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

Vision: The Data Security And Privacy Playbook

by John Kindervag, Heidi Shey, and Kelley Mak

July 7, 2016

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 S&R leader. Hacked customer data can erase millions in profits, stolen IP can destroy competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while damaging reputations. S&R pros must take a data-centric approach that ensures security travels with the data regardless of user population, location, or even hosting model; position data security and privacy capabilities 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

S&R 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 by embracing Forrester's Zero Trust Model.

Forrester's Data Security And Control Framework Puts Security Closer To The Data

Forrester has created a framework to help S&R professionals 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 John Kindervag, Heidi Shey, and Kelley Mak
with Stephanie Balaouras, Alexander Spiliotes, and Peggy Dostie

July 7, 2016

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and industry experts.

Related Research Documents

Rethinking Data Discovery And Data Classification Strategies

TechRadar™: Data Security, Q1 2016

Understand The State Of Data Security And Privacy: 2015 To 2016

FORRESTER®

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

Data Security And Privacy Is A Source Of Growth And Differentiation

Most S&R 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 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.** The relentless parade of data breaches and privacy violations has cast a shadow on this relationship in recent years. Firms must give customers assurance and an additional reason to do business — and continue doing business — with them. This is why financial services firms like Wells Fargo specifically call out their security efforts in marketing and customer outreach.[2] It's also why technology giants like Apple and Microsoft have been willing to fight very public and contentious legal battles to protect customers' privacy.[3]
- **Elevate data security and privacy as a corporate social responsibility (CSR).** Behind every stolen customer record is a person who must deal with the negative consequences. This makes data protection an ethical and moral imperative. More and more companies are adding privacy as a CSR, from Nestle to BMW to IBM. 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]
- **Enable premium pricing for your products or offer dedicated privacy products.** There are explicit and implicit premiums. For example, AT&T is explicitly charging users $29 a month to opt out of online activity tracking for targeted ads.[5] Others like Silent Circle have an implicit premium attached, where privacy is the value proposition for its Blackphone handset. There is a growing market for solutions that enable consumers to protect their online privacy, like AVG Technologies' Safe Surf and Abine's Blur.[6]
- **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 risk that you must address — from data collection to appropriate use, data access, and more. S&R pros must help manage and mitigate the risks.
- **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. S&R 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.[7]

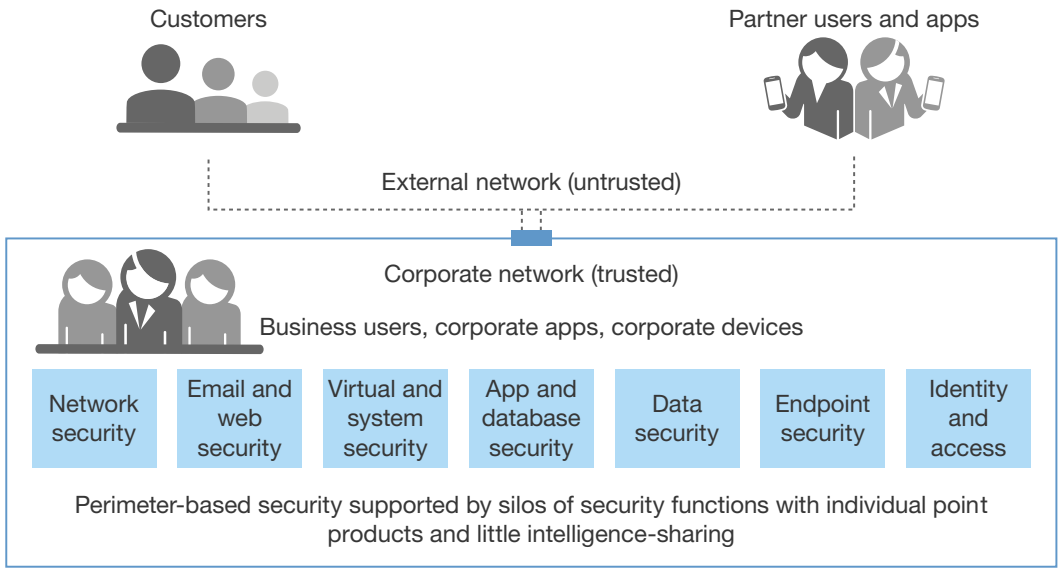
Perimeter-Based Security Can't Provide Security Or Protect Privacy

When they're trying to protect their firm's customer data and IP, S&R 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 (see Figure 1). 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. Based on Forrester's 2015 data, 39% of North American and European business and technology decision-makers at firms with 20 or more employees that had a security breach in the past 12 months said that internal incidents within their organization were one of the most common ways in which the breaches occurred.[8]
- **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. These third parties may also have legitimate access to the data for business purposes but misuse the data. Alternatively, governments may also 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, S&R pros must be 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 Forrester's Global Business Technographics® Devices And Security Workforce Survey, 2015, 21% of global information workers access at least one of seven types of information for work (customer data, employee data, etc.) on a tablet, smartphone, or other device (not including desktop/laptop).[10] It's now far less important to focus on protecting individual devices that the organization no longer owns or attempting 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. Our survey data shows that 19% of breached firms report incidents with business partners/third-party suppliers as among their most common causes of breaches.[11]

FIGURE 1 Yesterday's Traditional Perimeter-Based Security



Source: "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem" Forrester report

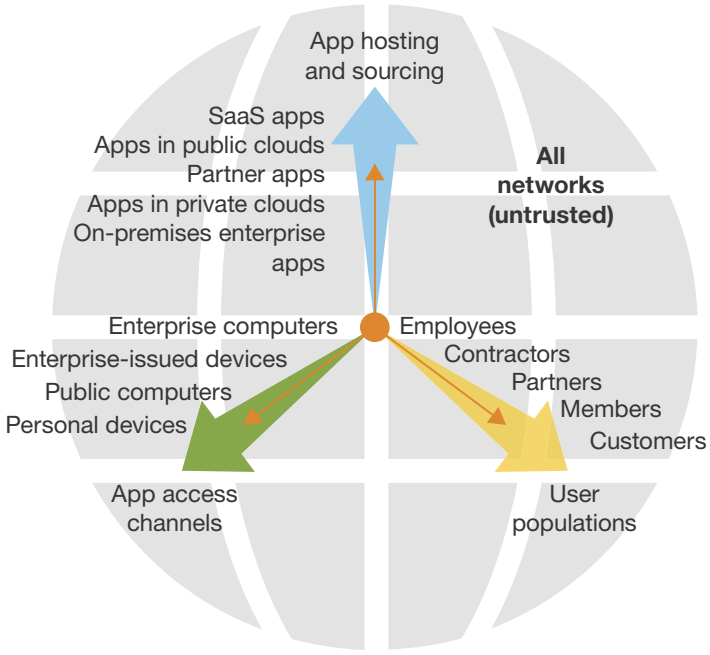
S&R Pros Must Apply A Zero Trust Lens To Data Security And Privacy

Forrester's Zero Trust Model of information security states that S&R pros must eliminate the idea of a trusted internal network and an untrusted external network. Three concepts underpin Zero Trust. S&R 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. To accomplish this, S&R pros need 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 (see Figure 2). Unlike legacy, perimeter-based approaches to security, Zero Trust:

› **Never takes data security and privacy for granted.** A Zero Trust approach: 1) never assumes trust — "trust" is continuously assessed though a risk-based analysis of all available information; 2) fundamentally shifts the focus from the perimeter to the data itself; and 3) marshals the functions of many security domains, such as network, identity, and application security, in a unified approach to data protection.

› **Accelerates digital business initiatives.** Zero Trust is a fundamental rethinking of corporate security from a failed, perimeter-centric approach to a data and identity-centric approach so that your business can improve the customer experience, adopt new systems of engagement, and develop a complex digital ecosystem. Imagine the old way of doing security as an imposing castle and the Zero Trust way of doing security as a modern city that encourages commerce to flourish but still provides security with oversight and specific protections. Better yet, imagine this city attracting more business precisely because of the security and privacy it affords its citizens and businesses.

FIGURE 2 A Zero Trust Approach To Data Security



Data-centric security supported by integrated security functions and consolidated controls that form a security ecosystem

Data control — the ability to apply universal security policies to protect sensitive data regardless of location, device type, hosting model, or user population. This requires the ability to:

- Inventory and classify data across networks, devices, and apps.
- Encrypt data in-flight-to and at-rest in any application, device, or network regardless of location.
- Enforce access control across user populations, apps, and devices.
- Apply and enforce declarative policy dynamically via APIs.

Intelligence — combining real-time analysis and visibility with contextual information to identify threats, address vulnerabilities, and uncover incidents in progress. This requires:

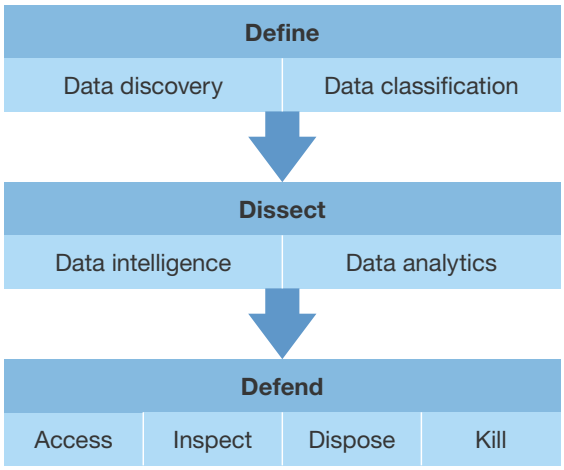
- Real-time analysis and visibility across networks, devices, apps, user, and data.
- Contextual information about the user, transaction risk, and overall security state such as traffic flows, device state, user identity and biometrics, behavior, app state, app classification, data classification, location, and time.

Source: "Transform Your Security Architecture And Operations For The Zero Trust Ecosystem" Forrester report

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, 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, S&R pros often don't know where to start. Forrester has created a framework to help S&R 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 3).

FIGURE 3 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. Companies generate data every day, and in many cases, they're amassing vast amounts of data in big data stores. 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. Therefore, S&R professionals, together with their counterparts in legal and privacy, should define data classification levels based on toxicity.[12] This allows S&R 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 — especially toxic 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 the DLP technology.[13] Without strong policies in place regarding data handling, storage, and records management, users can store sensitive information on laptops and even mobile devices that are often outside the control of security teams. S&R 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.

› **Data classification catalogs data to make it easier to control.** S&R pros can't properly protect data until it has been classified. Each data chunk must contain information that lets various users and tools understand the level of toxicity implicit in that data. 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). PCI mandates that security professionals protect cardholder data according to strict guidelines.[14]

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

Data classification is not a one-time event; S&R pros must continuously reassess classification as conditions change. In addition to data classification, S&R pros also need continuous visibility into the changing threats to the data. Look for security information management (SIM) and network analysis and visibility (NAV) solutions to intersect with big data to enhance security decision-making:

› **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. Some data, such as acquisition plans or product road maps, can be toxic one day and unimportant the next. Classifications can also change because of changes in regulations. 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.[15] In addition to changing classification, it's important to understand the current state of data. Has someone compromised its integrity? Is an exfiltration in process? How does data normally flow through the firm? For example, by linking SIM and NAV data, S&R pros will be able to determine the state of their network in near real time, thereby finding potential breaches or insider abuse much more quickly.

› **Data analytics identifies changing threats to data and guides decision-making.** S&R pros must do a much better job of anticipating threats to their industry and enterprise, targeting efforts where it matters most, and limiting the damage of breaches that have already occurred. The promise of analytics married with big data processing includes the ability to analyze more and more data in near real time. S&R pros can use this insight to more proactively protect toxic 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.

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 S&R professionals must do a better job of defending data. Forrester's data security and control framework provides basic ways to defend and protect data:

- **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.[16] 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. S&R 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.[17] Even more alarming, S&R pros often don't have much insight into the access privileges of third-party users with whom data is shared.[18]
- **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 NAV tools such as metadata analysis, packet capture analysis, or flow analysis tools and integrating them with your SIM solution to give you the unparalleled network visibility you need to proactively protect toxic data.[19]
- **Disposing of data when it's no longer needed is a powerful defensive tactic.** 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. With proper classification and supporting controls, you can defensively dispose of any toxic data no longer required by real business interests, compliance mandates, or data preservation obligations for investigations or litigation.[20] Resist the temptation to keep every byte of data just because you can. 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.
- **"Killing" data devalues it so that cybercriminals can't use or sell it.** Cybercriminals use underground markets on the internet to buy and sell toxic 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 or "kill" data using data abstraction techniques like

encryption, tokenization, and masking.[21] Generally, cybercriminals can't easily decrypt or recover data that you've encrypted or otherwise abstracted — 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 cost 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 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. S&R 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, S&R 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 S&R 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. 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. S&R 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 S&R 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.[22] 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, S&R pros must also investigate technology solutions that will enforce and support data control and protection:

- **Move your controls closer to the data itself.** S&R 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.
- **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 data protection vendors like Actifio, BetterCloud, Blue Coat Systems (Perspecsys), CipherCloud, CipherPoint, CloudLock, Digital Guardian, EMC (CloudLink), Imperva (Skyfence), HPE (Voltage Security), Microsoft (Adallom), nCrypted Cloud, SkyHigh Networks, Sookasa, Trend Micro, and Vaultive.[23]
- **Diligently control access to data resources, and watch user behavior.** 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.
- **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.[24]

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

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

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 "Digital Insights Are The New Currency Of Business" Forrester report.

[2] Source: "Wells Fargo — A History of Protection," YouTube video, May 2, 2016 (https://www.youtube.com/watch?v=tqLmajvFLmI).

[3] 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).

[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 "Meet Customers' Demands For Corporate Responsibility" Forrester report.

[5] Source: Mark Hachman, "You'll pay more for privacy with AT&T's gigabit broadband," PCWorld, February 17, 2015 (http://www.pcworld.com/article/2885163/youll-pay-more-for-privacy-with-atandts-gigabit-broadband.html).

Source: Troy Wolverton, "FCC Rules Would Boost Web Privacy," NewsFactor, June 7, 2016 (http://www.newsfactor.com/news/FCC-Rules-Would-Boost-Web-Privacy/story.xhtml?story_id=01300170RGQN#).

[6] Source: AVG (http://www.avg.com/us-en/home-small-office-security#all-tab) and Abine (https://www.abine.com/index.html).

[7] Source: "Economic Espionage," FBI (https://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage).

[8] In Forrester's Global Business Technographics Security Survey, 2015, respondents said the top three most common ways in which breaches occurred in the past 12 months were: 1) internal incident within their organization (39%); 2) external attack targeting their organization (27%); and 3) external attack targeting a business partner/third-party supplier (22%). See the "Understand The State Of Data Security And Privacy: 2015 To 2016" Forrester report.

[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 "Quick Take: The Patriot Act Is Dead. Long Live The Patriot Act" Forrester report.

[10] Source: Forrester's Global Business Technographics Devices And Security Workforce Survey, 2015.

[11] Source: Forrester's Global Business Technographics Security Survey, 2015.

[12] Defining data via data discovery and classification is an often overlooked, but critical, component of data security and privacy. Security and risk (S&R) pros can't expect to adequately protect data if they don't have knowledge about what data exists, where it resides, how valuable it is to the firm, and who can use it. In this report, we help S&R pros rethink overly complex and haphazard legacy approaches to discovery and classification. With the right approach, S&R pros can craft policies and deploy the right mix of controls that will protect customer data and the firm's intellectual property. See the "Rethinking Data Discovery And Data Classification Strategies" Forrester report.

[13] 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 "Rethinking Data Loss Prevention With Forrester's DLP Maturity Grid" Forrester report.

[14] PCI is controversial and is here to stay. It's time to move beyond complaining and embrace PCI to extract value. For more information on PCI guidelines, see the "PCI Unleashed" Forrester report.

[15] 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 "Rules Of Engagement: A Call To Action To Automate Breach Response" Forrester report.

[16] There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For today's digital business, this perimeter-based security model is ineffective against malicious insiders and targeted attacks. Security and risk (S&R) pros must eliminate the soft chewy center and make security ubiquitous throughout the digital business ecosystem — not just at the perimeter. In 2009, we developed a new information security model, called the Zero Trust Model, which has gained widespread acceptance and adoption. This report explains the vision and key concepts of the model. See the "No More Chewy Centers: The Zero Trust Model Of Information Security" Forrester report.

[17] 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 "Your Data Protection Strategy Will Fail Without Strong Identity Context" Forrester report.

[18] Human error, in addition to data security policy and data handling process failures, is a common cause of data breach and security incidents. In 2015, out of 1,309 publicly reported cyberevents, 321 were caused by a data governance or collection failure, representing 25% of incidents overall. As employees engage in collaboration and file sharing, do so from various device types, or seek to sync files across devices for easy access on the go, they also risk losing or exposing information. See the "Market Trends: Secure File Sharing And Collaboration In The Enterprise, Q1 2014" Forrester report.

CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure, as of June 15, 2016. Source: CyberFactors (http://cyberfactors.com/).

[19] Forrester's Zero Trust Model of information security demands that organizations know what types of activities take place on their internal network as well as their external network. To provide this type of deep insight into internal and external networks, Forrester has defined a functional space called network analysis and visibility (NAV). See the "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" Forrester report.

[20] 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 "Q&A: eDiscovery Fundamentals For Content & Collaboration Professionals" Forrester report.

[21] 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 "TechRadar™: Data Security, Q1 2016" Forrester report.

[22] This assumes that the information in question isn't subject to eDiscovery or investigative preservation obligations.

[23] To support their firms' cloud strategy without compromising security or compliance, security and risk (S&R) pros need to develop a number of important capabilities. They need the capability to: 1) discover sanctioned and unsanctioned cloud app adoption; 2) prevent the unauthorized transfer of sensitive data to the cloud; 3) protect and encrypt sensitive data in the cloud; and 4) identify suspicious employee behaviors and threats in cloud services. This report examines the vendor landscape for cloud access security intelligence (CASI) solutions that provide some or all of these capabilities. See the "Vendor Landscape: Cloud Access Security Intelligence (CASI) Solutions" Forrester report.

[24] 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 "Quick Take: Use 'Customer-Managed Keys' To Regain Control Of Your Data" Forrester report.

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.