A Forrester Consulting
Thought Leadership Paper
Commissioned By Varonis

January 2017

The Data Security Money Pit

Expense In Depth Hinders Maturity

FORRESTER®

Table Of Contents

Executive Summary 1

Expense In Depth Creates A False Sense Of Data Security Maturity 2

Companies Struggle With Disparate Data Security Products 2

A Strong Data Strategy Requires A Unified Data Security Platform 4

Key Recommendations 6

Appendix A: Methodology 7

Appendix B: Supplemental Material 7

Appendix C: Endnotes 7

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Project Director: Andia Vokshi, Market Impact Consultant
Contributing Research: Forrester's Security and Risk research group

FORRESTER®

Executive Summary

What is the value of data security? Most companies define this value in terms of risk, cost, and regulatory compliance. "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. It is, in fact, a driver of revenue and growth."[1]

Organizations today are aggregating many parts of security into platforms to improve manageability, streamline processes, lower costs, and simplify reporting. However, data security is one area that is still fragmented.

In September 2016, Varonis commissioned Forrester Consulting to evaluate the need for a data security platform. Then to further explore this trend, Forrester developed a hypothesis that tested the assertion that in order to have a strong, secure network, organizations need a data strategy that aggregates data security into a single platform and combines data classification, analytics, and reporting in one place.

In conducting in-depth surveys with 150 data security decision-makers, Forrester found that changing strategies from a product to a platform will transform data security for companies. In fact, data security decision-makers expect to improve their ability to respond to breaches, reduce costs of legacy solutions, reduce exposure from a breach, and lower complexity.

A strong, secure network requires a data strategy that aggregates data security into a single platform and combines classification, analytics, and reporting in one place.

KEY FINDINGS

Forrester's study yielded three key findings:

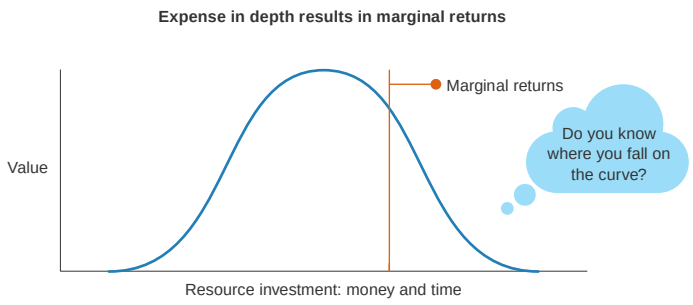
- **Investing in data security products does not translate to maturity.** Most organizations have implemented a variety of technology solutions to help with data security. But a high security investment does not translate to high maturity with data security, nor does it mean a unified security strategy.
- **Low maturity with data security manifests itself through challenges.** Despite claims of high maturity, an overwhelming majority of companies face technical and organizational challenges with data security, are focused on threats rather than their data, and do not have a good handle on understanding and controlling sensitive data.
- **There is an appetite for a unified data security platform.** A unified data security platform will improve data strategy by helping to provide the data visibility and governance that firms desire, while controlling costs and addressing integration concerns.

Expense In Depth Creates A False Sense Of Data Security Maturity

Digital business mandates personalization in order to win, serve, and retain customers. In this effort, companies collect all the customer data they can get their hands on, ranging from personally identifiable information to cardholder information. But a successful digital business goes beyond collecting customer data; it requires a robust and unified data security strategy to derive insights and protect that data.[2] In fact, over 40% of data security decision-makers reported that customers or partners are demanding that their data is protected.

Companies have responded: They have invested widely in data security tools to help manage risk and meet compliance requirements, implementing technology for encryption, monitoring, analytics, classification, and collaboration. As a result of these efforts, 76% of data security professionals in this study believe their organization has a mature or very mature data security strategy. The reality is that companies have spent a lot of money on individual technology — instead of a unified data security strategy — and are judging their maturity based on money spent. While "defense in depth" is a vital element of most organizations' security strategies, organizations use this to justify their investments in new technology. Forrester calls this "expense in depth," an approach where companies buy and buy to ensure marginal returns on their security investment (see Figure 1).[3]

FIGURE 1
Expense In Depth Results In Marginal Returns



Source: Forrester Research, Inc.

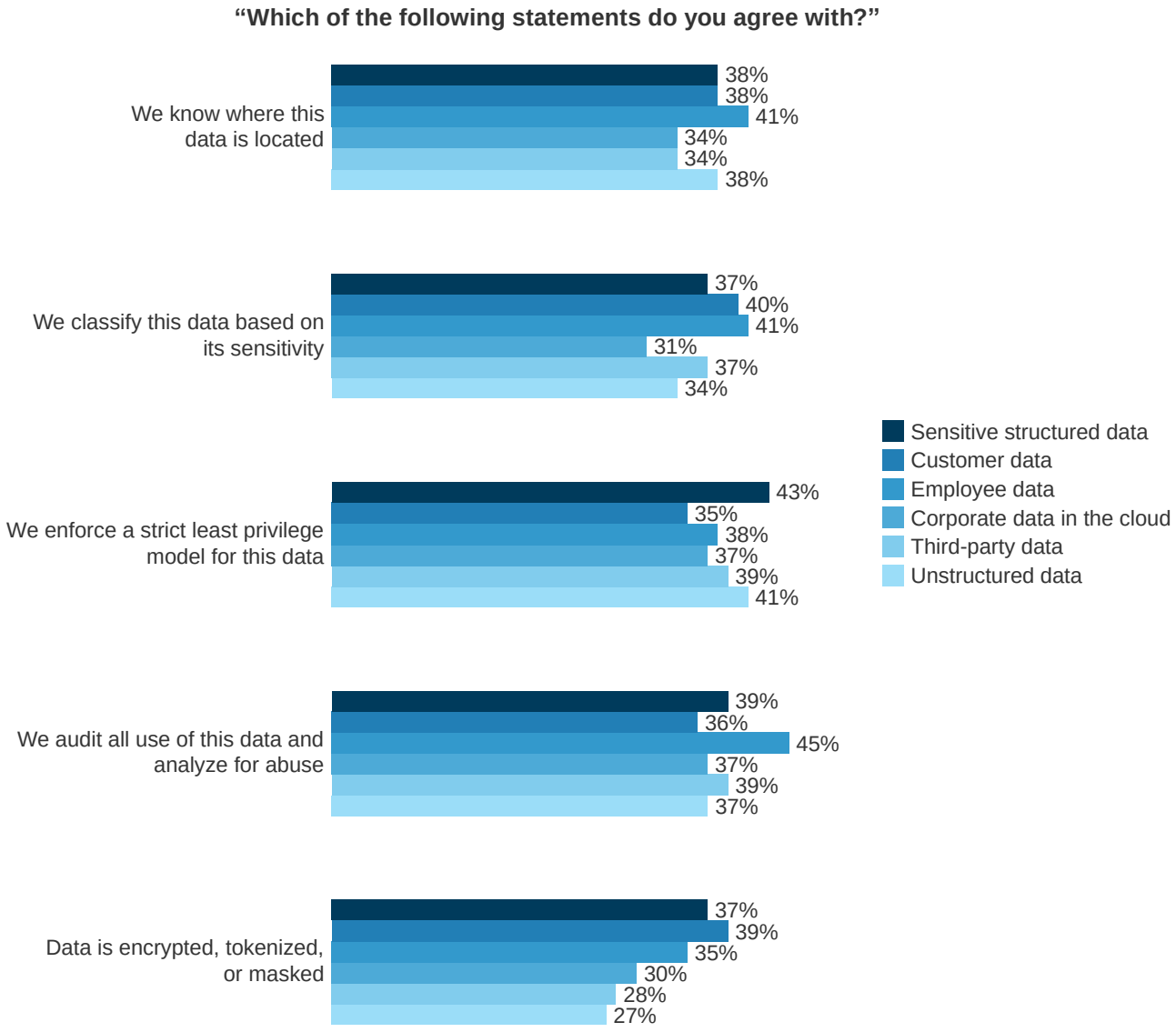
We've seen this before. Years ago when network security was without a firewall, companies bought numerous technologies to protect themselves. Once the next-generation firewall came out, companies realized they were, in fact, not mature at all. The same inflection point exists with data security today.

Companies Struggle With Disparate Data Security Products

Despite investments in a variety of security products and claims of high maturity with data security, signs of low maturity manifest themselves:

- **Data privacy is still a top concern.** Almost 80% of data security decision-makers are concerned or very concerned with customer and employee data privacy. The fact that organizations are concerned with privacy further reinforces their lack of maturity with managing data security.
- **Technical challenges exist with data security.** Ninety-three percent of data security professionals experience technical challenges with data security. There are many issues causing pain, including keeping up with evolving cyberthreats, encrypting data, dealing with disparate products that don't communicate, and controlling access to data, to name a few.
- **Organizational challenges also exist.** Ninety percent experience organizational challenges that impede them from securing data effectively. Topping the list is an inability to keep up with the regulatory landscape, insufficient processes to support data security, and lack of budget for technology.
- **Attempts to understand and control sensitive data fall short.** While organizations feel confident with their data security, they are not getting the visibility and control they need for data. This is likely a combination of issues with existing tools as well as processes and procedures. Most companies have data dispersed across platforms, from browser-based collaboration platforms to cloud-based or on-premises file shares and email. Taking a deeper look, Forrester found that most companies struggle to encrypt data, audit it for abuse, enforce a strict least privilege model, classify it, and even understand where it's located (see Figure 2):

FIGURE 2
Attempts To Understand And Control Sensitive Data Fall Short



Base: 150 North American decision-makers at the manager level and above responsible for data security
Source: A commissioned study conducted by Forrester Consulting on behalf of Varonis, November 2016

- Less than 40% of data security professionals classify their firm's sensitive structured data based on its sensitivity.
- Only 36% of data security professionals audit all use of customer data and analyze it for abuse.
- Less than 40% of data security professionals enforce a strict least privilege model for employee data.
- About one-third (34%) of data security professionals know where their corporate data in the cloud is located.
- Just over a quarter (28%) of data security professionals encrypt, tokenize, or mask third-party data.
- Even fewer data security professionals (27%) encrypt, tokenize, or mask unstructured data.

Buying technology is not a strategy. What companies need is a unified data security strategy that combines all these different products into one platform, thus streamlining classification, security analytics, and reporting into one place.

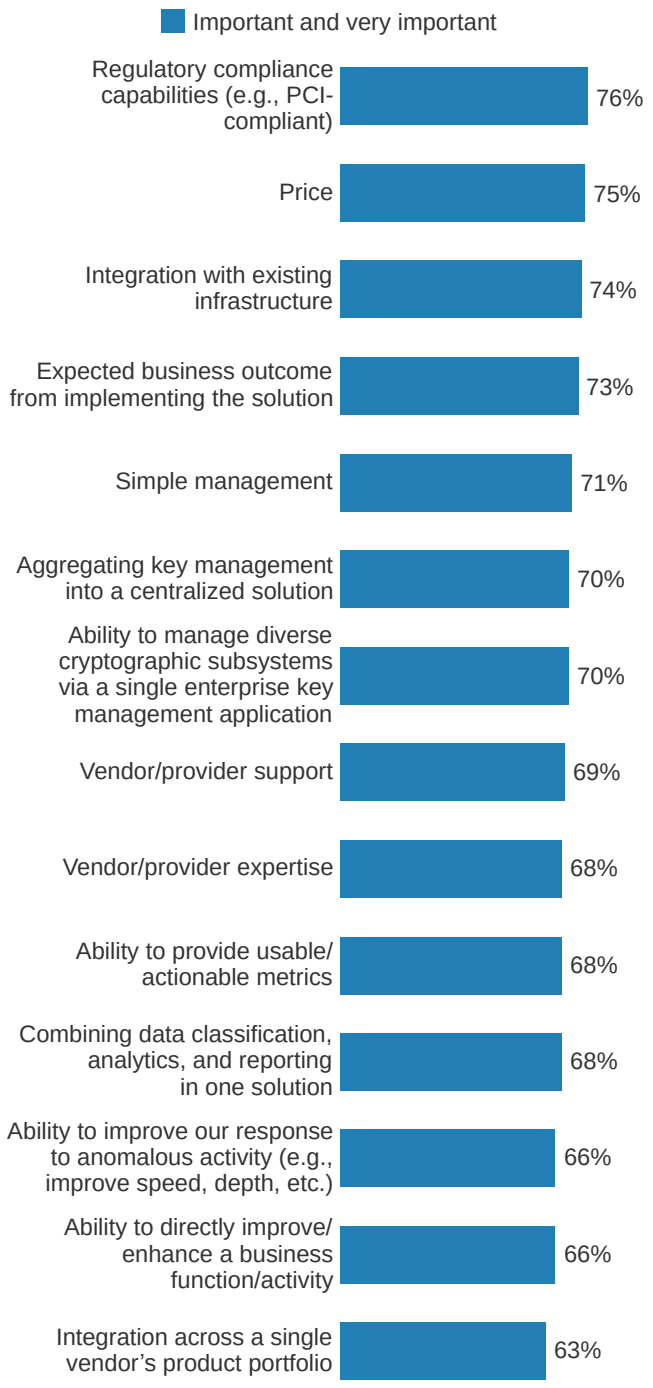
A Strong Data Strategy Requires A Unified Data Security Platform

Given the fragmented state of the market, there is both a need and an appetite for one data security platform that combines data classification, security analytics, and reporting. Almost 90% of decision-makers responsible for data security are interested or very interested in unifying disparate data security products into such a platform. In addition to risk reduction, the majority of companies value a platform that has regulatory compliance capabilities, keeps prices low, and integrates with existing infrastructure. Additional criteria are also at play (see Figure 3). By combining disparate data security tools into a single, unified platform, a data security platform has an opportunity to do for data security what next-generation firewalls have done for network security.

Ninety percent of companies are interested in combining disparate data security products into a unified platform.

FIGURE 3

Companies Have A Long List Of Criteria For A Data Security Platform



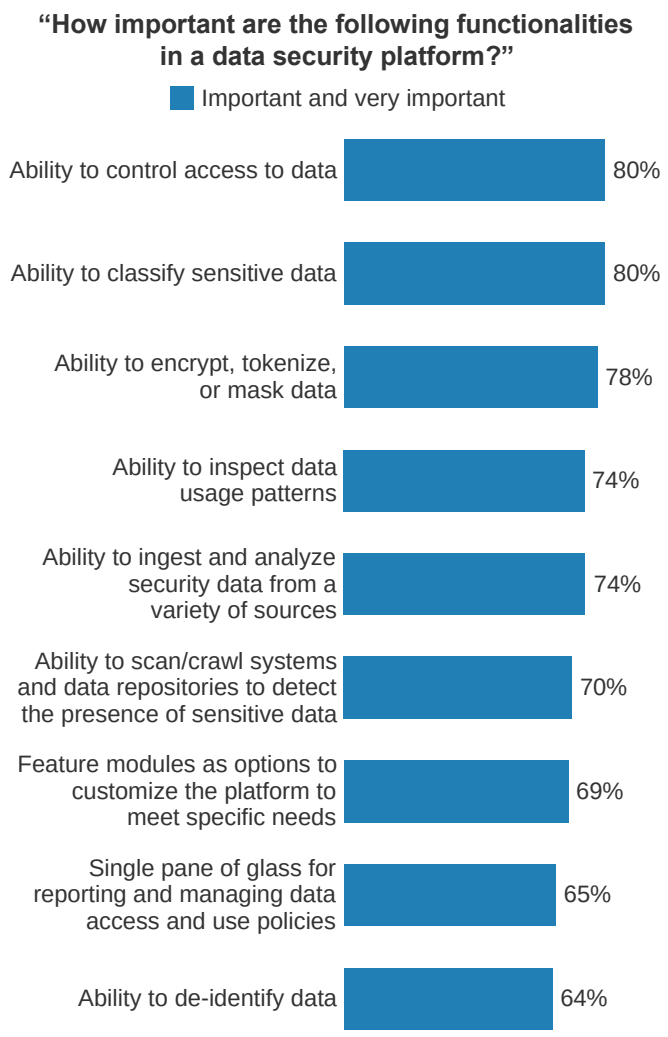
Base: 150 North American decision-makers at the manager level and above responsible for data security

Source: A commissioned study conducted by Forrester Consulting on behalf of Varonis, November 2016

Data security decision-makers also place importance on a variety of functionalities in a data security platform. The top five most important functionalities in a data security platform are access control, classification, encryption, inspection for usage patterns, and analysis (see Figure 4). This supports the notion that firms need to better control their data.

FIGURE 4

Companies Value Many Functionalities In A Data Security Platform



Base: Variable North American decision-makers at the manager level and above responsible for data security

Source: A commissioned study conducted by Forrester Consulting on behalf of Varonis, November 2016

Ninety-six percent of companies believe that changing strategies from many products to a single platform for data would benefit them. A unified data security platform will help provide the data visibility and control that firms desire, while controlling cost and integration concerns.

Ninety-six percent of companies expect to experience benefits as a result of aggregating data security products into a centralized solution.

To manage risk, meet compliance requirements, and go beyond compliance with data security strategy, executives responsible for data security need the capability to define data and bring controls closer to the data. A platform can help to address concerns and challenges that have sprouted from trying to make use of many disparate tools, freeing up resources to allow for greater focus on ensuring that firms have the correct policies, procedures, and remediation actions in place to meet business and data security strategy objectives.

Key Recommendations

A unified data security platform offers core capabilities to help organizations not just establish a robust technology foundation for their data security strategy but also create conditions that help to push firms toward greater security maturity and value-add to the business. With improved integration with existing infrastructure, simplified (and unified) solution management, and greater visibility and control over data, security teams can help the business take on strategic data initiatives with confidence. It's time to put a stop to expense in depth and wrestling with cobbling together core capabilities via disparate solutions. To build your business case for a unified security platform:

- **Expand your view of what constitutes sensitive data.** Think beyond compliance as a primary driver for identifying sensitive data types to take intellectual property and corporate secrets into account. Treat data protection as a corporate fiduciary and social responsibility to better identify sensitive data from customers and employees that may not currently fall under compliance requirements.
- **Answer five key questions to assess your current state of control for sensitive data.** Where is this data? Is it classified by sensitivity? How do you control access? How do you audit the access and use of this data? Is this data encrypted, tokenized, or masked? Also consider where the data comes from and how it is used. It's great if you have taken precautions to secure sensitive data in a particular database, but those efforts are wasted if an authorized user can run and export a report of this sensitive data that is left unsecured and treated as public information.
- **Identify gaps and create your road map for data security capabilities.** Your assessment of the current state of control will give you a sense of strengths and areas for improvement when it comes to data controls for your systems and data repositories, in addition to specific data types of concern. Prioritize your capabilities road map based on the areas where your gaps create the greatest risk.
- **Rethink how you justify and measure the value of investment in data security.** A large security budget is worthless if those resources aren't spent in a meaningful way. Assessing and measuring your data security maturity enables you to define a road map and vision for enduring success. This helps justify and prioritize spending on investments that provide a tangible return on data security.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 150 cross-industry organizations in the US and Canada to evaluate challenges with data security. Survey participants included decision-makers in data management, security, compliance, network infrastructure and operations, application development, and tech support who are responsible for data security at their organization. Questions provided to the participants asked about maturity with data security, adoption of tools, challenges experienced, interest in a data security platform, and potential benefits derived as a result of unifying products in one platform. Respondents were offered incentives as a thank you for time spent on the survey. The study began in September 2016 and was completed in November 2016.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"Planning For Failure: How To Survive A Breach," Forrester Research, Inc., September 9, 2016

"Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities," Forrester Research, Inc., January 7, 2015

"The Future Of Data Security And Privacy: Growth And Competitive Differentiation," Forrester Research, Inc., July 7, 2016

"Digital Insights Are The New Currency Of Business," Forrester Research, Inc., April 27, 2015.

Appendix C: Endnotes

[1] Source: "The Future Of Data Security And Privacy: Growth And Competitive Differentiation," Forrester Research, Inc., July 7, 2016.

[2] Source: "Digital Insights Are The New Currency Of Business," Forrester Research, Inc., April 27, 2015.

[3] Source: "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities," Forrester Research, Inc., January 7, 2015.