FORRESTER®

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

Operationalize Security To Secure Your Data Perimeter

GET STARTED ▶

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

Operationalize Security To Secure Your Data Perimeter

Protecting Your Data Without Sacrificing Business Agility

Every day, companies generate mountains of data that are critical to their business. With that data comes a clear challenge: How do you protect exabytes of data that's strewn across global data centers, computer rooms, remote offices, laptops, desktops, and mobile devices, as well as hosted by many different cloud providers, without choking business agility, employee productivity, and customer experience? The solution lies not in throwing more technology at the network, but in taking specific steps to identify malicious actions and respond to them in order to fix the issue, a process known as operationalizing security.

In August 2017, IBM commissioned Forrester Consulting to conduct a custom survey of 127 IT and security decision makers across industries to explore how organizations are attempting to operationalize security in order to protect their vast stores of data. See the demographic breakdown for respondents below:

Region

- 39% United States
- 27% China
- 25% Germany
- 9% Canada

Company size

- 13% 500 to 999 employees
- 42% 1,000 to 4,999 employees
- 20% 5,000 to 19,999 employees
- 25% 20,000+ employees

Department

- 59% IT
- 41% Security and risk

Job title

- 28% Manager
- 31% Director
- 9% Vice president
- 31% C-level executive

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

Operationalize Security To Secure Your Data Perimeter

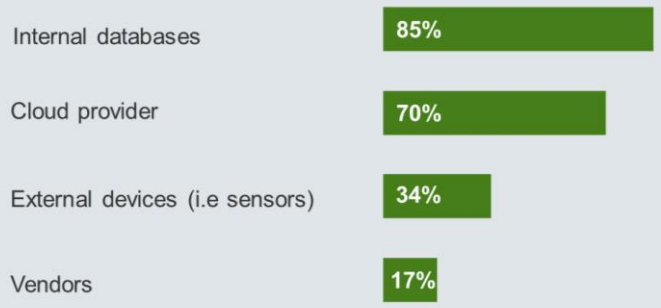
1

Firms Are Confident In Their Ability To Define Their Data Perimeter

The responsibility to secure mountains of data can be challenging. But fortunately, the vast majority of firms believe that they possess the technical details they need in order to accurately define their data perimeter. No small task, considering not just the amount of data, but the fact that the most critical data is sourced from multiple places. Though most firms source this critical data from internal databases, cloud providers, external devices, and vendors also come into play, further complicating matters.

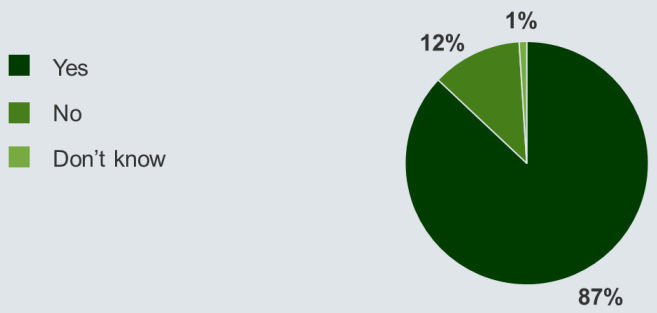
Defining a security perimeter is necessary in order to isolate and segment critical data away from other areas of the network where it would be more vulnerable.

Source Of Most Critical Data



Base: 127 IT and security decision makers at organizations of 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

Do you believe that your organization has the technical details to define what its data perimeter is?



Base: 127 IT and security decision makers at organizations of 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

1 2 3

Data Encryption Is Determined Via Classification Schemes

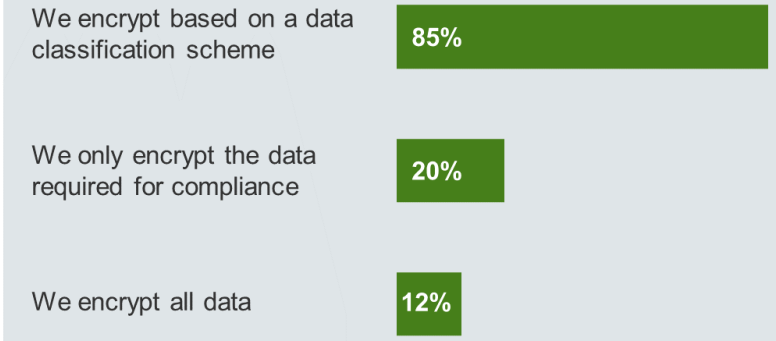
Though regulations are certainly important, the majority of firms choose to encrypt their data based on specific classification schemes rather than on simple compliance. Classification schemes can be any system that indicates what needs to be protected. The US government, for instance, classifies data as “unclassified, classified, secret, or top secret.” Only 12% of respondents we surveyed said that they encrypt all of their data.

NOT ALL DATA IS ENCRYPTED

Shockingly, nearly half of firms say they encrypt little to none of their data. It would seem that although these organizations can define their data perimeter, they are not yet up to the task of securing it.

Forty-six percent of organizations encrypt little to none of their data.

How does your organization determine what data to encrypt?



Base: 127 IT and security decision makers at organizations of 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

1 2 3

Operationalizing Security Is Critical To Protection Efforts

Encryption issues aside, firms are clearly prioritizing data protection:

- 77% of firms protect their data above all else.
- 66% of respondents subscribe to a Zero Trust approach to security.

Additionally, nearly three-quarters of firms note that operationalizing security to secure their data perimeters is a high priority. This indicates that many firms understand the need to move toward a more data-centric approach to security rather than concerning themselves with the legacy perimeters of yesterday.

Despite the move towards operationalizing security and Zero Trust, more than 75% of firms still subscribe to a legacy perimeter approach to security.

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

Operationalize Security To Secure Your Data Perimeter

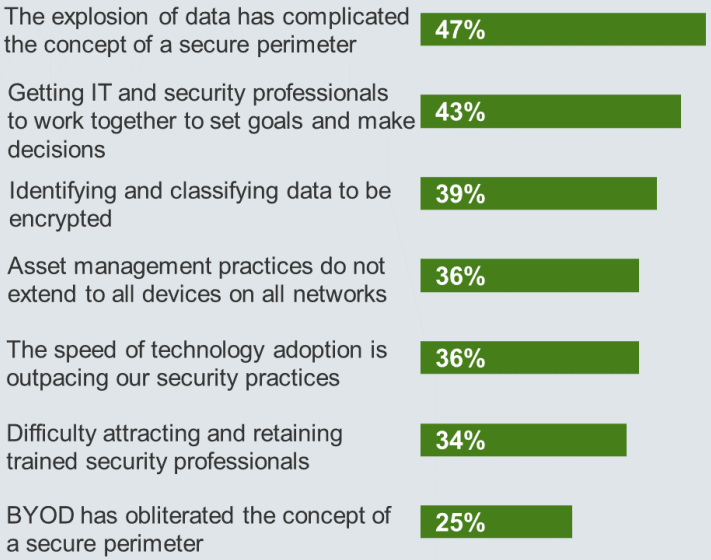
1 2 3

Data Explosion Is The No. 1 Challenge To Operationalizing Security

The main reason that legacy perimeter approaches to security are no longer sufficient today is because of the sheer amounts of data with which each firm must contend. Not surprisingly, nearly half of respondents note that the concept of a secure perimeter is no longer simple because of this data explosion. Identifying and classifying all the data that must be encrypted is also a barrier for 39% of respondents. And a quarter of respondents take it a step further, saying that bring-your-own-device (BYOD) cultures have completely obliterated the concept of a secure perimeter. Clearly, the perimeter approach is not the way to go anymore.

Organizational issues shouldn't be ignored: 43% say that getting IT and security teams to work together effectively is a key challenge.

Challenges To Operationalizing Security



Base: 127 IT and security decision makers at organizations of 500 or more employees (not all responses shown)
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

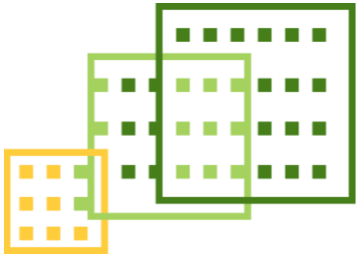
Operationalize Security To Secure Your Data Perimeter

1 2

Firms Are Taking The Necessary Steps To Operationalize Security

Despite the challenges, firms are moving in the right direction. The majority of organizations are continuously measuring for acceptable levels of risk, implementing access controls, and automating authorization and verification rules, which shows a decisive move toward operationalizing security. However, not everyone is there yet. A full third of firms are not currently assessing the totality of devices that touch their network, indicating that many are still only mid-journey. Without a thorough understanding of applicable devices, organizations' views of their data perimeter will remain incomplete, leaving them vulnerable to breaches.

Data encryption remains a challenge for many, though 59% are currently working toward full encryption.



Actions Taken To Operationalize Security

Base: 127 IT and security decision makers at organizations of 500 or more employees (not all responses shown)
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

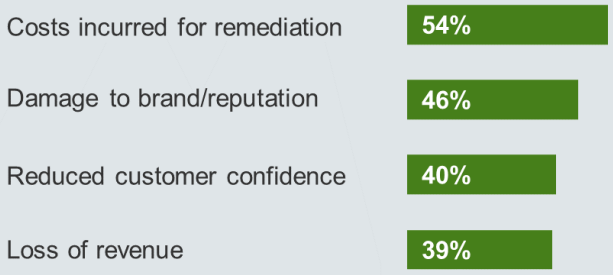
Operationalize Security To Secure Your Data Perimeter

1 2

Operationalizing Security Benefits The Customer, The Brand, And The Bottom Line

Security breaches are a clear threat to the livelihood of firms, resulting in costly remediation, damage to brand reputation, and reduced customer confidence. But this is not just about reducing breaches. When security is optimally operationalized, businesses experience increased customer trust, improved reputations, and improved customer acquisition and retention, in addition to simply cutting costs. When done right, protecting your data perimeter is not just about negating potential costs, but allowing firms to remove the stress of constant impending threats and focus more on the customer and their needs.

Impact Of Security Breaches



Base: 127 IT and security decision makers at organizations of 500 or more employees (not all responses shown)
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

Benefits Of Operationalizing Security

Base: 127 IT and security decision makers at organizations of 500 or more employees (not all responses shown)
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

A Custom Technology Adoption Profile Commissioned By IBM | September 2017

Operationalize Security To Secure Your Data Perimeter

Conclusion

Contending with the data explosion is no small feat for today's security professionals. In order to avoid costly breaches and win and retain their customers' trust, firms must work to clearly define their data perimeter while operationalizing the security processes that protect it. By understanding the totality of devices that touch the network, enacting strict change management practices, and enforcing role-based access control across the enterprise, organizations will be better equipped to secure their customer's data, regardless of how much of it there is or where it's stored.

METHODOLOGY

- This Technology Adoption Profile was commissioned by IBM.
- To create this profile, Forrester Consulting conducted a custom survey of 127 IT and security professionals at North American, German, and Chinese companies with at least 500 employees across industries. Respondents had to be responsible for their organization's security infrastructure and operations.
- The survey was completed in August 2017. For more information on Forrester's data panel and Tech Industry Consulting services, visit forrester.com.

Project Director
Rachel Linthwaite
Market Impact Consultant