITY

Shifting from traditional perimeter security to a data-first model requires a structured, phased approach:

PHASE 1: ASSESS RISKS & IDENTIFY GAPS

- Conduct a data risk assessment to identify unprotected PII, PHI, or PCI data.
- Audit user access controls and remove excessive permissions.

PHASE 2: APPLY PROTECTION AT THE SOURCE

- Deploy tokenization, encryption, and dynamic masking at data entry points.
- Ensure consistent protection across cloud, on-prem, and hybrid environments.

PHASE 3: STANDARDIZE SECURITY & COMPLIANCE POLICIES

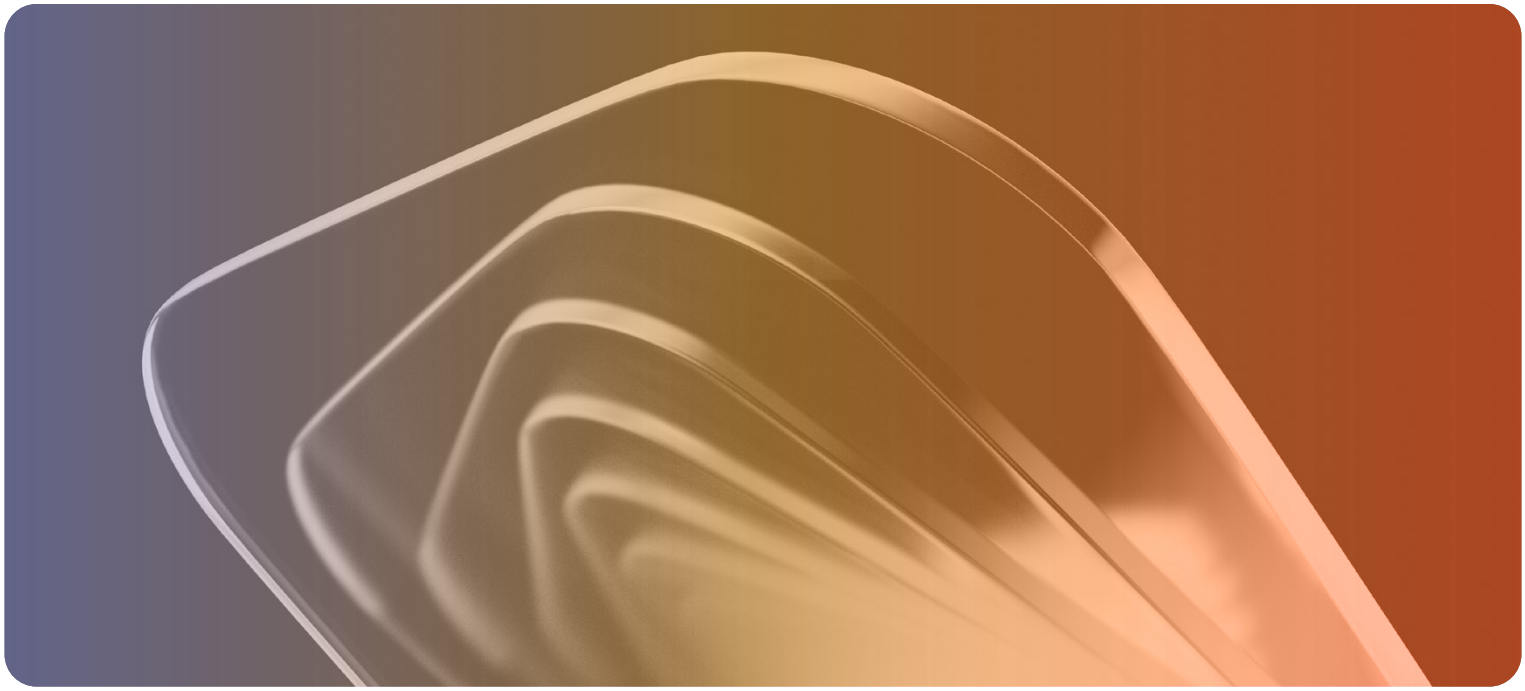
- Implement centralized governance to enforce security policies across databases, applications, and analytics platforms.
- Automate audit logging and compliance reporting.

PHASE 4: MONITOR, ADAPT & OPTIMIZE

- Integrate real-time monitoring and threat intelligence tools.
- Continuously refine security policies based on risk assessment insights.

A structured, data-centric security strategy ensures organizations can protect sensitive data at every stage while maintaining regulatory compliance and business agility.

In Chapter 6, we'll explore how Protegrity operationalizes data-centric security.



06

Protegrity's Approach to Data-Centric Security

Chapter 5 outlined the steps to implementing data-centric security—from discovering and classifying sensitive data to enforcing encryption, access controls, and continuous monitoring. But execution requires the right technology.

This is where Protegrity helps. Organizations face growing regulatory pressure, rising breach risks, and increasing data complexity across on-prem, cloud, and third-party environments. Traditional security models can't keep up, but a data-centric approach can—when it's backed by the right tools.

Protegrity enables organizations to put data-centric security into action, embedding compliance, security, and governance controls directly into their ecosystems. By securing data at the source, businesses can simplify regulatory adherence, mitigate breach risks, and unlock the value of their information—without compromising security.

WHY PROTEGRITY? A DATA-CENTRIC APPROACH TO COMPLIANCE, SECURITY, AND RISK REDUCTION

Organizations must strike a balance between compliance, security, and data usability. Protegrity enables businesses to do the following:

DATA-CENTRIC SECURITY PRINCIPLE	PROTEGRITY ALIGNMENT & PRODUCTS
Data Discovery & Classification: Identifying and categorizing sensitive data across the organization's ecosystem.	Automate data discovery and classification across structured and unstructured environments to eliminate compliance blind spots.
Access Controls & Permissions: Implementing role-based access controls and least privilege to ensure only authorized users can access specific data.	Enforce role-based access controls (RBAC) and dynamic masking to secure access across SAP, Salesforce, and financial applications.
Data Protection Mechanisms: Applying encryption, tokenization, and masking to secure data in various states.	Vaultless Tokenization and Encryption protect sensitive data at the source across SQL Server, AWS S3, Snowflake, AI, and ETL pipelines.
Continuous Monitoring & Auditing: Tracking data usage to detect anomalies and unauthorized access in real-time.	Real-time monitoring and audit logging provide GDPR, DPDP, HIPAA, and PCI DSS audit trails and ensure proactive risk detection.
Data Governance: Enhancing regulatory compliance by managing data according to industry standards.	Policy-driven security automates enforcement across hybrid environments, ensuring continuous compliance with data privacy laws and regulatory frameworks.

HOW PROTEGRITY EMBEDS COMPLIANCE CONTROLS INTO YOUR ECOSYSTEM

1. COMPREHENSIVE DATA DISCOVERY AND RISK ASSESSMENT

- Scan structured and unstructured data across on-prem, cloud, and hybrid environments to identify sensitive data exposure risks.
- Automated discovery eliminates compliance blind spots, ensuring organizations maintain visibility over regulated data assets.

Case Study: A top-5 bank reduced compliance costs by 25% by automating data classification and policy enforcement with Enterprise Security Architecture (ESA) on Azure.

2. SOURCE-LEVEL PROTECTION: SECURING DATA AT THE POINT OF ORIGIN

- Database Protector encrypts and tokenizes sensitive data in IBM Db2, SQL Server, and Oracle—applying controls before data moves downstream.
- Cloud Protector secures workloads in AWS, Azure, and Google Cloud to prevent unauthorized access and exposure.

Case Study: A global healthcare provider secured patient data in IBM Db2, reducing compliance risk and avoiding costly HIPAA violations.

3. POLICY-DRIVEN SECURITY AND ACCESS CONTROLS

- Application Protector applies dynamic masking, ensuring data access policies are automatically enforced across SAP, Salesforce, and financial applications.
- File Protector secures structured and unstructured data in ETL pipelines, AWS S3, and enterprise file repositories—minimizing compliance risk.

Case Study: JustGiving leveraged vaultless tokenization on AWS, reducing PCI DSS compliance costs while building donor trust.

4. CONTINUOUS MONITORING AND COMPLIANCE READINESS

- Real-time logging ensures organizations are always audit-ready for GDPR, DPDP, HIPAA, PCI DSS, and industry-specific regulations.
- Centralized compliance dashboards help businesses prove regulatory adherence without manual compliance reporting overhead.

ENSURING COMPLIANCE WHILE ENABLING SECURE GROWTH

Protegrity enables organizations to embed compliance controls into their data ecosystem, reducing regulatory risk, preventing fines, and simplifying adherence to complex data privacy laws.

NEXT STEPS TO IMPLEMENT PROTEGRITY'S DATA-CENTRIC SECURITY

1. **Assess your compliance risk exposure –** Use ESA's automated discovery to locate and classify sensitive data across databases, cloud platforms, and analytics environments.
2. **Apply security at the source –** Deploy Protectors in high-risk areas such as SQL Server, AWS S3, Salesforce, and ETL pipelines, implementing tokenization and dynamic masking.
3. **Enforce policy-driven security –** Use ESA to automate governance, enforce security rules, and align policies across hybrid environments.
4. **Monitor and optimize security operations –** Ensure real-time compliance, track data access, and support secure AI, analytics, and digital transformation.

CONCLUSION: A SMARTER APPROACH TO SECURITY AND COMPLIANCE

Data-centric security is no longer optional—it is the only way for businesses to reduce compliance burdens, protect sensitive data, and avoid regulatory fines.

Protegrity provides the expertise, technology, and automation needed to enforce security at scale, ensuring compliance is embedded into business operations, not treated as an afterthought.

To learn more, visit **protegrity.com/demo** to see for yourself or explore **protegrity.com/api-playground** to try it firsthand.

PROTEGRITY.COM