

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

Vision: The Data Security And Privacy Playbook

by Heidi Shey and Enza Iannopolo

October 25, 2017

Why Read This Report

Data is the lifeblood of today's digital businesses; protecting it from theft, misuse, and abuse is the top responsibility of every security and privacy leader. Hacked customer data can erase millions in profits, stolen IP can destroy competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and regulatory fines while damaging reputations. Security and privacy pros must ensure security travels with the data across the business ecosystem; position data security and privacy as competitive differentiators; and build a new kind of customer relationship.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

Data Security And Privacy Is A Competitive Differentiator In A Data-Driven World

The promise of big data and digital businesses has just started to be realized. With this promise, data security and privacy is emerging as a competitive differentiator. Take the necessary steps to prepare for the digital revolution today.

As The Business Becomes Digital, Security Must Become Data-Centric

Security leaders of enterprises undergoing a digital transformation will soon realize that to adequately ensure customer protection and enable a digital workforce, they must abandon traditional perimeter-based security and put the focus on the data with a Zero Trust security architecture.

Forrester's Data Security And Control Framework Builds Your Strategic Approach

Forrester has created a framework to help security and privacy leaders embark on the data security journey. Forrester's data security and control framework breaks down the problem 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.

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

Vision: The Data Security And Privacy Playbook

by [Heidi Shey](#) and [Enza Iannopolo](#)

with [Stephanie Balaouras](#), Bill Barringham, Elsa Pikulik, and Peggy Dostie

October 25, 2017

Table Of Contents

- 2 Data Security And Privacy Is A Source Of Growth And Differentiation
- 3 Perimeter-Based Security Can't Provide Security Or Protect Privacy
- 4 Apply A Zero Trust Lens To Data Security And Privacy

Use Forrester's Data Security And Control Framework As Your Detailed Guide

Defining The Data Simplifies Its Control

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

Defending Data Protects It From The Vast Array Of Modern Threats

Recommendations

- 9 Don't Shy Away From Data Security And Privacy; Embrace It

Related Research Documents

[Rethinking Data Discovery And Classification Strategies](#)

[TechRadar™: Data Security And Privacy, Q4 2017](#)



Share reports with colleagues.
[Enhance your membership with Research Share.](#)

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

Vision: The Data Security And Privacy Playbook

Data Security And Privacy Is A Source Of Growth And Differentiation

Most security and privacy pros still explain the value of data security to the business only in terms of risk reduction, cost reduction, and regulatory compliance (at the lowest possible cost, of course). The problem with this narrative is that it fails to connect to the single most important goal of most companies — driving revenue and growth. However, at a time when the biggest source of competitive differentiation comes from how businesses exploit data and digital technologies to create new value for customers, increase their operational agility to serve customers, and form digital ecosystems that generate entirely new revenue streams, data security and privacy is so much more than cost reduction.¹ It is, in fact, a driver of revenue and growth. Today, robust security and privacy strategies, processes, and protections serve to:

- › **Build trusted customer relationships that drive loyalty and retention.** Firms must give customers assurance and an additional reason to do business — and continue doing business — with them. It's why technology giants like Apple and Microsoft have been willing to fight very public and contentious legal battles to protect customers' privacy.² The Electronic Frontier Foundation (EFF) also publishes an annual "Who Has Your Back" report to highlight the positions of major technology companies when it comes to handing data to the government.³ Yet security and privacy pros must also recognize that this is not limited to technology companies; you are a data business today, no matter what industry your organization is in.
- › **Elevate data security and privacy as a corporate social responsibility (CSR).** Behind every compromised customer record is a person who must deal with the negative consequences. This makes data protection an ethical and moral imperative. In 2014, Forrester found 47% of CSR reports we reviewed contained information about security controls to enforce protection and fair use of personal data, intellectual property, and other sensitive information — a 50% increase from 2007.⁴ This includes companies such as Nestle, BMW, and IBM. More and more companies are also embracing privacy as their CSR. We found that 22% of the companies appearing on the Global Fortune 100 list in 2017, from Italian electricity provider Enel to GE to Japanese Nippon Telegraph and Telephone, explicitly reference privacy in their CSR reports.
- › **Capitalize on risk.** From workforce mobility, to the growing interest in the internet of things, to big data analytics, firms have plenty of ways to carve out new opportunities to help drive growth. All come with varying levels of security, privacy, and ethical risks that you must address — from data collection to appropriate use, data access, and more. Security and privacy pros must help manage and mitigate the risks.⁵
- › **Protect future revenue streams.** Research and development efforts, corporate secrets, and intellectual property can hold the key to future growth and direction for the company. Security and privacy pros must safeguard this data against cyberespionage, theft, and careless compromise. The FBI estimates that economic espionage costs US businesses billions of dollars each year.⁶

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

Vision: The Data Security And Privacy Playbook

- › **Use the EU General Data Protection Regulation (GDPR) to grab broad attention.** With the EU GDPR coming into effect in a few months, almost every firm globally must set up their compliance strategy. But our data shows that only little more than half will be ready on time. With fines as high as 4% of global revenues and customers' demand for privacy on the rise, security and privacy pros cannot risk being unprepared. On the contrary, they should take this opportunity to improve their data handling practices and open the board's eyes on the role that privacy and security plays on company reputation, share values, and customer engagement. In the words of a risk officer at a large US bank: "I made GDPR my Trojan horse into the board."

Perimeter-Based Security Can't Provide Security Or Protect Privacy

When they're trying to protect their firm's customer data and IP, security and privacy leaders of enterprises undergoing a digital transformation will soon realize that their perimeter-based approach to security is completely inadequate. In a digital business, processes are rarely, if ever, self-contained within the infrastructure confines of the company. Customers engage with us across numerous digital channels; our business applications live in our data centers and in the cloud; and we have dozens of third-party relationships critical to our operations. This exposes a fatal flaw in the main assumption underpinning perimeter-based security — that there is a "trusted" internal network where data is safe and an "untrusted" external network where data is unsafe. This implicit trust assumption is both incredibly naive and untenable in a digital enterprise because it:

- › **Can't protect customer data and IP from insider theft and abuse.** You must protect customers' data not only from cybercriminals but also from individuals operating inside the "trusted" network: malicious insiders cooperating with cybercriminals or driven by other motivations, whether political, social, or retaliatory; unwitting employees who accidentally leak sensitive data through email, file sharing, social networks, and other channels; and even well-intentioned employees who unintentionally violate privacy laws while processing and using customer data. In a 2017 Forrester survey, 54% of North American and European network security decision makers at firms with 20 or more employees that had a security breach in the past 12 months said that at least one breach was an internal incident within their organization.⁷
- › **Can't protect your customer data from third-party privacy abuses.** Attackers can compromise your business partners, contractors, and other third parties that have access to your data.⁸ These third parties may also have legitimate access to the data for business purposes but misuse the data or undermine their regulatory obligations. GDPR, for example, makes it a priority to mitigate third-party risks, requiring organizations to gain an unprecedented level of visibility into third-party data handling practices. Alternatively, governments may request access to customer data for purposes of surveillance.⁹
- › **Can't protect your customer data in new engagement models.** From efforts to personalize advertising, products, and services to create a better customer experience to exploring beacons and video surveillance as a means of segmenting customers, security and privacy pros must be

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

Vision: The Data Security And Privacy Playbook

vigilant in tackling the data security and privacy risks and concerns that inevitably emerge with the collection and use of personal and sensitive data. In these new engagement models, customer data is sourced from a variety of places — direct from the consumer as well as from sensors and devices — and analyzed outside your corporate network.

› **Fails to empower a digital workforce to better serve customers while protecting data.**

According to a 2016 Forrester Data survey, 37% of global information workers access information for work on a tablet or smartphone.¹⁰ It's now far less important to focus on protecting individual devices that the organization no longer owns or attempt to lock down the devices that connect to the network — and far more important to protect the organization's sensitive data regardless of device type, app, or location.

- › **Doesn't securely integrate partners and suppliers into business operations.** Something as simple as onboarding a new customer and fulfilling an order could potentially include the services of a global payment processor; your own eCommerce, CRM, and ERP platforms (hosted in the cloud or on-premises); and warehouse and other logistics partners that deliver your products. These partners often need access to your network or specific data to do their jobs, but too much access can lead to gaping holes in security. Some 39% of respondents whose firms were breached in the past 12 months indicated that they had at least one breach involving business partners/third-party suppliers.¹¹

Apply A Zero Trust Lens To Data Security And Privacy

Forrester's Zero Trust Model of information security states that security and privacy pros must eliminate the idea of a trusted internal network and an untrusted external network. Three concepts underpin Zero Trust. Security and privacy pros must: 1) verify and secure all resources regardless of location; 2) limit and strictly enforce access control across all user populations, devices/channels, and hosting models; and 3) log and inspect all traffic, both internal and external.¹² To accomplish this, security and privacy pros need to:

- › **Never take data security and privacy for granted.** A Zero Trust approach: 1) never assumes trust — “trust” is continuously assessed through a risk-based analysis of all available information; 2) fundamentally shifts the focus from the perimeter to the data itself; and 3) makes security architecture and operations workload-first, data-driven, and identity-aware rather than static and perimeter-centric (see Figure 1).
- › **Take a data-centric approach.** Gain visibility into the interaction between users, apps, and data across a multitude of devices and the ability to set and enforce one set of policies irrespective of whether the user is connected to the corporate network. This data-centric approach to security is supported by integrated security functions and consolidated controls that form a security ecosystem (see Figure 2). Data centrality requires data control and intelligence (see Figure 3).

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

Vision: The Data Security And Privacy Playbook

FIGURE 1 The Three Fundamental Components Of Zero Trust In Digital Transformation

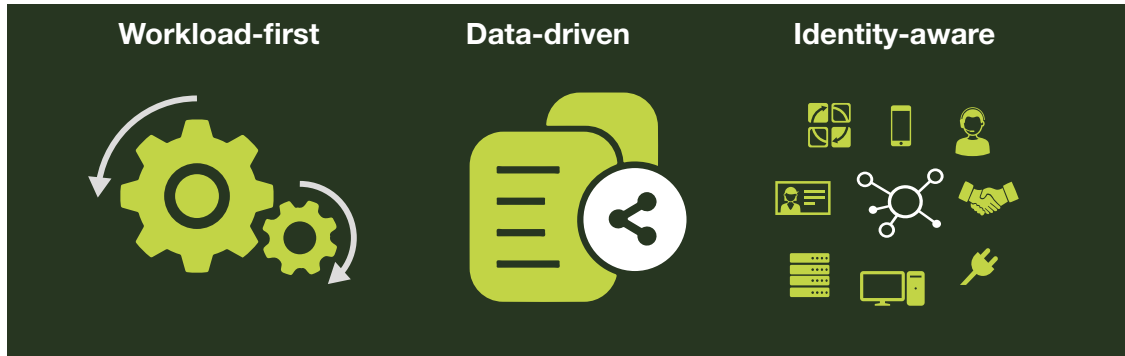
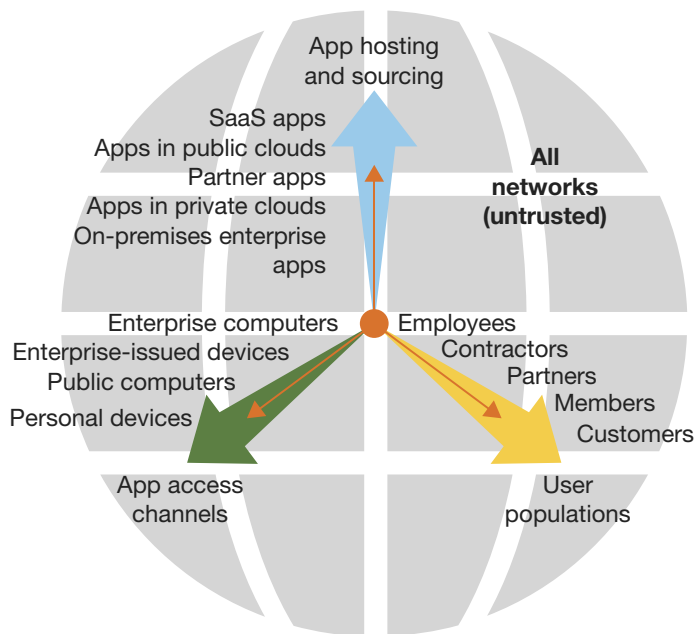


FIGURE 2 A Zero Trust Approach To Data Security In A Perimeterless World





- Continuously assess “trust” (don’t assume) through a risk-based analysis of all available information.
- Gain visibility into the interaction between users, apps, and data.
- Set and enforce policies irrespective of whether the user is connected to the corporate network.
- Integrate security functions and consolidate controls.

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

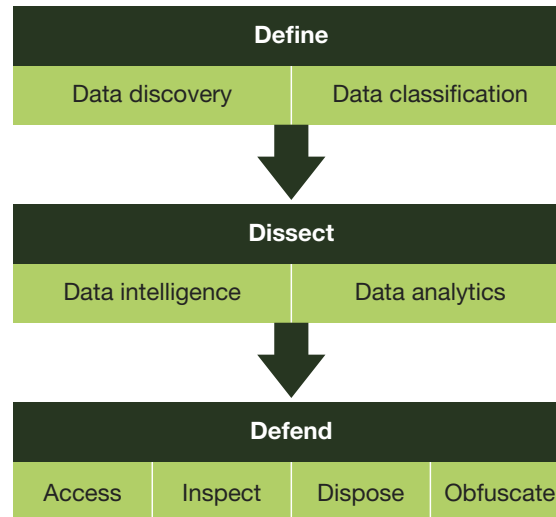
Vision: The Data Security And Privacy Playbook

FIGURE 3 A Data-Centric Approach Requires Capabilities For Data Control And Intelligence

	<p>Data control: ability to apply universal security policies to protect data regardless of location, device type, hosting model, or user population</p>	Inventory and classify data
		Encrypt data in-flight-to and at-rest
		Enforce access control
		Apply and enforce declarative policy dynamically via APIs
	<p>Intelligence: real-time analysis and visibility with contextual information to identify threats, address vulnerabilities, and uncover incidents in progress</p>	Gain visibility across networks, devices, apps, users, and data
		Augment analysis with contextual information about the user, transaction risk, overall security state (traffic flows, device state, user identity, user behavior, app state, app classification, data classification, location, time, etc.)

Use Forrester’s Data Security And Control Framework As Your Detailed Guide

It has never been more important to bring together separate silos of data control and security such as archiving, data loss prevention (DLP), and access management and move them closer to the data itself, instead of at the edges (perimeters) of networks. In organizations that are complex or that have huge amounts of data, security and privacy pros often don’t know where to start. Forrester has created a framework to help security and privacy pros embark on this journey. We break down the problem 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 4).

FIGURE 4 Forrester's Data Security And Control Framework

Defining The Data Simplifies Its Control

Today, enterprises don't talk about terabytes of data; they talk about petabytes, even exabytes, of data. Few enterprises have proper data governance in place; as a result, they have data strewn across global data centers, computer rooms, remote offices, laptops, desktops, mobile devices, and cloud storage. 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. Therefore, security pros, together with their counterparts in legal and privacy, should define data classification levels based on data value and risk.¹³ This allows security pros to properly protect data based on its classification once they know where that data is located in the enterprise. Discovery and classification are critical because:

- › **Data discovery locates and indexes data.** To protect data, you must first know where users have stored it. Unfortunately, data has proliferated throughout the enterprise and can be difficult to discover. 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.¹⁴ Without strong policies in place regarding data handling, storage, and retention, users can store sensitive information on laptops and even mobile devices that are often outside the control of security teams. Security professionals, together with legal and privacy teams, must undertake a data discovery project to locate and index existing data and develop a life-cycle approach that continuously discovers data as users create it throughout the extended enterprise network.

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

Vision: The Data Security And Privacy Playbook

- › **Data classification tags data to make it easier to control and use.**¹⁵ Each data chunk must contain information that lets various users and tools understand value of that data in order to better understand how to properly handle and use it. Data classification can be an arduous process, and organizations will try to skip this step. Don't let your organization do that — proper data defense depends on accurate classification. Effective classification can indicate whether you must archive the data for regulatory compliance purposes (e.g., to comply with SOX or SEC Rule 17a-4) or whether it's subject to a regulation such as the Payment Card Industry Data Security Standard (PCI DSS) or EU GDPR.

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

Data classification is not a one-time event; security and privacy pros must continuously reassess classification as conditions change. In addition to data classification, security and privacy pros also need continuous visibility into the changing threats to the data as well as information about data use. Specifically:

- › **Data intelligence provides business and other contextual insights about data.** The classification of data (e.g., individual files, emails, database fields, etc.) can change as the value of the data changes over time.¹⁶ The business value of the data drives security strategy and granular policy. For example, for the most sensitive data, the security team can deploy solutions that will automatically stop exfiltration — without human intervention.¹⁷ In addition to changing classification, it's important to understand the current state of data. Has someone compromised its integrity? Is exfiltration in process? How does this data normally flow; how should it flow?
- › **Security data analytics identifies changing threats and guides decision making.** The promise of analytics married with big data processing includes the ability to analyze more and more data in near real time. Security and privacy pros can use this insight to more proactively protect valuable sensitive data, prioritize security initiatives, and more effectively place the proper security controls. 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. By linking and analyzing security data from sources like security information management (SIM), network analysis and visibility (NAV), security user behavior analysis (SUBA), DLP, and other security tools, security and privacy pros will be able to determine the state of their network and data movement in near real time, thereby detecting potential breaches or insider abuse much more quickly.

Defending Data Protects It From The Vast Array Of Modern Threats

As the number of attacks increases and their sophistication improves, it's clear that security and privacy professionals must do a better job of defending data. Forrester's data security and control framework provides basic ways to defend and protect data:

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

Vision: The Data Security And Privacy Playbook

- › **Access control ensures the right user gets access to the right data at the right time.** One of the tenets of Forrester's Zero Trust Model of information security is that you should limit access to all resources according to the principle of least privilege and strictly enforce this access control.¹⁸ To secure data throughout your ecosystem, strictly limit the number of people who can access data and continuously monitor those users' 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.¹⁹ Security and privacy pros also often don't have much insight into the access privileges of third-party users with whom data is shared.
- › **Inspecting data usage patterns can alert security teams to potential abuses.** It's impossible to protect against attacks you can't see. 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 SUBA or NAV 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.²⁰
- › **Disposing of data when it's no longer needed is a powerful defensive tactic.** 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.²¹ Resist the temptation to keep every byte of data just because you can.²² Securely and defensively disposing of data in accordance with your retention policies 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.
- › **Obfuscating data devalues it so that cybercriminals can't use or sell it.** Cybercriminals use underground markets on the internet to buy and sell sensitive data, such as credit card numbers, credit reports, and even intellectual property. This underground market operates according to the economic principles of supply and demand. If you can remove the value of data, you can eliminate incentives to steal it. You can devalue data using data abstraction and obfuscation techniques like encryption, tokenization, and masking.²³ Generally, 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

Don't Shy Away From Data Security And Privacy; Embrace It

While the costs of breach remediation and IP theft remain unacceptably high, the prevailing concern is the erosion of trust that can occur when customers lose confidence in an enterprise's commitment and ability to protect their privacy and personal data. Customers don't have to do business with you; they have to want to do business with you. If you begin to treat customer data like it was your own, you're on

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

Vision: The Data Security And Privacy Playbook

the right path, but you can go a step further. Your approach to data security and privacy doesn't have to be solely about cost avoidance and risk mitigation; depending on your firm and your industry, you can begin to position it as a competitive differentiator and growth driver. Security and privacy leaders must consider policy, people, and tools when establishing their data security and privacy approach.

Involve The Wider Organization In Setting Policy And Culture

As enterprises embark on digital transformation and as big data initiatives become more important, security and privacy leaders must work to create awareness and understanding of the associated responsibilities, risks, and opportunities at the highest levels of the organization. To prepare for the digital revolution, we recommend that security and privacy pros:

- › **Monitor changing privacy regulations for risks — and opportunities.** Involve your legal team here as well. Global privacy laws will continue to evolve and change, not just addressing what types of data constitute personal information but also providing restrictions on how your business can use, store, or transfer the data of a country's citizens.²⁴ At times, these regulations may be driven more by political pressures and used by governments as a means of creating trade barriers and exerting control over their domestic economy.
- › **Ensure a cross-functional team sets data security and privacy policy.** Do not create your policies in a vacuum. Involve a cross-functional team composed of technology management, customer care, marketing, legal, HR, finance, and leads of other major business units. Security and privacy pros can benefit from a better understanding of the concerns and objectives of representatives on this cross-functional team and thus better align security and privacy policies to business requirements. Team members will also be in the loop earlier on with policy creation and can help security and privacy pros champion these policies within their respective areas in the enterprise.
- › **Ask legal to define clear policies for data archiving and data disposal.** As data volumes grow into the petabytes, protecting sensitive information becomes an almost Herculean task for the security organization. Data security becomes more manageable and realistic when you reduce data volumes. Imagine that your organization no longer stores every terabyte of information it collects or generates but follows defensible disposal practices to archive information and then delete it when its value to the business declines or its retention policy expires.²⁵ In this scenario, discovering, dissecting, and defending your sensitive information is much easier.

Use Technology To Enforce The Control And Protection Of Your Data

While policy and behavior are important, security and privacy pros must also investigate technology solutions that will enforce and support data control and protection:

- › **Move your controls closer to the data itself.** Security and privacy pros apply most controls at the very edges of the network. However, if attackers penetrate your perimeter, they will have full and unrestricted access to your data. By placing controls as close as possible to the data store and the data itself, you can create a more effective line of defense.

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

Vision: The Data Security And Privacy Playbook

- › **Leverage existing technologies to control and protect data.** Most security organizations have already deployed numerous data security technologies, such as database activity monitoring and database encryption. As data volumes explode and data formats and types proliferate, vendors of these technologies will upgrade their products to deal with the vast array of unstructured data types and even new platforms specifically for big data environments.
- › **Look to new solutions for cloud visibility and data protection.** Gain visibility into the types of cloud services in use within the enterprise. Pull in features like encryption, anomaly detection, and cloud access governance with help from cloud security gateway vendors like Bitglass, Blue Coat/Symantec, CipherCloud, CloudLock/Cisco, Imperva, Microsoft, Netskope, and Skyhigh Networks.²⁶
- › **Control access to data resources, and watch user behavior while respecting privacy.** Every byte of data could contain information about people — customers, employees, and business partners. Privacy laws worldwide mandate that you protect their personal information and that no one deserves to have their finances and credit destroyed by a cybercriminal. Intellectual property, such as trademarks, formulas, and product designs, is the key to your organization's global competitive advantage. Your first line of defense is to limit data access to only those individuals whose job function requires it. It's no longer acceptable to allow unfettered data access to the vast majority of your employees, and you must monitor those with access for proper data access behavior — and respect employee privacy in the process.
- › **Always seek to control your encryption keys.** Bring your own encryption, or hold the keys to your kingdom. The Snowden/NSA leaks raised questions and concerns about government surveillance and access to data, sparking discussions between service providers and customers about the security and privacy of their data. For example, some file-sharing and collaboration solutions today offer customer-managed keys as an option.²⁷

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

Vision: The Data Security And Privacy Playbook

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

[Learn more.](#)

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

[Learn more.](#)

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

[Learn more.](#)



Forrester's research apps for iOS and Android.

Stay ahead of your competition no matter where you are.

Endnotes

¹ Businesses are drowning in data but starving for insights. Worse, they have no systematic way to consistently turn data into action. This can't continue. Demanding customers and competitive pressures require firms to treat insights — not just data — as a business asset. Forrester's research into incumbents like Ford Motor, General Electric (GE), and USAA as well as digital insurgents like Netflix and LinkedIn found that these leaders are fusing a new business discipline with technology to create "systems of insight." This combination of people, process, and technology closes the gap between insights and action. See the Forrester report "[Digital Insights Are The New Currency Of Business.](#)"

² Source: Lev Grossman, "Inside Apple CEO Tim Cook's Fight With the FBI," Time, March 17, 2016 (<http://time.com/4262480/tim-cook-apple-fbi-2/>).

Source: Jay Greene and Devlin Barrett, "Microsoft Sues Justice Department Over Secret Customer Data Searches," The Wall Street Journal, April 14, 2016 (<http://www.wsj.com/articles/microsoft-sues-justice-department-over-secret-customer-data-searches-1460649720>).

Source: Peter J. Henning, "Digital Privacy to Come Under Supreme Court's Scrutiny," The New York Times, July 10, 2017 (<https://www.nytimes.com/2017/07/10/business/dealbook/digital-privacy-supreme-court.html>).

³ Source: Rainey Reitman, "Who Has Your Back? Government Data Requests 2017," Electronic Frontier Foundation, July 10, 2017 (<https://www.eff.org/who-has-your-back-2017>).

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

Vision: The Data Security And Privacy Playbook

- ⁴ There are many reasons for companies to spend time and money to become more environmentally, socially, and economically responsible: They may save money by reducing resource requirements, they may gain access to more capital from socially conscious investors, and they may open doorways with foreign governments that prefer to see ethical companies do business with their constituents. Now, an increasingly critical driver among these others is customer expectation; business and consumer customers alike are demanding that companies they buy from demonstrate environmental, social, and financial responsibility. See the Forrester report "[Meet Customers' Demands For Corporate Responsibility.](#)"
- ⁵ Much of the data that companies process, store, and analyze could be sensitive and therefore subject to global laws and regulation. S&R pros must help oversee data-driven business initiatives and make calculated risks to create conditions for success. See the Forrester report "[Six Frameworks To Manage Your Big Data Privacy Concerns And Risks.](#)"
- ⁶ Source: "Economic Espionage," FBI, July 23, 2015 (<https://www.fbi.gov/audio-repository/news-podcasts-inside-economic-espionage.mp3/view>).
- ⁷ Respondents said the three most common ways in which breaches occurred in the past 12 months were: 1) an external attack targeting their organization (72%); 2) an internal incident within their organization (54%); and 3) an external attack targeting a business partner/third-party supplier (39%). See the Forrester report "[Understand The State Of Data Security And Privacy: 2016 To 2017.](#)" Source: Forrester Data Global Business Technographics® Security Survey, 2017.
- ⁸ Source: Iain Thomson, "14 MEEELLION Verizon subscribers' details leak from crappily configured AWS S3 data store," The Register, July 12, 2017 (https://www.theregister.co.uk/2017/07/12/14m_verizon_customers_details_out/).
- ⁹ The Freedom Act is compromise legislation that prohibits the government's bulk collection of metadata on US citizens but preserves surveillance in other forms. In this quick take, we provide S&R pros with an overview of the changes and how they will affect your data security and privacy policies. See the Forrester report "[Quick Take: The Patriot Act Is Dead. Long Live The Patriot Act.](#)"
- ¹⁰ Source: Forrester Data Global Business Technographics Devices And Security Workforce Survey, 2016.
- ¹¹ Source: Forrester Data Global Business Technographics Security Survey, 2017.
- ¹² S&R leaders should consider migrating to a Zero Trust security architecture as their organization develops hybrid cloud strategies as well as mandate digital transformation. See the Forrester report "[Future-Proof Your Digital Business With Zero Trust Security.](#)"
- ¹³ 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.](#)"
- ¹⁴ Data loss prevention (DLP) remains a key technology to help prevent the leakage and exfiltration of the firm's most sensitive data. Using client feedback, survey data, and input from security leaders in Forrester's Security & Risk Council, we looked at DLP with a different lens to address common pitfalls and implementation challenges. In this report, we help S&R pros assess the current state of their DLP efforts against data loss vectors and process maturity. See the Forrester report "[Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid.](#)"
- ¹⁵ Data classification facilitates defining and understanding data, identifying the way employees should handle it, and the security controls necessary. Forrester examined adoption, market trends, best practices for data classification, as well as defending the business case for these tools. See the Forrester report "[Market Overview: Data Classification For Security And Privacy.](#)"
- ¹⁶ Some data, such as acquisition plans or product road maps, can be highly confidential one day, and then outdated and unimportant the next.

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

Vision: The Data Security And Privacy Playbook

- ¹⁷ It seems that not a day goes by that there isn't another massive security breach in the news. Consumers around the globe hear about continual threats to their personal data while name brand retailers and enterprises are spending millions to respond, remediate, and recover from the theft of sensitive customer data and intellectual property. As the costs of data breaches skyrocket and regulators add more compliance burdens to the enterprise, the security industry must find new ways to more comprehensively meet these threats and prevent the exfiltration of proprietary data into the hands of cybercriminals and other malicious actors. See the Forrester report "[Rules Of Engagement: A Call To Action To Automate Breach Response.](#)"
- ¹⁸ S&R leaders should consider migrating to a Zero Trust security architecture as their organization develops hybrid cloud strategies as well as mandate digital transformation. See the Forrester report "[Future-Proof Your Digital Business With Zero Trust Security.](#)"
- ¹⁹ Protecting against a breach is difficult because you have an enormous amount of data to protect stored in many silos and growing at an alarming rate. Security professionals often turn to technologies such as data leak prevention (DLP) and enterprise rights management (ERM), but these don't perform well alone without an identity context. You need to have a full understanding of how users join, move, and leave the enterprise so that you can assign and revoke access to sensitive data assets. See the Forrester report "[Your Data Protection Strategy Will Fail Without Strong Identity Context.](#)"
- ²⁰ Forrester provides a definition of security analytics, discusses its benefits, and explains how S&R leaders should be using SA in their security program. See the Forrester report "[Counteract Cyberattacks With Security Analytics.](#)"
- Security analytics solutions help security teams with better visibility, improved detection, and enhances workflows. Forrester examined capabilities of SA solutions and give S&R pros an overview of key vendors. See the Forrester report "[Vendor Landscape: Security Analytics \(SA\).](#)"
- Forrester analyzed the most significant security analytics providers to help S&R risk professionals make the right choice. See the Forrester report "[The Forrester Wave™: Security Analytics Platforms, Q1 2017.](#)"
- ²¹ Many enterprises report significant eDiscovery 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.](#)"
- ²² 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.
- ²³ As data volumes explode, it's becoming a Herculean task to protect sensitive data from cybercriminals and malicious actors while preventing privacy infringements and abuses — intentional and unintentional. Every day, vendors introduce a new product or service that claims to be the cure-all to data security challenges. This TechRadar assesses 21 of the key traditional and emerging data security technologies that S&R leaders and their staff can use to underpin the best practices and recommendations of our framework. See the Forrester report "[TechRadar™: Data Security, Q1 2016.](#)"
- ²⁴ There is a complex landscape of data privacy laws around the world. See the Forrester report "[Forrester's 2017 Interactive Data Privacy Heat Map.](#)"
- ²⁵ This assumes that the information in question isn't subject to eDiscovery or investigative preservation obligations.
- ²⁶ Forrester analyzed the most significant cloud security gateway (CSG) providers to help security and risk professionals make the right choice. See the Forrester report "[The Forrester Wave™: Cloud Security Gateways, Q4 2016.](#)"
- ²⁷ There has been so much excitement for bring-your-own-encryption (BYOE) solutions — solutions that enable S&R pros to retain control of their encryption keys and, thus, retain control of the security state of their data, regardless of its storage location. To date, BYOE solutions have come primarily from startups and data security specialists, but in the coming days and weeks, many cloud vendors will offer their own functionality for customer-managed encryption keys. This quick take provides a primer on customer-managed encryption keys for the S&R pro as well as outlining implications for the security market. See the Forrester report "[Quick Take: Use 'Customer-Managed Keys' To Regain Control Of Your Data.](#)"

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.