FORRESTER®

FOR CIOS

# Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks

### Increase Business Agility By Adopting Zero Trust

by Martha Bennett

June 14, 2017

## Why Read This Report

Legacy, perimeter-centric models of information security are of no use in today's digital businesses, as they are no longer bounded by the four walls of their corporation. Instead, CIOs must move toward a Zero Trust approach to security that is data- and identity-centric — and in our view is the only approach to security that works. In this report, we outline what constitutes Zero Trust, provide guidance on how to implement it, and summarize the key business benefits.

## Key Takeaways

**Current Approaches To Security Can't Mitigate The Consequences Of A Breach**

As long as criminals can move around networks with impunity once they're in, CIOs and chief information security officers (CISOs) are fighting a losing battle, and businesses remain at risk of major data-loss events. That's why leading organizations and governments are adopting a Zero Trust approach to security.

**A Zero Trust Approach To Security Doesn't Distinguish Between Internal And External**

Treat all traffic and users the same, regardless of location or hosting model, and segment internal networks appropriately. This will mitigate the risk of internal breaches (whether deliberate or accidental) and localize the damage from potential infiltration or malware.

**Zero Trust Security Leverages Existing Investments In Technology And Skills**

In addition to addressing critical security and risk management challenges, a Zero Trust approach brings benefits such as better understanding of data and process flows as well as improved alignment between the CIO, CISO and business executives.

# Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks

## Increase Business Agility By Adopting Zero Trust

by Martha Bennett
with Stephanie Balaouras and Michael Glenn
June 14, 2017

## Table Of Contents

Recommendations

## Related Research Documents

Calculate The Business Impact And Cost Of A Breach

Creating Actionable Security And Privacy Policy

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

FORRESTER®

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

© 2017 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

## Adopting A Zero Trust Approach To Security Is Imperative

Ask CIOs what keeps them awake at night, and security is bound to be on the list, if not at the top. While security has always been a concern, CEOs now care about security to a degree they mostly didn't in the past. A key catalyst for this sentiment change was the Target hack in 2013, which was the first documented and well-publicized occurrence of a CEO and CIO losing their jobs as the result of a security breach.[1] Since then, a parade of mega breaches and nation-state cyberattacks on government and enterprise systems has underlined the fact that existing approaches to security aren't the answer.[2] The Zero Trust approach to security is the only strategic model that can create a win-win situation for the business as well as the CIO — and it's a model that security teams and their counterparts can begin to implement today. Any CIO who remains ambivalent about moving to Zero Trust should bear in mind that:

› **Current approaches to security can't mitigate the consequences of a breach.** While the Target breach and its aftermath marked a major milestone in attitudes, security in most organizations still hasn't evolved from conventional approaches that clearly don't work. Another CEO made headlines in late 2015 when UK telecom firm TalkTalk suffered a major breach, and she admitted publicly that nobody quite knew what security measures were actually in place, despite the widely held view that the company was taking security very seriously.[3] In the weeks following TalkTalk's customer breach, the company's shares plummeted by 20%.[4] A few months later, the company reported the loss of 100,000 customers and costs of about £60 million.[5]

› **Major government organizations are moving toward Zero Trust.** On September 7, 2016, The US House Committee on Oversight and Government Reform (OGR) issued a scathing rebuke of the US Office of Personnel Management's (OPM's) security practices, which led to one of the most significant data breaches in history.[6] In the OGR report, the committee suggested that government agencies "reprioritize federal information security efforts toward a zero trust model." It also asked the US Office of Management and Budget to "provide guidance to agencies to promote a zero trust IT security model." In the US, as more federal CIOs and CISOs adopting Zero Trust, we expect this adoption to ripple to the industries that do business with and sell technology to the US government. As nation-state attacks and concerns increase, we expect other governments to adopt Zero Trust.

### Take "Zero Trust" Literally, And Stop Differentiating Between Internal And External

Zero Trust is an architectural model for how security teams should redesign networks into secure microperimeters, increase data security through obfuscation techniques, limit the risks associated with excessive user privileges, and dramatically improve security detection and response through analytics and automation. Zero Trust demands that CIOs and CISOs move away from legacy, perimeter-centric models of information security — which are useless for today's digital businesses, no longer bounded by the four walls of their corporation — to a model that is both data- and identity-centric and extends security across the entire business ecosystem. We call our model Zero Trust because we want to warn security leaders about the dangers of the numerous trust assumptions

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

they make in their architecture — whether that's trusting that internal network traffic is legitimate by default, trusting your employees to always have the best intentions or to never make bad decisions, trusting partners to treat access to your systems and your data like it was their own, and so on (see Figure 1). Three concepts are at the heart of Zero Trust:[7]

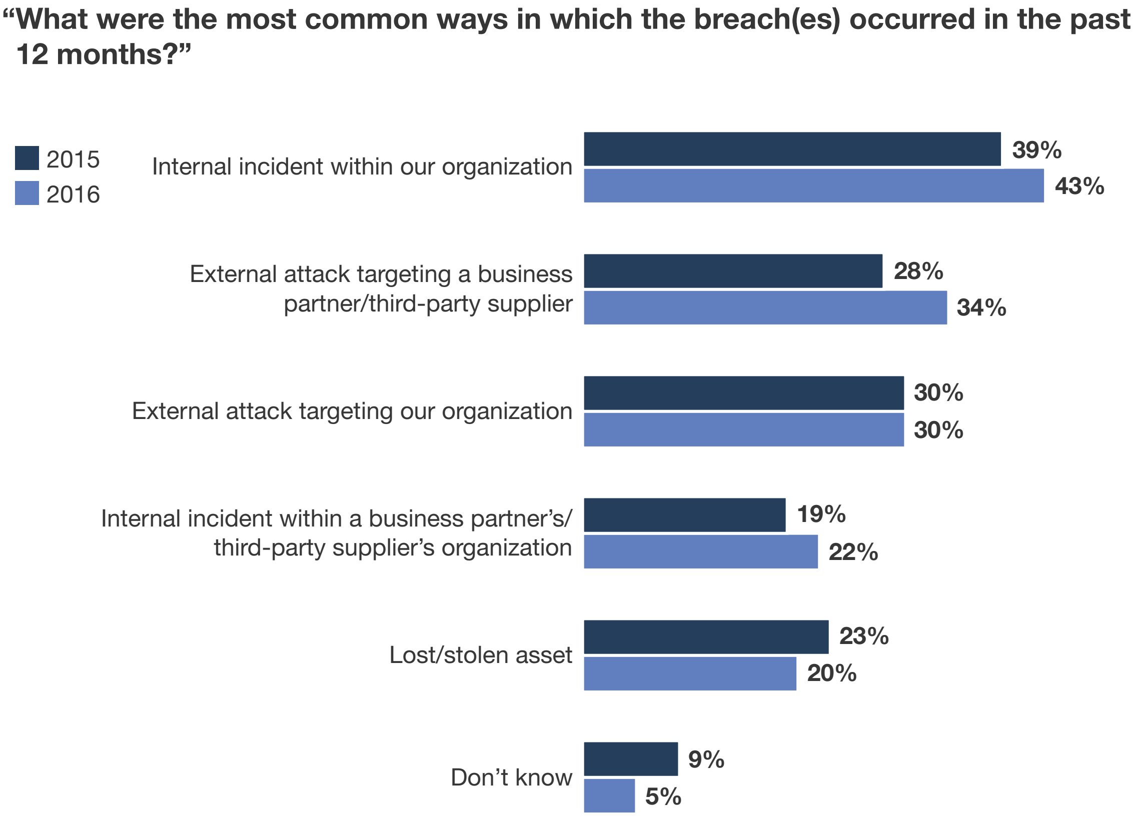
› **Ensure all resources are accessed securely, regardless of location or hosting model.** This means working on the assumption that all traffic is threat traffic until you've authorized, inspected, and secured it, regardless of whether an internal or external party is accessing your systems and regardless of whether the data is located within your data center or in the cloud. It also means adopting a data- and identity-centric approach. Integral to this is the concept of microperimeters, which support more granular access restrictions and additional security controls. If you segment your sensitive systems and data into a series of microperimeters, rather than simply design one monolithic network akin to a castle wall, then a breach of the network doesn't give cybercriminals or malicious insiders free reign across the entire environment.

› **Adopt a "least privilege" strategy and strictly enforce access control.** Providing people with only the right amount of access they require to do their job not only mitigates against the risk of malicious access, it also reduces the risk of employees leaking data. While Zero Trust doesn't specify role-based access as the preferred access control methodology, it's the most commonly used today. To go with it, you'll also need an identity and access governance strategy to periodically review and recertify access rights.[8] For employees with access to the most sensitive systems, implement privileged identity management solutions; these provide additional control mechanisms, such as the requirement to check out passwords.[9]

› **Inspect and log all traffic for suspicious activity.** Even the strictest access controls only go so far. That's why it's important to change the "trust but verify" paradigm to the more appropriate "verify and never trust." Security teams could have detected and contained some of the largest breaches in the recent past if they had been monitoring for anomalous user behavior or network activity. For example, in January 2014, financial regulators revealed that a contractor at the Korea Credit Bureau stole more than 105 million records containing the personal information of 20 million South Koreans — nearly 40% of the population. When a privileged user downloads 105 million records containing sensitive information from a production database to removable media, security analysts in the security operations center should notice. They should automatically block the transfer of this data, reset user passwords and privileges, and begin an investigation.[10]

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

**FIGURE 1** The Most Common Security Breaches Remain Internal Events



Base: 565 (2015) and 619 (2016) global network security decision makers whose firms had a security breach in the past 12 months

Note: Multiple responses are accepted; "Other" responses are excluded.

Source: Forrester Data Global Business Technographics® Security Survey, 2015 and 2016

## Follow These Five Steps To Zero Trust Information Security

A Zero Trust architecture is an essential element in your overall security strategy, but it isn't the only element. You still need, for example, to scope the responsibilities of your security function, its organizational structure and staffing, as well as a road map for capital and operating expenditure. Moving toward Zero Trust clearly has implications for the other components of your security strategy, which are beyond the scope of this report. Focusing on Zero Trust, Forrester recommends your organization's security team take the following steps:[11]

1. **Identify and classify sensitive data, and segment your network accordingly.** When classifying your data, keep it simple. Three overarching categories will suffice: public (loss doesn't harm either employees or customers), toxic (loss is undesirable but harm is minimal), and radioactive

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

(loss results in privacy or other compliance violations; intellectual property is compromised). Categorizing data in this way makes it more likely that your classification project works. In terms of network design, the goal is to create small network segments, or microperimeters, which you can then combine to create a larger Zero Trust network (see Figure 2).

2. **Map the flow of your sensitive data.** Before you design a Zero Trust network, you must understand how your data flows across your network as well as between users and applications (including associated resources such as storage). You'll need to engage multiple stakeholders at this stage and establish a cross-functional team; these typically include application architects, network architects, enterprise architects, and business domain experts. The team will need to locate and map all dependent network and computer objects; while this sounds onerous, it's a critical step that has other benefits, such as providing you with the opportunity to optimize flows, retire redundant hardware or software, and so on. You can leverage data flow and network diagrams from compliance initiatives such as PCI.

3. **Architect your Zero Trust security network.** The design of your Zero Trust network will reflect how transactions flow across it and how users and other systems access sensitive data. Create microperimeters around sensitive data. You can enforce these segments with physical or virtual appliances, such as next-generation firewalls from vendors like Check Point Software, Cisco Systems, Fortinent, and Palo Alto Networks, but there are alternative approaches that use obfuscation techniques for network segmentation, such as Unisys' Stealth offering.

4. **Create fine-grained security policies to enforce access controls and segmentation.** To enforce strictly limited access, security pros must put in place fine-grained authorizations. Too often, security teams rely on inaccurate, manual, and inefficient identity processes. CIOs and CISOs should adopt an identity management and governance platform (e.g., SailPoint or RSA) that provides user account provisioning, role management, access request management, and access certification. Security leaders should also ensure that security teams configure, continuously audit, and optimize the rule sets in network access controls, next-generation firewalls, and other network-based solutions that can analyze, control, and block network traffic. Today, these solutions have app layer visibility that enables security teams to allow, deny, or restrict access to specific applications.

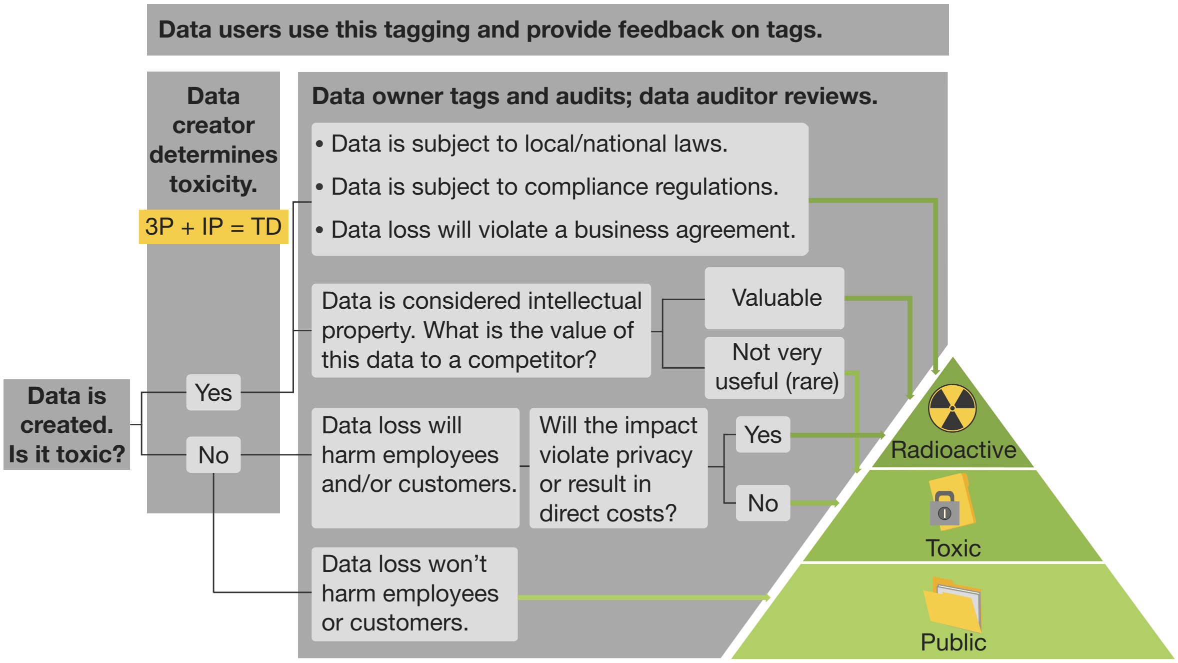
5. **Continuously monitor your Zero Trust ecosystem.** As discussed, a key characteristic of a Zero Trust network is the logging and inspecting of all traffic, regardless of whether it's internal or external. When preventive controls fail, security teams must rely on network and application visibility to quickly identify and respond to security incidents. Today's security analytics solutions ingest and correlate data from

> When classifying your data, keep it simple. Three overarching categories will suffice.

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

multiple disparate sources, including network flow data, identity data, user behavior data, and app-specific data. Features like security user behavior analytics provide insight into user activity to identify malicious users and compromised accounts. Carefully examine your network traffic to identify signs of malicious behavior like compromised accounts or infected endpoints.[12]

**FIGURE 2** Create A Zero Trust Model With Three Classifications Of Data


Data users use this tagging and provide feedback on tags.
Data creator determines toxicity.
3P + IP = TD
Data owner tags and audits; data auditor reviews.
• Data is subject to local/national laws.
• Data is subject to compliance regulations.
• Data loss will violate a business agreement.
Data is considered intellectual property. What is the value of this data to a competitor?
Valuable
Not very useful (rare)
Data is created. Is it toxic?
Yes
No
Data loss will harm employees and/or customers.
Will the impact violate privacy or result in direct costs?
Yes
No
Data loss won't harm employees or customers.
Radioactive
Toxic
Public

## Zero Trust Security Delivers Many Business Benefits

Protecting the business from harm is the core of all security measures and initiatives. A Zero Trust approach to security clearly has the same aim, but the benefits for the business go much further. We have identified eight key business and security benefits.[13] Zero Trust:

› **Improves visibility throughout the network and reduces time to breach detection.** Common refrains in reports about serious breaches include "the hackers were able to work undetected for X number of months" and "once the bad guys were in, they were able to move around the network unhindered." With Zero Trust, security pros have visibility into exactly what's going on at all times, and they are able to stop an attack as soon as the tell-tale signs become apparent. In 2016, Yahoo revealed that cybercriminals had compromised the personally identifiable information (PII) for up to

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

1 billion user accounts. The initial breach occurred in late 2014, but Yahoo did not discover it until August 2016, in the course of a separate breach investigation. As a result, Verizon slashed its offer price for Yahoo by $350 million. Additional breach costs, particularly from lawsuits, are inevitable.[14]

- **Stops malware propagation and lateral movement.** In traditional networks, malware typically penetrates much more deeply into systems than is apparent, due to lack of segmentation and poor network visibility. It's different in a Zero Trust network: The combination of more granular network rules and microperimeters around specific data types, assets, services, and applications makes it much harder for malware to propagate or for an attacker to gain access to other systems. For example, if you're a hospital, a breach of the POS system in the cafeteria or gift shop doesn't allow attackers to gain access to clinical systems. If you're a retailer, a malware infection in one corporate system doesn't allow attackers to infect every one of your brick-and-mortar locations within two weeks.

- **Reduces both capital and operational expenditures on security.** Improving security is invariably associated with increased cost. With Zero Trust, this is typically not the case; to the contrary, improved security enables CIOs and security pros to reduce both one-off and ongoing outlays. For example, next-generation firewalls consolidate disparate security controls into a single solution with a single management console. Combined with centralizing the location of security tools, the reduction in the number of disparate security solutions also means reduced training costs, and it enables security pros to focus on key security activities rather than spend time managing the environment.

- **Shrinks the scope and cost of compliance initiatives.** Because Zero Trust networks are by definition segmented, a compliance initiative need only involve the relevant network segment. By comparison, without network segmentation, it's likely that the entire network is in scope when it comes to proving regulatory compliance (as is the case with PCI DSS, for example). Compliance with the EU's General Data Protection Regulation (GDPR) will also be much easier to achieve and prove under a Zero Trust approach. Compliance audits also become a lot less painful, as many of the things auditors will look for — and typically recommend for remediation — are inherently part of a Zero Trust network design.

- **Eliminates finger-pointing and fosters a more mature tech management approach.** CIOs typically have a variety of organizational units reporting to them: network teams, operations teams, computing/virtualization teams, application development teams, security teams, and so on. When something goes wrong, the buck-passing starts: It was the fault of the network team; no, it was the fault of the security team; no, the app dev folks are to blame; and so on. By contrast, Zero Trust builds bridges by requiring collaboration between teams. The real-time root-cause analysis, transparency, and visibility inherent in Zero Trust further support the move from finger-pointing to cooperation. This breaking down of silos in turn provides a good basis for the entire technology management organization to become more agile and develop a more mature approach.

- **Increases data awareness and insight.** Once you know what data you have, where it is, and how you should classify it, security pros can set the right policies and make sure that the most sensitive data is subject to the strongest controls. And just as Zero Trust gives you visibility into

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

potential threat traffic, it also gives you greater insight into your data and how it moves across the network. This enables you to identify potential compliance breaches before they become a problem (e.g., sharing data with a third party without approval or transferring personal data outside of the jurisdiction where it's meant to reside).

› **Protects your business as well as your customers.** Allowing sensitive data to get into the wrong hands can have serious and material business consequences, whether it's large fines for not taking sufficient care of personal data or loss of revenue resulting from the theft of IP or strategic plans. The direct business benefits of stopping the exfiltration of data are obvious. But there's another positive effect: If your customers' data can't get stolen, they won't have to deal with the aftermath, which can be traumatic and long-lasting for those whose personal details are subsequently used to commit other crimes. Sparing your customers this inconvenience and distress can only be good for your reputation as a company to do business with.

› **Enables digital business transformation.** Digital businesses have no boundaries, and they exist wherever your customers, partners, and employees choose to connect and interact with your services. The disappearance of corporate perimeters increasingly applies to physical environments, too, as we outfit retail environments with Wi-Fi and beacons, equip elevators and air conditioning systems with sensors and the ability to "phone home," and connect machines on the factory floor in real time. While this ubiquitous connectivity increases the attack surface, Zero Trust enables you to manage the risk by, for example, creating microperimeters around internet-of-things (IoT) devices. A Zero Trust approach also makes it easier to connect or adjust services, which in turn increases agility and allows you to realize transformational potential.

**Recommendations**

## Use Zero Trust As An Opportunity To Transform Your Business

It seems paradoxical, but by never assuming trust in our technology architecture and operations, we actually make the reliability, dependability, and security of our organization more trustworthy for the customers that choose to engage with us, the citizens and patients that rely on us, and the partners that do business with us. These trusted relationships will fuel the success and growth of your organization. For CIOs and the security teams that report to them, Zero Trust represents an opportunity to move away from the "department of no" label to become an enabler of business transformation. To get the Zero Trust journey underway, CIOs should:

› **Position Zero Trust as a foundational business initiative, not a security project.** In addition to the business benefits arising from improved security and lower risk, Zero Trust puts in place an essential building block for any analytics initiative an organization might wish to embark upon: the understanding of what data you've got, where it resides, and who can handle it for what purpose.

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Align with the chief information security officer around Zero Trust.** CISOs and CIOs typically have different objectives and incentives, which can lead to conflict and finger-pointing. Zero Trust allows CIOs and CISOs to work toward a common goal and give the CISO a stronger story to share with the board. However, CISOs should report to the CEO, not the CIO; whether perceived or real, a CIO reporting line leads to a potential lack of transparency, which in turn can increase business risk.
- **Refuse to take "no" for an answer.** There are no legitimate business objections to Zero Trust security. You're not proposing to embark upon a potentially risky and costly rip-and-replace exercise; you'll be using off-the-shelf tools and existing skills. In other words, over time, you'll break the seemingly endless upward spiral of security expenditure and instead lower costs — but with much improved security.

> There are no legitimate business objections to Zero Trust security.

## 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 iPhone® and iPad®**
Stay ahead of your competition no matter where you are.

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

## Supplemental Material

### Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2016 was fielded in the March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services.

The Forrester Data Global Business Technographics Security Survey, 2015 was fielded in April through June of 2015 of 3,543 business and technology decision makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics provides demand-side insight into the priorities, investments, and customer journeys of business and technology decision makers and the workforce across the globe. Forrester collects data insights from qualified respondents in 10 countries spanning the Americas, Europe, and Asia. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

## Endnotes

[1] Source: "Target tech chief resigns as it overhauls security," CNBC, March 5, 2014 (http://www.cnbc.com/2014/03/05/target-chief-investment-officer-beth-jacob-resigns-in-wake-of-data-breach.html) and Clint Boulton, "Target Breach Fallout Shows CEOs, CIOs Share Cybersecurity Stakes," The Wall Street Journal, May 5, 2014 (https://blogs.wsj.com/cio/2014/05/05/target-breach-fallout-shows-ceos-cios-share-cybersecurity-stakes/).

[2] Examples of corporate data loss include: Evernote: 50 million records compromised in 2013; Living Social: 50 million records compromised in 2013; eBay: 145 million records compromised in 2014; Home Depot: 56 million records compromised in 2014; Chase: 76 million records compromised in 2014. Yahoo: Several breaches between 2014 and 2016, with over 1 billion user accounts compromised. Anthem: 80 million records compromised in 2015. One example of a nation-state attack is the OPM data breach in the US. Source: "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," United States House Committee on Oversight and Government Reform, September 7, 2016 (http://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf).

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

[3] Source: Andrew Saunders, "TalkTalk boss Dido Harding is stepping down," Management Today, February 1, 2017 (http://www.managementtoday.co.uk/talktalk-boss-dido-harding-handled-its-big-cyber-attack/leadership-lessons/article/1406542).

[4] Source: Clara Guibourg and Billy Ehrenberg, "TalkTalk share price plunges twice as deep as Sony, Carphone Warehouse, Barclays and EBay after cyber attacks," City A.M., November 13, 2015 (http://www.cityam.com/228714/talktalk-share-price-plunges-twice-as-deep-as-sony-carphone-warehouse-barclays-and-ebay-after-cyber-attacks).

[5] Source: Matt Burgess, "TalkTalk hack toll: 100k customers and £60m," Wired, February 2, 2016 (http://www.wired.co.uk/article/talktalk-hack-customers-lost).

[6] Source: "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," US Committee on Oversight and Government Reform, September 7, 2016 (https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf).

[7] See the Forrester report "No More Chewy Centers: The Zero Trust Model Of Information Security."

[8] See the Forrester report "Build Your Identity And Access Management Strategy."

[9] See the Forrester report "The Forrester Wave™: Privileged Identity Management, Q3 2016."

[10] See the Forrester report "Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14."

[11] See the Forrester report "Five Steps To A Zero Trust Network."

[12] See the Forrester report "The Forrester Wave™: Security Analytics Platforms, Q1 2017."

[13] See the Forrester report "The Eight Business And Security Benefits Of Zero Trust."

[14] Source: Scott Moritz, "Verizon Reaches Deal for Lowered Yahoo Price After Hacks," Bloomberg Technology, February 21, 2017 (https://www.bloomberg.com/news/articles/2017-02-21/verizon-said-to-reach-deal-for-lowered-yahoo-price-after-hacks).

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.