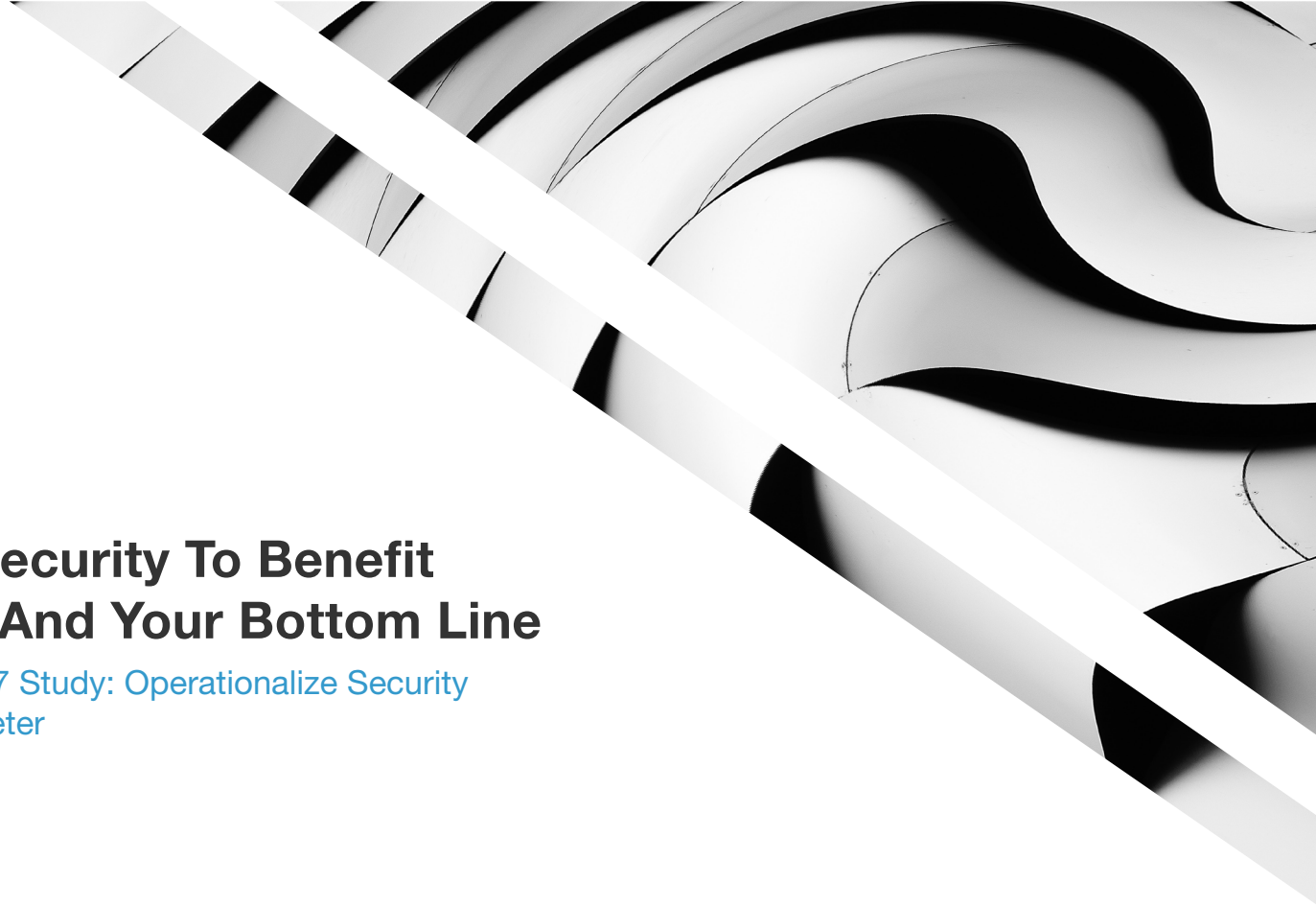
FORRESTER®



Operationalize Security To Benefit Your Customers And Your Bottom Line

A 2019 Refresh Of The 2017 Study: Operationalize Security To Secure Your Data Perimeter

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY IBM | OCTOBER 2019

Operationalizing Security Is Critical To Protecting Your Data

The data explosion has put firms in a difficult situation when it comes to securing their data perimeter. Operationalizing security — that is, the process of taking specific steps to identify potentially malicious actions and responding to them in order to fix the issue — came to the forefront in a 2017 study on IT and security decision makers commissioned by IBM. Two years later, firms are making progress toward their ultimate goal of a secure data perimeter, though there's still plenty of work to be done.

In 2019, IBM commissioned a follow-up study from Forrester Consulting to understand how firms are continuing to address the need for operationalizing security in order to maintain customer trust, align internal resources, and drive the bottom line.

Key Findings

Though there has been some progress, many firms are still struggling to encrypt the majority of their data.

Ultimately, firms are headed in the right direction, focusing on data protection by operationalizing security and adopting Zero Trust frameworks to a greater degree than they were just two years prior.

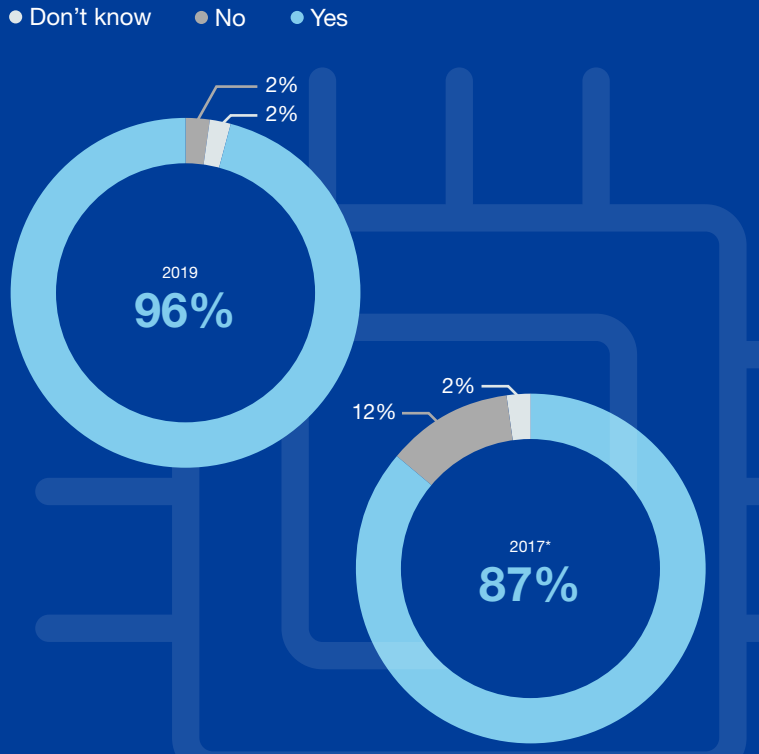
Security professionals are finally starting to focus on both gaining and maintaining customer trust and the benefits of operating from a customer-obsessed perspective.

Nearly All Firms Believe They Can Accurately Define Their Data Perimeter . . .

Despite the mountains of data that enterprises continue to collect and generate, today's respondents are even more confident than they were two years ago in their ability to define their data perimeter, that is the boundary around information used to provide added value to customers and recipients of content for a business. Today, 96% of respondents say they have the technical details to accurately complete this task, an increase from 87% two years ago.

Defining a data perimeter is necessary in order to isolate and segment critical data away from other areas of the network where it would be more vulnerable. This is no small task as data can be sourced from multiple internal and external sources. There can also be several concentric perimeters based on the criticality and value of the data itself. For example, it is critical to keep personally identifiable information (PII) secure in order to maintain regulatory compliance and keep customers' information private.

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



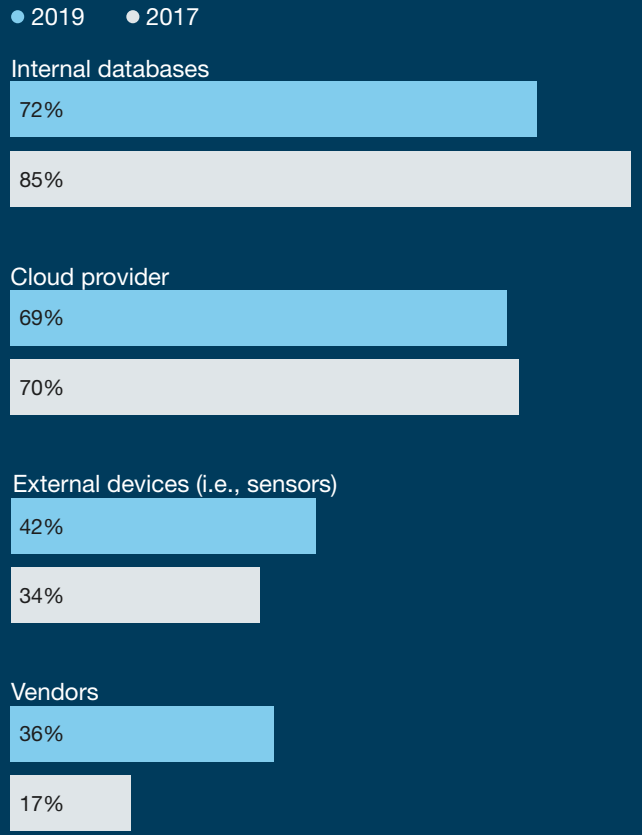
Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

. . . Despite An Increasingly Complex Data Environment

The fact that nearly everyone believes they can distinguish their most critical data, and securely segment it, is impressive considering that more of firms' most critical data is being sourced from outside of their internal databases.

The rise of IoT has contributed to 42% of critical data being sourced from external devices (up from 34% two years ago). Similarly, 36% of firms source this critical data from vendors, a huge leap from the 17% in 2017. While critical data is still most often sourced internally and from cloud providers, vendors and external devices are playing a larger role than they did in 2017, further complicating an already complex data landscape.

Source Of Most Critical Data



Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

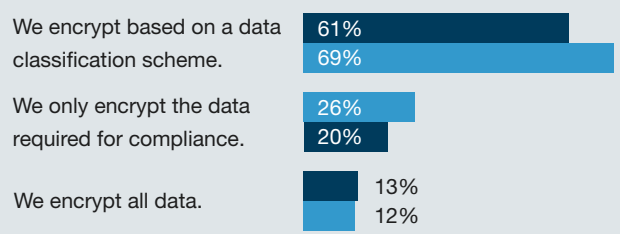
Yet Nearly Half Of All Firms Still Fail To Encrypt The Majority Of Their Data

Despite firms' newfound confidence in defining what data needs to be segmented and isolated to avoid vulnerabilities, they have made no strides in data encryption. Today, 45% of firms encrypt little to no data, which is nearly identical to the 46% of firms which said the same in 2017. This is an alarmingly large number considering that 77% of firms claim to be focused on protecting data above all else.

While the amount of data being encrypted has remained stunningly stagnant, the methods for determining encryption have shifted some. Specifically, those encrypting based on compliance requirements have increased to 26% (from 20% in 2017), perhaps due to the advent of regulations like the EU's General Data Protection Regulation (GDPR). Nevertheless, the majority of firms still encrypt based on classification schemes which, given the current state of encryption, likely need revision.

45% say their organization encrypts little to none of their data, which is essentially the same as in 2017 (46%).

"How does your organization determine what data to encrypt?"



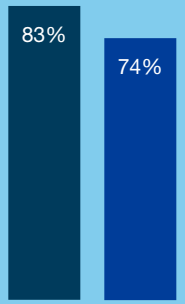
Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

Firms Are Starting To Update Their Approach To Security

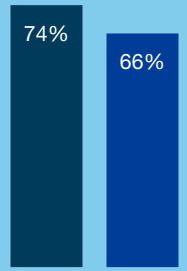
Firms' failure to encrypt is not indicative of a resistance to improve security overall. In fact, operationalizing to secure data perimeters is the highest priority for firms in 2019, growing 9% from 2017. Likewise, the amount of firms adhering to a Zero Trust approach — a conceptual and architectural model for security that abolishes the idea of a trusted network inside a defined corporate perimeter — has increased to 74%. Zero Trust and operationalizing security have overtaken a perimeter approach to security, which has fallen by 6% since 2017. And while there are still plenty of firms that subscribe to this traditional approach, the movement toward operationalizing security and Zero Trust indicates a shift toward more advanced, modernized security strategies that prioritize data privacy over the increasingly outdated perimeter method.

Firms Are Taking A Step In The Right Direction

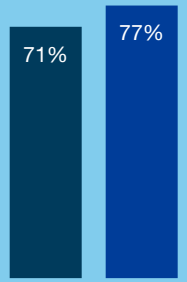
- Strongly agree/agree 2019
- Strongly agree/agree 2017*



Operationalizing security to secure our data perimeters is a high priority for our firm.



Our organization subscribes to a Zero Trust approach to security.



Our organization subscribes to a perimeter approach to security.

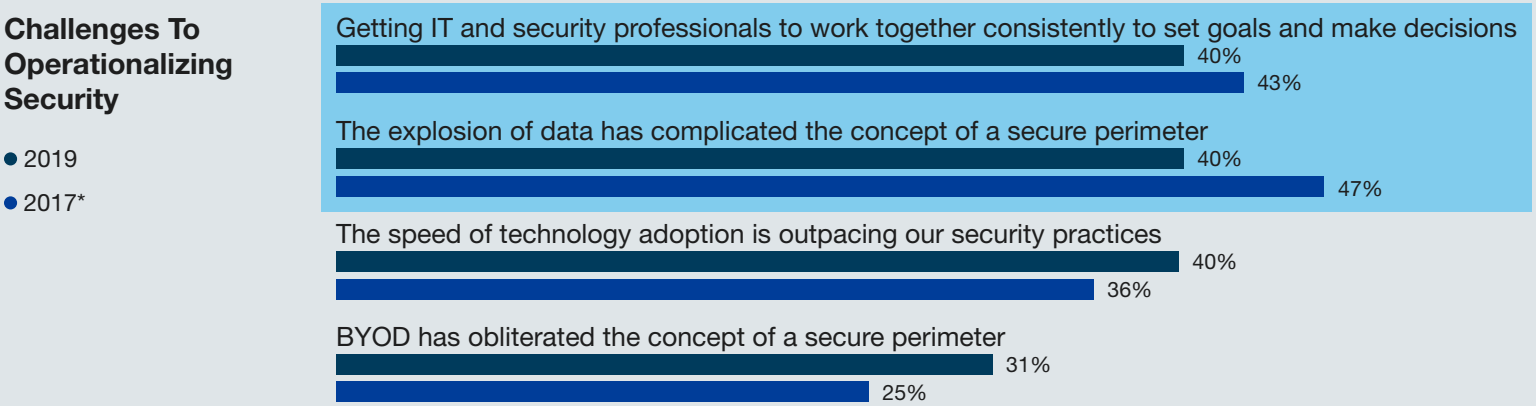
Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

Firms Remain Challenged By Vast Amounts Of Data On Their Quest To Operationalize Security

As it was in 2017, so it remains today. The main reason that legacy perimeter approaches are no longer sufficient is because of the shear amounts of data with which each firm must contend. The explosion of data remains the No. 1 challenge for firms. The increasing popularity of bring-your-own-device (BYOD) models, which obliterates the idea of a secure perimeter and introduces myriad vulnerabilities into enterprise networks (in addition to strict regulations surrounding PII and privacy), also complicates matters.

Still, data is not the only concern. Bridging the gap between IT and security employees remains a top challenge, moving up to share the No. 1 spot in this year's study. This lack of an effective working relationship if left unsolved will only exacerbate problems going forward. It also shows the need for a deeper progression toward DevSecOps — the philosophy of integrating security practices within the DevOps process.[1]

Challenges To Operationalizing Security



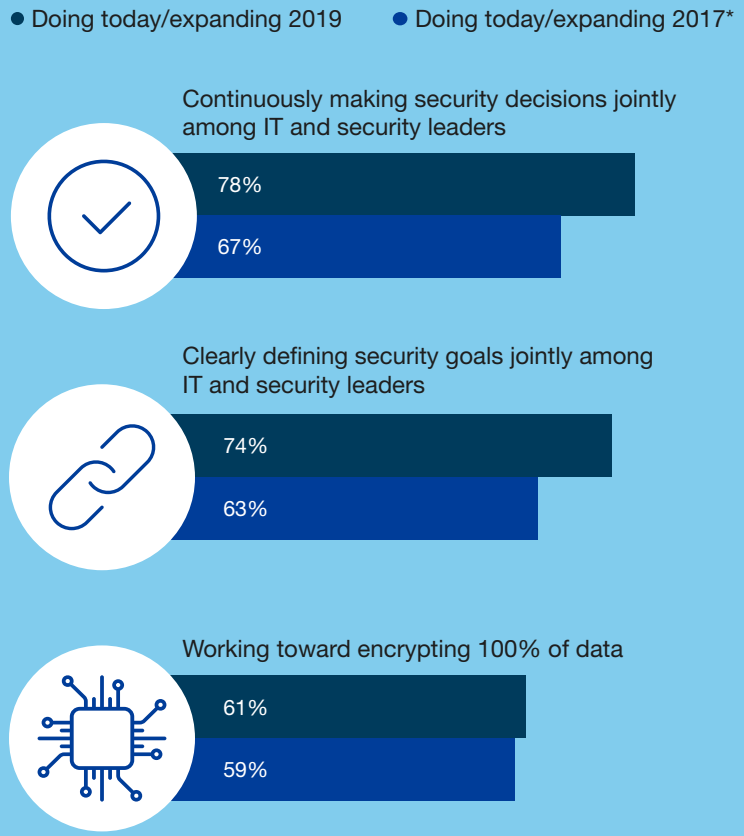
Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

Firms Are Making More Progress With Organizational Issues Than Data Concerns

Firms are working toward operationalizing security, but data problems have proved most difficult to address. Only 61% of firms are working toward 100% data encryption, a percentage that has remained consistent. Why is this a problem? Data breaches are a fact of life today, and while intruders can often compromise networks, the data they extract is only valuable if it can be read.[2] Firms that successfully encrypt their data are less vulnerable, even if breached.

However, firms are making progress with their teams: 78% of firms are continuously making joint security decisions among IT and security leaders, and 74% are clearly defining security goals jointly among these same teams. Both numbers are higher than they were in 2017, showing that when firms put their mind to solving an issue, they can make real progress.

Actions Taken To Operationalize Security



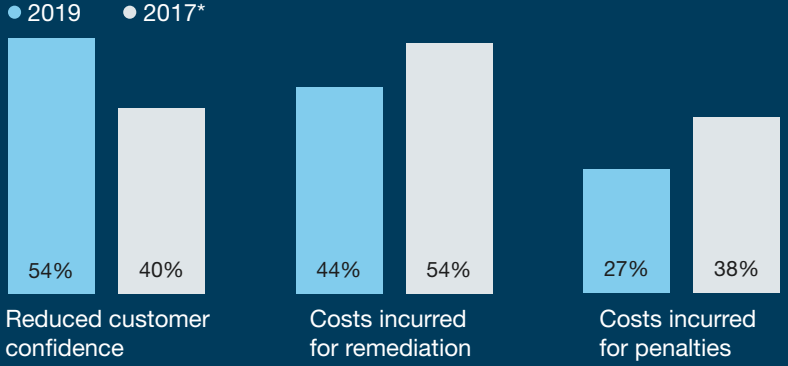
Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

Security Teams Have A New Focus On Customers

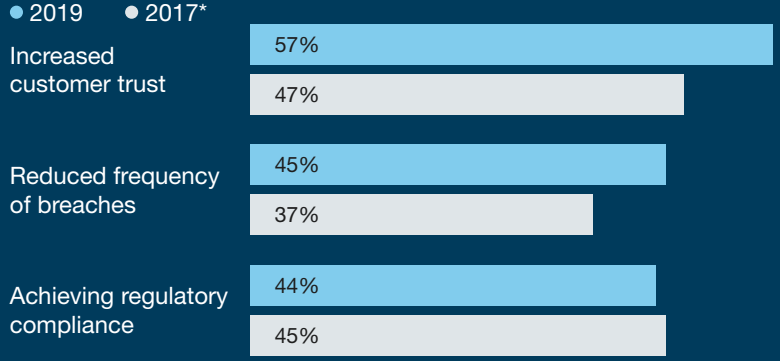
Today, firms are putting their customers before cost savings. More respondents in this year's study were concerned over losing their customers' confidence than in 2017. Furthermore, the desire to cut costs is no longer the primary motivator for improving security. Today's security professionals are far less worried about incurring costs for penalties and remediation than they were two years ago. This new focus on gaining and maintaining customer trust suggests that security teams are starting to understand the importance of customer obsession.

This is not to say, of course, that operationalizing security won't have any financial benefits: 41% of firms expect to spend less on breach remediation, and 36% anticipate cutting losses due to breaches. Firms also expect to see less breaches and improved compliance as a result of their work.

Impact Of Security Breaches



Business Benefits Of Operationalizing Security



Base: 121 IT or security decision makers in North America, Germany, China
*Base: 127 IT and security decision makers in North America, Germany, China
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2019

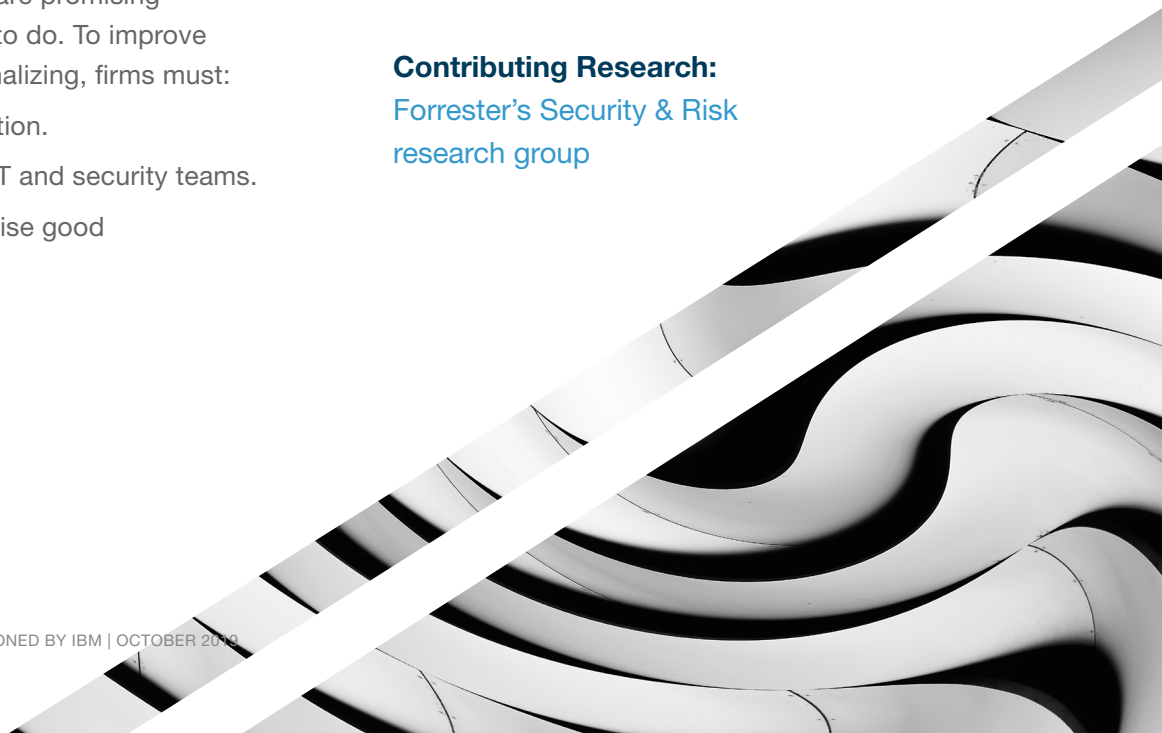
Conclusion

While firms are making important improvements toward operationalizing security, they still have a long way to go to full optimization. An increased focus on customer trust and a move away from dated perimeter approaches are promising developments, but there is still plenty of work to do. To improve their overall security posture through operationalizing, firms must:

- Continue to work toward 100% data encryption.
- Optimize the working relationship between IT and security teams.
- Ensure that security efforts do not compromise good customer experiences.

Project Director:
Rachel Linthwaite, Senior Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group



Methodology

This Opportunity Snapshot was commissioned by IBM. To create this profile Forrester Consulting conducted a custom survey of 121 IT and security professionals at North American, German, and Chinese companies with at least 500 employees across industries. Survey participants are responsible for their organization's security infrastructure and operations. The custom survey began and was completed in September 2019.

The original study was conducted in August of 2017. For that study, Forrester Consulting conducted a custom survey of 127 IT and security professionals. Every effort was made to ensure consistency across samples for the 2017 and 2019 studies.

ENDNOTES

[1] DevSecOps: development, security, and operations.

[2] Source: "Use Advanced Encryption For Data Security," Forrester Research, Inc., January 30, 2019.

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.

Demographics

GEOGRAPHY

- 32% US
- 7% Canada
- 30% Germany
- 31% China

COMPANY SIZE

- 39% 500 – 900 employees
- 38% 1,000 – 4,900 employees
- 17% 5,000 – 19,999 employees
- 7% 20,000 or more employees

RESPONDENT LEVEL

- 34% Manager
- 36% Director
- 10% VP
- 20% C-level executive

TOP INDUSTRIES

- 19% Manufacturing
- 17% High tech
- 14% Financial services
- 6% Healthcare

FORRESTER®