A Strategic Guide For Controlling And Securing Your Data

Forrester's Data Security Control Framework

by Heidi Shey

January 19, 2021

Why Read This Report

In organizations that are complex or that have huge amounts of data, security, risk, and privacy pros often don't know where to start. A Zero Trust approach where data security is a key pillar is one path. Security standards provide another means forward. Compliance requirements offer yet another road, but we know compliance is not security. Security compliance is also not privacy compliance. This report provides a strategic framework for controlling and securing your data that is the foundation for what you can then adapt for security, compliance, and privacy needs.

Key Takeaways

A Strategic Foundation Enables You To Adapt Tactically

Security best practices, standards, and compliance requirements have commonalities. Understand these common points to build your core capabilities for data control. As new requirements arise, you can identify the gaps and tactical actions needed to fill them.

Build Your Foundation In Three Key Areas

Our data security and control framework breaks down the challenge of controlling and securing data into three areas: 1) defining the data; 2) dissecting the data; and 3) defending the data.

A Strategic Guide For Controlling And Securing Your Data

Forrester's Data Security Control Framework

by Heidi Shey
with Amy DeMartine, Kate Pesa, and Peggy Dostie

January 19, 2021

Table Of Contents

Related Research Documents

The Future Of Data Security And Privacy: Growth And Competitive Differentiation

The Zero Trust eXtended Ecosystem: Data

Zero Trust For Compliance

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

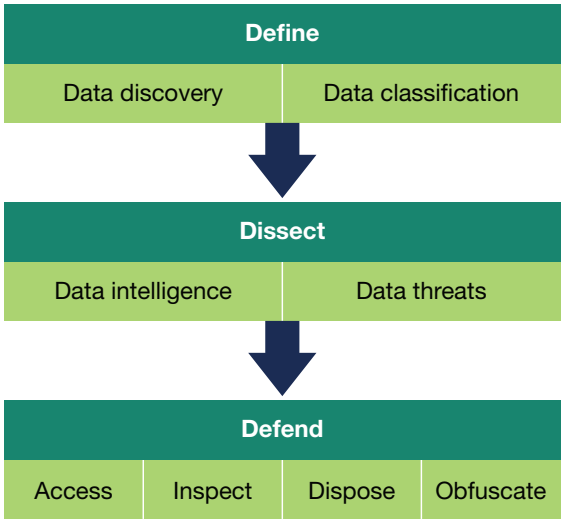
Build A Strong Foundation For Data Security And Compliance

For many organizations, an approach to data security means some combination of the following: data loss prevention, access control, and encryption. Then, it's a checklist of additional requirements that they must meet to be in compliance, meet contractual obligations, or remedy a failed audit. It's time to take a strategic — and data-centric — approach. This is what data security pros need to build core capabilities for data security that are shared across security best practices, standards, and compliance requirements.[1] It will also enable you to expand on these capabilities to support your privacy program.[2]

Start With Forrester's Data Security And Control Framework

Where to start? Here. Forrester's data security and control framework breaks down the challenge of controlling and securing data into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data (see Figure 1).

FIGURE 1 Forrester's Data Security And Control Framework



Defining The Data Simplifies Its Control

You can't protect it all: It's too operationally complex to encrypt everything, and it's too costly given all of your other responsibilities. In many cases, it's not even necessary: GDPR, for example, covers personally identifiable information of your customers and employees specifically. To better understand what you need to protect, discovery and classification are critical. Consider that:

- **Data discovery locates and indexes data.** To protect data, you must first know where users have stored it.[3] Data is strewn across their global data centers, file shares, laptops, desktops, mobile devices, and cloud storage. Security professionals, together with legal and privacy teams, must undertake data discovery to locate and index existing data and develop a lifecycle approach that continuously discovers data as users create it throughout the extended enterprise. Many tools that discover and classify data will allow you to know where data is, and what that data is — that is, they will discover and identify that data for you.[4]
- **Data classification tags data to make it easier to control and use.**[5] Classification here is often referred to as labeling or tagging. Security pros, together with their counterparts in legal and privacy, should define data classification levels based on data value and risk — such as public, internal, and confidential.[6] The classification of data (e.g., individual files, emails, database fields, etc.) can change as the value of the data changes over time.[7] Proper data defense depends on accurate classification — both identifying what this data is as well as its level of sensitivity — over time. Effective classification can also indicate whether you must archive the data for compliance purposes or whether it's subject to a privacy regulation.

Dissecting Data Helps Determine Its Value And Risk To The Business And To Security

Security and privacy pros also need continuous visibility into information about data use and the changing threats to the data. You want to build as thorough an understanding as possible of which networks, devices, apps, and users touch data. Specifically:

- **Data intelligence provides business and other contextual insights about data.** The business value of the data drives security strategy, policy, and technology decisions. For example, for the most sensitive data that is often exchanged with external parties, the security team can deploy solutions that will enable secure collaboration. For sensitive data that the business wants to use for data analytics, this could call for protection for data-in-use or de-identification tools.[8] It's also important to understand the state of data: How does this data normally flow, and how should it flow? Who is using this data, how often, and for what purpose? Why does the business have this data, how is it collected, and what is its useful lifecycle? What are the consequences if data integrity is compromised?
- **Data threat analysis identifies vulnerabilities, activity, and insight to guide decisions.** Understanding threats and risks to data helps S&R pros prioritize defenses. For example, comparing vulnerability data with device configuration and real-time threat data will tell the organization where its most vulnerable assets lie and help it create defenses that are more targeted and proactive. This visibility into user behaviors and actions, endpoint telemetry data and anomalies, access patterns, and more will allow S&R pros to quickly detect potential breaches or insider abuse.[9] It also provides a rich feed for security analytics platforms, improving an organization's detection and investigation capabilities.[10]

Defending Data Protects It From The Vast Array Of Modern Threats

As the number and sophistication of attacks increases, it's clear that security and privacy professionals must do a better job of defending data. Forrester's data security and control framework outlines four core measures to take:

- **Control access.** This ensures that the right user gets access to the right data at the right time.[11] To secure data throughout your ecosystem, strictly limit the number of people who can access data and continuously monitor their access levels throughout their employment. Security and privacy pros don't always recertify access when an employee shifts roles within the company. Employees often accumulate access and privileges as they are promoted or transferred within the firm. Security and privacy pros also often don't have insight into the access privileges of third-party users with whom data is shared.[12]
- **Inspect data usage patterns.** This can alert security teams to potential abuses. Both external cybercriminals and malicious internal users will leave artifacts of their attempts to breach your data security controls. Our Zero Trust Model mandates that you inspect and log all traffic on both your internal and external networks. You can accomplish this by deploying UBA or network analysis and visibility tools (such as metadata analysis, packet capture analysis, or flow analysis tools) and integrating them with your security analytics solution to give you visibility you need to proactively protect sensitive data.[13]
- **Dispose of data when it's no longer needed.** With proper classification and supporting controls, you can defensively dispose of any sensitive data no longer required by real business interests, compliance mandates, or data preservation obligations for investigations or litigation.[14] Resist the temptation to keep every byte of data just because you can.[15] Securely and defensively disposing of data in accordance with your retention policies is a powerful defensive tactic and mitigates legal risks, cuts storage and other IT costs, and reduces the risk of a data breach. This includes secure decommissioning and disposal of hard drives and storage devices.
- **Obfuscate data.** Cybercriminals use underground markets on the internet to buy and sell sensitive data, such as credit card numbers, credit reports, and even intellectual property.[16] This underground market operates according to the economic principles of supply and demand. If you remove the value of data, you eliminate incentives to steal it. You can devalue data using data abstraction and obfuscation techniques like encryption, tokenization, and masking.[17] Cybercriminals can't easily decrypt or recover data that you've encrypted or otherwise obfuscated — and then that data no longer has any value on the black market.

Recommendations

Five Additional Ways To Use This Strategic Framework

Forrester's data security and control framework is designed to help firms take a strategic, data-centric approach to securing their data. But it doesn't end there. You can use this framework to:

- **Communicate a high-level approach to executive management.** The details of your approach and controls matter, but it's easy to get lost in the tactical minutia and lose your audience. For executive management, this framework can help to break down and explain your overarching strategy in a way where both technical and non-technical stakeholders can clearly understand your direction, priorities, roadmap, and purpose.
- **Assess existing core capabilities to identify current gaps.**[18] This framework was originally designed because we saw how companies applied data controls without a clear understanding of their data, how it is used, and the most relevant risks to the data. While privacy compliance has helped to push competencies like data discovery and classification to the forefront, many organizations today may still find areas of improvement as they go through this framework. For example, secure data disposal is often a gap. You could revoke an encryption key or wipe a device to dispose of data in certain cases. However, disposal must also include considerations for secure shredding of hardcopy documents and IT asset disposition.
- **Evaluate portfolio vendors with these capabilities in mind.** There is no one single data security portfolio vendor to handle all your data security needs, given the range of data types you'd need to cover.[19] This framework outlines a data-centric and end to end approach. You can use it to see how your roster of portfolio vendors matches up with their built-in features, what capabilities you can complement from existing tools, and which capabilities you would need to augment or bring in best-of-breed.
- **Build a supporting business case for why security is not privacy.** Your data security strategy won't deliver privacy by default or enable your organization to meet privacy compliance requirements. While you may use some of the same tools, processes, and policies for both security and privacy use cases, privacy has specific and unique requirements. Three common areas for security and privacy that you can build on to expand your support for your organization's privacy program are data intelligence, identity awareness, and data controls.[20]
- **Engage for alignment with key data stakeholder groups' interests and requirements.** This can include risk management, data management, data governance, privacy, legal, marketing, and more. There will be shared interests and initiatives for building capabilities for data discovery and classification, supporting data lifecycle management (including secure disposal of data and assets), enabling data analytics or monetization (in a secure, compliant way), and securing data in data lakes to name a few.

Endnotes

[1] This report maps our Zero Trust framework against the control coverage for popular security frameworks and regulatory compliance requirements such as COBIT, FFIEC, and NIST CSF. In some cases, Zero Trust exceeds the security required by other compliance directives. For more information, see the Forrester report "Zero Trust For Compliance."

[2] For more information, see the Forrester report "The Future Of Data Security And Privacy: Growth and Competitive Differentiation."

[3] This is one of the significant struggles when security professionals attempt to deploy a DLP technology — if you can't locate where the enterprise stores its sensitive information, you don't know where to deploy controls. See the Forrester report "Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid."

[4] You can use data discovery and classification to gain greater visibility and understanding of the organization's sensitive data; secure sensitive data with appropriate controls and policies; and support compliance, privacy, and ethical data use. But to realize these benefits, you'll first have to select from a diverse set of vendors that vary by size, functionality, geography, and vertical market focus. For more information, see the Forrester report "Now Tech: Data Discovery And Classification, Q4 2020."

[5] To protect data and support data governance, security and risk (S&R) pros need to understand what data exists, where it resides, how valuable it is to the firm, and who can use it. This report outlines a five-step strategy to support your approach to sensitive data discovery and classification. For more information, see the Forrester report "A Five-Step Strategy For Data Discovery And Classification."

[6] Security and risk (S&R) pros can't expect to adequately protect customer, employee, and sensitive corporate data and IP if they don't know what data exists, where it resides, how valuable it is to the firm, and who can use it. See the Forrester report "Rethinking Data Discovery And Classification Strategies."

[7] Some data, such as acquisition plans or product roadmaps, can be highly confidential one day and then outdated and unimportant the next.

[8] For more information, see the Forrester report "The Forrester Tech Tide™: Data Security And Privacy, Q3 2019."

[9] With the growing threat of insider-driven security incidents, many companies are creating rigorous insider threat programs, but security and risk leaders need to ensure these programs remain compatible with privacy regulations such as GDPR. For more information, see the Forrester report "Don't Poison Your Employee Experience With The Wrong Approach To Insider Threat."

[10] As security information and event management (SIEM) technology becomes outdated and less effective, cloud-delivered security analytics platforms that provide custom detections will dictate which providers will lead the pack. For more information, see the Forrester report "The Forrester Wave™: Security Analytics Platforms, Q4 2020."

[11] For more information, see the Forrester report "Build Your Identity And Access Management Road Map."

[12] Asses your IAM maturity with Forrester's IAM maturity assessment tool. It is designed to help S&R professionals identify gaps in their current IAM strategy across all major identity and access management (IAM) functional areas, including identity management and governance (IMG), multifactor authentication (MFA), privileged identity management (PIM), and customer identity and access management. For more information, see the Forrester report "Forrester's Identity And Access Management Maturity Assessment."

[13] This report will break down the specific network tooling and packet level controls that security pros should consider as they move their organizations closer to a Zero Trust system. For more information, see the Forrester report "The Zero Trust eXtended Ecosystem: Networks."

[14] Many enterprises report significant e-discovery challenges, and awareness of key process elements varies greatly across tech management, legal, records management, security, and other functional roles. See the Forrester report "Q&A: eDiscovery Fundamentals For Content & Collaboration Professionals."

[15] Some data loses its value to the business as it ages. Corporate policy will also specify the length of time that technology management pros must retain data for regulatory compliance or broader information governance purposes.

[16] The dark web is connecting buyers and sellers of sensitive data, making it easy for them to find each other, negotiate the terms, and conduct the transaction. Forrester discusses the marketplace for insider information and how security and risk leaders can protect your sensitive data. See the Forrester report "How Insiders Use The Dark Web To Sell Your Data."

[17] Data security and privacy is critical to firms' ability to win, serve, and retain their customers. To protect sensitive data, meet compliance, and continue to mature their practices for data security and privacy, companies are evaluating and adopting a range of contributing technologies. This Forrester Tech Tide™ report presents an analysis of the maturity and business value of 20 key technology categories that support data security and privacy. Security and risk professionals should read this report to shape their firm's investment approach to these technologies. See the Forrester report "The Forrester Tech Tide™: Data Security And Privacy, Q3 2019."

[18] Data security is a key pillar of Zero Trust. This report highlights key categories of tools and controls for data security and intersections with technologies that support the ecosystem of adjacent pillars of Zero Trust: workloads, networks, devices, and people. Figure 6 includes questions to help identify gaps in data security controls and processes. For more information, see the Forrester report "The Zero Trust eXtended Ecosystem: Data."

[19] In our 25-criterion evaluation of data security portfolio providers, we identified the 13 most significant ones — Dell, Digital Guardian, Forcepoint, Google, GTB Technologies, IBM, Imperva, McAfee, Micro Focus, Microsoft, Oracle, Symantec, and Varonis — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals understand the respective strengths of each vendor's portfolio. For more information, see the Forrester report "The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019."

[20] For more information, see the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.