The Eight Business And Security Benefits Of Zero Trust

Business Case: The Zero Trust Security Playbook

by Chase Cunningham, David Holmes, and Jeff Pollard

September 25, 2019

Why Read This Report

In response to increasingly complex cyberattacks, security pros are devoting resources to granular aspects of their networks. This is understandable and necessary to a degree, but it's also a great way to lose sight of your ultimate goal: protecting customers and empowering the business. Zero Trust networks accomplish the dual tasks of deep, continuous data inspection across the network and lean operation and oversight — tasks that seem mutually exclusive in traditional networks. This report highlights the eight most significant ways Zero Trust boosts security and your business.

Key Takeaways

Network Security Starts And Ends With Visibility
Zero Trust gives you unprecedented visibility into your digital business, from network packets to applications. Visibility, detection, and prevention work together to secure your firm's most sensitive and valuable data assets.

Zero Trust Networks Have Breach Detection In Their DNA
The fundamental architecture of a Zero Trust network intercepts information in transit, inspects it, and deals with it according to rules that you've established. The continuous verification that Zero Trust structures build into your network allows security pros to detect breaches much faster than they would in traditional hierarchical networks, most often stopping them before intrusion occurs.

Zero Trust Strategy Drives Technology Adoption, Not The Other Way Around
The concept and practices of Zero Trust are composed of a focused and concise strategy. Often in cybersecurity, security professionals are motivated by the bells and whistles of a particular tool or technology. The decision to implement a Zero Trust network should instead be driven by achieving a strategic goal first and then deciding what technical assets fit that plan: Decide to work toward Zero Trust, then look for tech that meets your strategy.

The Eight Business And Security Benefits Of Zero Trust

Business Case: The Zero Trust Security Playbook

by Chase Cunningham, David Holmes, and Jeff Pollard
with Joseph Blankenship, Madeline Cyr, and Peggy Dostie

September 25, 2019

Table Of Contents

Related Research Documents

Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model

The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019

The Zero Trust eXtended (ZTX) Ecosystem

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

Security As Usual Is Bad Security And Bad For Business

Traditionally, the security team had no active role in conversations about organizational sustainability, revenue, profits, and executive competence. Those days are long gone, however, and security leaders need only look to the fallout from recent business and government cyberattacks for confirmation (see Figure 1).[1] In late 2017, Equifax's megabreach forced the CEO, CIO, and CISO to resign.[2] On July 29, 2019, Capital One, a top 10 US bank, announced that over 100 million accounts had been compromised by an attacker, leading to a class action lawsuit the following day.[3] These cyberattacks, breaches, and privacy abuses draw attention to: 1) the vulnerability of today's organizations to business- and brand-altering security failures and 2) the business' dependence on security outcomes.

FIGURE 1 Notable Hacks Of The Past Year

Corporation	Date made public	Industry	Impact
T-Mobile	August 2018	Telecommunications	T-Mobile said that more than 2 million people may have had their information stolen. T-Mobile alerted affected customers with text message notifications, informing them that hackers had accessed the names, billing ZIP codes, phone numbers, email addresses, account numbers, and account types of some customers.
British Airways	September 2018	Transportation	A large-scale hack on the British Airways website and mobile app compromised 380,000 passengers' personal identifying information as well as financial information. As a result, the Information Commissioner's Office (ICO), a data security watchdog in the UK, fined British Airways €183 million.
Facebook	September 2018	Social media	Nearly 50 million Facebook accounts were compromised by an attack in which attackers stole access tokens that allow users to stay logged into Facebook over multiple browsing sessions without entering their password every time.
Chegg	September 2018	Educational tech	Chegg reported to the SEC that it had discovered a security breach affecting over 40 million users. The attacker gained access to user names, email addresses, shipping addresses, and chegg.com passwords.
Google	October 2018	Tech	Up to 500,000 Google+ accounts were potentially affected by a software bug in the Google+ social network that exposed user information such as name, email address, occupation, gender, and age.
Marriott	December 2018	Hotel	Hackers had access to reservation systems of many of Marriott's hotel chains for four years, exposing the details of 500 million users' travel arrangements, names, addresses, phone numbers, email addresses, passport numbers, dates of birth, and gender. For some, they also stole payment card numbers and expiration dates.

FIGURE 1 Notable Hacks Of The Past Year (Cont.)

Corporation	Date made public	Industry	Impact
Quora	December 2018	Website	An adversary gained access to Quora's systems and stole the account data of approximately 100 million users. That includes personally identifiable information, as well as details about the actions of users on Quora itself, and data from other sites users linked to Quora accounts.
Dow Jones	March 2019	Finance	Due to an incorrectly configured and unsecured Elasticsearch database, a Dow Jones watchlist was publicly leaked containing more than 2.4 million individuals and organizations that its clients should consider "high-risk."
Facebook	March 2019	Social media	Hundreds of millions of Facebook users had their account passwords stored in plain text and which were searchable by more than 20,000 Facebook employees.
Georgia Tech	April 2019	Education	An unknown outside entity accessed a central database. Potentially affecting 1.3 million current and former students, faculty, and staff members at Georgia Tech, the exposed information included names, addresses, Social Security numbers, and birthdates.
Facebook	April 2019	Social media	More than 540 million records about Facebook users were publicly exposed on Amazon's cloud computing servers.
Bodybuilding.com	April 2019	Website	Hackers used the data they obtained from an employee phishing email to access the company's network, potentially accessing customer details including name, email address, billing/shipping addresses, phone number, order history, and anything included on profile for its 9 million users.

FIGURE 1 Notable Hacks Of The Past Year (Cont.)

Corporation	Date made public	Industry	Impact
Quest/ Labcorp	June 2019	Healthcare	A third-party data breach involving their vendor American Medical Collection Agency may have exposed the sensitive personal information of about 12 million customers. This includes credit card numbers, bank account information, medical details, and personal identity and contact details to include Social Security numbers.
Capital One	July 2019	Finance	A former Amazon employee was arrested and accused of carrying out a massive theft of 106 million Capital One records. This included 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers, and 80,000 bank account numbers, in addition to an undisclosed number of people's names, addresses, credit scores, credit limits, balances, and other information.
Poshmark	August 2019	Fashion platform	Profile information, including names and user names, gender, and city data was taken by an "unauthorized third party." Email addresses, size preferences, and scrambled passwords were also taken.

The Eight Business And Security Benefits Of Zero Trust

The Zero Trust Model of information security mitigates both attackers' ability to penetrate your network and their ability to wreak havoc on it.[4] Unlike traditional network infrastructures, Zero Trust enables the business while adapting the firm's security architecture to support new user populations (e.g., employees, partners, customers, and patients), customer engagement models, rapid cloud adoption, and new IoT devices and sensors. The model's effectiveness and efficiency are why more and more organizations are choosing to adopt Zero Trust for their next-generation security architectures.[5] There are numerous business and security benefits of deploying Zero Trust networks, but eight deserve the most focus.

No. 1: It Improves Network Visibility, Breach Detection, And Vulnerability Management

On September 7, 2017, Equifax revealed that it had suffered a massive security breach in which hackers stole the personal data of 143 million consumers.[6] The company discovered the breach on July 29 — months after the hackers had gained access to its critical systems and consumer data.[7] Unfortunately, Equifax is not alone in this: In breach after breach, we learn that it took weeks and months for security teams to detect the intrusion. With Zero Trust, security pros can:

- **Inspect all network traffic for malicious activity.** With Zero Trust, someone is watching; more specifically, your systems are watching, and continuous inspection is inherent to your network's DNA. In a Zero Trust network, security pros segment the network into microperimeters based on data sensitivity and place security controls as close as possible to the data itself — not out on the edge of the network. As a result, security controls, such as next-generation firewalls (NGFWs), not only enforce the segmentation but inspect all data flow. This ability to inspect all network traffic and packets through layer 7 (the application layer) provides security operations teams with visibility that would otherwise not exist.[8] There are also software-based solutions for microsegmentation from vendors such as Edgewise Networks, Illumio, and VMware that create secure zones in hybrid environments down to the workload level without requiring a hardware appliance.[9]

- **Prevent or limit the damage of data breaches.** Visibility is the key to defending any valuable asset. You can't protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the telltale signs of a breach in progress and to stop it. Today, many firms fail to detect an in-progress breach for weeks, even months, unable to limit the damage. In fact, in many instances, a third party (a customer, partner, or government agency) informs the firm of the breach. According to the FireEye M-Trends 2019 report, the median time to discover a breach is 78 days.[10] When cybercriminals remain undetected, they have unfettered access to steal as much customer and intellectual property as possible, increasing the scope, scale, and cost of the breach remediation.

- **Limit the pain of vulnerability management issues.** One of the most common avenues for exploit that results in a breach stems from outdated patches and poor vulnerability management. When networks and technology are developing and spreading as fast as they are in today's businesses, it's nearly impossible to keep ahead of the onslaught of vulnerabilities that lead to exploits. Embracing a Zero Trust strategy and implementation keeps the network segmented and isolates areas of concern into manageable chunks. It enables the network and security teams to be more tactical in their patching and vulnerability management protocols. This is critical considering that software exploits are the primary method of external attack: In 2018, over 16,500 vulnerabilities were added to the national vulnerability database.[11] Doing this one thing better can vastly improve the protections that your networks need to be safer and reduce the risk of future breaches.[12]

No. 2: It Stops Malware Propagation

Zero Trust networks have an inherent ability to stop the spread of malware. In a traditional network, malware travels through the existing routing and switch architecture, typically guided by a malicious actor through the command and control (C&C) channel. Malware typically requires a human being on the other side of the C&C connection to guide the malware through the network — but not always. The WannaCry ransomware and its derivatives affected organizations in more than 150 countries, including the US city of Atlanta, which was paralyzed for more than a week, eventually costing $17 million in mitigation and recovery.[13] With Zero Trust, security pros can:

- **Prevent malware propagation between critical systems.** In a Zero Trust network, security pros create microperimeters around specific data types, assets, services, and applications, making it harder for malware to propagate.[14] Each microperimeter uses microsegmentation software or hardware-based security controls such as a NGFW to enforce segmentation and inspect the traffic. This prevents the easy spread of malware. For example, assume an employee, partner, or contractor in your network clicks on a phishing link. That malware would have more difficulty moving into a Zero Trust network than a traditional one, because each microperimeter requires layer 7 inspection of all inbound traffic. Inspection will trigger alerts on potentially malicious traffic if certain rules/thresholds are met. Because traditional networks typically just use layer 3 firewalls, they lack the full packet visibility to stop the advanced threat traffic that firms face. Additionally, Zero Trust network rules are more granular and thus more likely to stop malicious activity.
- **Prevent malware propagation between users and critical systems.** Malware can still enter a Zero Trust network, and many security pros worry about it originating from well-intentioned employees. Let's say an employee brings a corrupted USB drive from home and plugs it into one of your corporate machines, infecting that machine. If you have a Zero Trust network, it would be difficult for the malware to propagate from that machine to a machine in another microperimeter. There would be no outbound rules allowing malware to connect to its C&C channel or move out of the microperimeter into the heart of the network.

  In 2016, Banner Health suffered a breach of 3.7 million records from patients, health plan members, café customers, and healthcare providers. The breach began with a POS compromise in the café, but the attackers were then able to access protected health information (PHI).[15] In a Zero Trust network, security teams would segment any device or network into its own microperimeters to prevent malware from jumping to other segments.

No. 3: It Reduces Both Capital And Operational Expenditures On Security

Your old, 20th-century network is likely a mess, and you have spent a tremendous amount of money adding controls to patch holes and manage its complexity. This strategy used to be called "defense in depth," but in practice it became "expense in depth" — an exercise wherein more and more appliances and software are layered onto one another with the hope of blindly preventing unknown threats. This is a poor strategy for protecting specific data and the applications using it. With Zero Trust, security pros can:

- **Consolidate multiple, disparate security controls from across the network.** Technological advancements mean that security pros have the option to consolidate multiple security functions into a single platform such as a NGFW. Security pros frequently use NGFWs to enforce microperimeters in Zero Trust environments. This translates into significant cost savings as multiple security controls are brought together into a single virtual or physical appliance. NGFWs combine traditional stateful firewall capabilities, advanced intrusion prevention functionality, and advanced malware analysis features into a single solution with a single management console.

- **Reduce management costs.** In addition to centralizing the location of security tools, Zero Trust also reduces expenditures by centralizing security management. In a traditional network, each security control has its own management interface or consoles, so operational, maintenance, and training costs soar. By reducing the number and types of controls, Zero Trust reduces the number of management consoles the network needs. Security employees spend less time on management and more on substantive security activities. Remember, hackers don't accommodate for "change management." They will take over your network as quickly and completely as they can, and it's your security team's responsibility to respond with strength and agility.[16]

No. 4: It Reduces The Scope And Cost Of Compliance Initiatives

Segmenting your network typically reduces the scope of compliance initiatives for your organization because many regulations only have certain data types in scope. A good example is PCI, which states, "Without adequate network segmentation (sometimes called a 'flat network'), the entire network is in the scope of the PCI DSS assessment."[17] With Zero Trust, security pros can:

- **Reduce the scope of industry regulations.** The Payment Card Industry Data Security Standard (PCI DSS) set a de facto standard: Once a network has been properly segmented, only the relevant network segment is in scope for a given regulation. Zero Trust networks are segmented by default: Segmentation of the network at layers 2 through 7 is a design paradigm of Zero Trust. In addition, Zero Trust networks go beyond VLANs for segmentation, frequently using physical or virtual security controls for enforcement.

- **Ease the pains of compliance audits.** The concise logic of a Zero Trust network facilitates audits: Most audit requirements focus on remediating the shortcomings of hierarchical network structures and, thus, are not applicable to Zero Trust networks. One enterprise tech firm CISO told us that the Zero Trust network he had deployed "is fairly easy for an auditor to conceptualize." His internal auditors had reviewed the network and had no audit findings that year. This is because the network was properly segmented, and the scope of the audit was smaller and less complex. Many of the things auditors look for are inherent to Zero Trust.[18]

No. 5: It Eliminates Intersilo Finger-Pointing

In almost every technology organization, CIOs have numerous silos: network teams, operations teams, storage teams, computing/virtualization teams, application development teams, security teams, and so on. Each has a different set of priorities and incentives that drive them and that naturally conflict with the drivers for other teams. This becomes most noticeable when incidents such as network downtime occur. Suddenly, the veneer of interteam cooperation is stripped away. That's when the finger-pointing starts. The network team blames security, and security blames networking. Zero Trust forces technology organizations to break down the barriers between various teams. With Zero Trust, security pros can:

› **Foster close relationships with other technology teams.** A result could be that networking and security teams focus on secure networking instead of on their individual domains. When WestJet began its Zero Trust journey, it found that breaking down interdepartmental silos was a significant and unexpected outcome of its Zero Trust deployment. The company built a center of excellence (CoE) that required collaboration between various teams to solve technical and business problems using Zero Trust processes and design. A representative stated: "The purpose of the CoE was to serve as a resource for technical ideas and knowledge sharing. This group helped build a bridge between the architects and the implementers, as well as between the different silos of technology management."

› **Break down interdepartmental silos.** A Zero Trust network inevitably leads to more cooperation and less finger-pointing, since the visibility and transparency of the solution provides significant insight into any issues that might arise. By breaking down their traditionally siloed approach, organizations can become more agile and develop a more mature technology management structure.

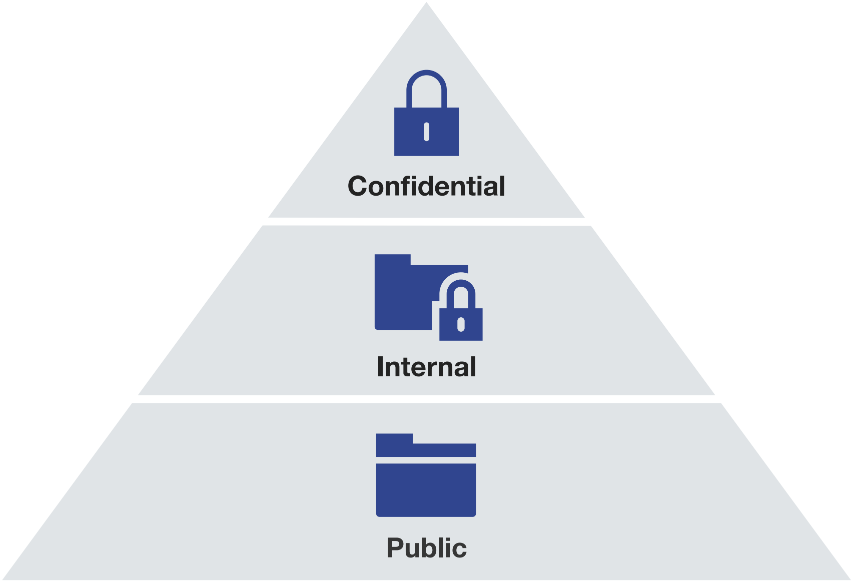
No. 6: It Increases Data Awareness And Insight

Just as your Zero Trust network will give you visibility into potential threat traffic, it can give you insight into your data and how it moves on your network. Because Zero Trust allows you to see everything inside your network's packets, you can detect the types of data in transit and track their journey in your network.[19] With Zero Trust, security pros can:

› **Support data privacy initiatives.** In the pursuit of customer loyalty, data security and privacy have taken on new importance because they underpin trusted customer relationships.[20] As customers have become increasingly sensitive to how firms collect, store, and use their PII, governments around the world have responded with tough privacy regulations. The penalty for the EU's General Data Protection Regulation (GDPR) is an eye-watering 4% of a firm's global turnover.[21] On the other side of the Atlantic, the United States Federal Trade Commission (FTC), in July of 2019, fined Facebook $5 billion for repeated privacy violations. The ability to map sensitive data flows throughout your business ecosystem can help you identify not only threats to the data but violations of privacy law (e.g., transferring or storing PII in a non-EU country) and the potential for privacy abuses (e.g., sharing data in an unapproved manner with a third party).

- **Accurately inventory and classify sensitive data.** Too often, security leaders set data policies without a clear understanding of feasibility and purpose within their business because they themselves are in the dark about their data — from what data they have to where it resides. However, discovering data can be very difficult. For security teams embarking on a data discovery and classification journey, the visibility and sight into the transmission and usage of your firm's most sensitive data can help significantly uplift data security programs. When you know what you have and where it is, you can develop the right policies and target your strongest security controls such as encryption to that data (see Figure 2).[22]

FIGURE 2 Zero Trust Networks Are Data-Centric



No. 7: It Stops The Exfiltration Of Sensitive Data Into The Hands Of Malicious Actors

Many security professionals confuse the terms breach and intrusion. An intrusion occurs when a nonapproved entity enters, or intrudes upon, the network. An intrusion is not a breach. A breach is a term of art defined by legal entities and regulations. A breach occurs when sensitive data (PII of customers or employees, regulated data, intellectual property) is exfiltrated from your networks or systems into the hands of malicious actors. Breaches are significant because of the business consequences. Top executives from major organizations such as Bangladesh Bank, Sony, and Target have been forced to resign as a result of breaches. The director of the US Office of Personnel Management resigned after the breach of more than 20 million records on government employees, contractors, and others.[23] The cost of these breaches is exorbitant, as well, totaling well into the billions of dollars. The settlement with the FTC alone cost Equifax $575 million.[24] Zero Trust is designed to stop data exfiltration. With a Zero Trust network, security pros can:

- **Protect the firm's intellectual property and future revenues.** When cybercriminals exfiltrate intellectual property, such as designs, formulas, road maps, and corporate strategy, it can lead to millions in lost revenues or even a permanent erasure of competitive advantage when competitors bring cheaper knock-offs to market.[25] It can also undermine long-term corporate strategy when competitors suddenly compete for acquisition targets. In 2019, 33% of security decision makers at firms that had experienced a breach in the preceding 12 months reported that intellectual property may have been compromised.[26] Codan, a metal detection and mining technology firm, had to cut prices on its metal detectors after hackers stole its designs and flooded the market with imitations.[27] Hackers stole sensitive information about Coca-Cola's potential $2.4 billion acquisition of China Huiyuan Juice Group.[28]

- **Protect customers from the emotional and financial toll of a breach.** Behind every breached customer record or incident of privacy abuse is someone who has to deal with the aftermath. Depending on what PII was involved, people will have to close and reopen financial accounts, reset all of their passwords, work with credit agencies to ensure their credit scores remain unaffected, etc. Complex identity theft can be much more painful to untangle, especially when criminals use PII to commit tax or medical fraud. Firms need to have robust breach response plans in place to deal with incidents responsibly and in a way that puts customers first, but it's far better to prevent the breach in the first place and spare your customers the anxiety and distress.[29] Customer frustration can also lead to years of class action lawsuits. Verizon paid $350 million less than its original offering to purchase Yahoo following Yahoo's data breaches; in addition, Verizon required Yahoo to split the cost of legal liabilities stemming from the breaches.[30]

No. 8: It Enables Digital Business Transformation

Today's digital business has no defined perimeter; your digital business lives everywhere your customers connect, your employees or partners interact with your services, and your data is used. As we extend our businesses into the cloud, outfit our retail locations with beacons, and digitize our physical environments with internet-of-things (IoT) components, a perimeter-based approach to security is completely ineffective — one could argue even negligent.[31] Zero Trust allows security pros to:

- **Become a partner in digital transformation.** In a perimeter-based approach to security, the security team earned a reputation as paranoid custodians because once they allowed access into the corporate perimeter in support of a new cloud service, partner, or customer engagement model, they were opening a door or connection to the entire corporate network. In a Zero Trust network where the security team has segmented apps and data into secure enclaves or microperimeters, security pros can quickly support new services with the appropriate granular privileges and data protection without inhibiting existing business and employee productivity. For example, WestJet was able to actualize its goal of increasing agility because its Zero Trust network made it easier to connect or adjust services.[32]

- **Accelerate the adoption of IoT.** Most IoT devices are connected to a network, which may be segregated but may also communicate with the firm's corporate network or the internet. Using these connections, hackers can launch large-scale attacks against the firm's own infrastructure and on other firms' resources.[33] With Zero Trust network segmentation plus explicit permissions, security pros can manage the risks of device proliferation. Proper segmentation and visibility provide telemetry that helps to categorize devices, expected operational parameters, and anomalies. Segmenting devices based on function (such as POS terminals versus medical imaging machines) can reduce the IoT attack surface.[34]

  As the CISO of a major US hospital lamented: "How can I implement a security policy for a connected medical device when I don't manage or control it? All I know is I have a big black hole in my network. I have knife-wielding robots, radiation, nuclear, and drug dispensers, all on my network — high-powered stuff that I own but don't manage."

Endnotes

[1] Source: Jennifer Calfas, "T-Mobile Says a Data Breach Is Affecting Millions of Its Customers. Here's What You Need to Know," Money, August 24, 2018 (http://money.com/money/5377773/tmobile-data-breach-august-2018/).

Source: Jordan Bishop, "380,000 Passengers Affected By 'Malicious' British Airways Hack," Forbes, September 9, 2018 (https://www.forbes.com/sites/bishopjordan/2018/09/09/british-airways-hacked/#4bfa2de467ae).

Source: Adam Smith, "British Airways Fined $229M for 2018 Data Breach," PCMag Asia, July 8, 2019 (https://sea.pcmag.com/news/33279/british-airways-fined-229m-data-breach).

Source: Julia Carrie Wong, "Facebook says nearly 50m users compromised in huge security breach," The Guardian, September 29, 2018 (https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach).

Source: Jordan Lutke, "Chegg Data Breach Affects 40 Million Customers," Security Today, September 28, 2018 (https://securitytoday.com/articles/2018/09/28/chegg-data-breach-affects-40-million-customers.aspx).

Source: Kate O'Flaherty, "Google+ Security Bug -- What Happened, Who Was Impacted And How To Delete Your Account," Forbes, October 9, 2018 (https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/#473b1b736491).

Source: Taylor Telford and Craig Timberg, "Marriott discloses massive data breach affecting up to 500 million guests," The Washington Post, November 30, 2018 (https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/).

Source: Brad Chacos, "Quora data breach FAQ: What 100 million hacked users need to know," PCWorld, December 4, 2018 (https://www.pcworld.com/article/3325199/quora-data-breach-faq-100-million-hacked-users.html).

Source: Adam Shepherd, "Terrorists and politicians exposed by Dow Jones data leak," IT PRO, February 28, 2019 (https://www.itpro.co.uk/data-breaches/33112/terrorists-and-politicians-exposed-by-dow-jones-data-leak).

Source: Brian Krebs, "Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years," Krebs on Security, March 21, 2019 (https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/).

Source: Chelsea Prince and Joshua Sharpe, "Data breach exposes up to 1.3M Georgia Tech faculty, students," Atlanta News Now, April 2, 2019 (https://www.ajc.com/news/breaking-news/breaking-data-breach-exposes-georgia-tech-faculty-students/zAUUNWy5hoHQ8bNvMxcsWL/).

Source: Jason Silverstein, "Hundreds of millions of Facebook user records were exposed on Amazon cloud server," CBS News, April 4, 2019 (https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/).

Source: Chris Grundy, "All Data Breaches in 2019 – An Alarming Timeline," SelfKey blog, June 12, 2019 (https://selfkey.org/data-breaches-in-2019/).

Source: Scott Ikeda, "Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed," CPO Magazine, June 11, 2019 (https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/).

Source: Rob McLean, "A hacker gained access to 100 million Capital One credit card applications and accounts," CNN Business, July 30, 2019 (https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html).

Source: Zack Whittaker, "Clothing marketplace Poshmark confirms data breach," TechCrunch, August 2, 2019 (https://techcrunch.com/2019/08/01/poshmark-confirms-data-breach/).

[2] Source: Jonathan Berr, "'WannaCry' ransomware attack losses could reach $4 billion," CBS News, May 16, 2017 (https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/); Chris Graham, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history," The Telegraph, May 20, 2017 (https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/); Ron Lieber and Stacy Cowley, "Trying to Stem Fallout From Breach, Equifax Replaces C.E.O.," The New York Times, September 26, 2017 (https://www.nytimes.com/2017/09/26/business/equifax-ceo.html); and Jennifer Surane, "Equifax Says CIO, Chief Security Officer to Exit After Hack," Bloomberg, September 16, 2017 (https://www.bloomberg.com/news/articles/2017-09-15/equifax-says-cio-chief-security-officer-to-leave-after-breach).

Source: Jeff Pollard and Joseph Blankenship, "Equifax Does More Than Credit Scores," Forrester Blogs, September 8, 2017 (https://go.forrester.com/blogs/equifax-does-more-than-credit-scores/). See the Forrester report "Ransomware Protection: Five Best Practices."

[3] Source: "Capital One Announces Data Security Incident," Capital One press release, July 29, 2019 (https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/).

[4] See the Forrester report "Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model."

[5] See the Forrester report "Future-Proof Your Digital Business With Zero Trust Security" and see the Forrester report "Jump-Start Zero Trust With Forrester's Reference Architecture."

[6] Source: Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, and Ron Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," The New York Times, September 7, 2017 (https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=0).

[7] Source: Michael Riley, Anita Sharpe, and Jordan Robertson, “Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed,” Bloomberg, September 19, 2017 (https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed).

[8] One of our goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. If S&R professionals look at everything from a data-centric perspective, we can design networks from the inside out and make them more efficient, more elegant, simpler, and more cost-effective. See the Forrester report “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture.”

[9] See the Forrester report “The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2018.”

[10] Source: “M-Trends 2019,” FireEye (https://content.fireeye.com/m-trends/rpt-m-trends-2019).

[11] See the Forrester report “The Forrester Wave™: Vulnerability Risk Management, Q1 2018.”

[12] See the Forrester report “Vendor Landscape: Vulnerability Management, 2017” and see the Forrester report “Introducing Forrester’s Prioritized Patching Process (P3).”

[13] Source: Benjamin Freed, “One year after Atlanta’s ransomware attack, the city says it’s transforming its technology,” StateScoop, March 22, 2019 (https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/).

Source: Alan Blinder and Nicole Perlroth, “A Cyberattack Hobbles Atlanta, and Security Experts Shudder,” The New York Times, March 27, 2018 (https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html) and Nick Statt, “Boeing production plant hit with WannaCry ransomware attack,” The Verge, March 28, 2018 (https://www.theverge.com/2018/3/28/17174540/boeing-wannacry-ransomware-attack-production-plant-charleston-south-carolina).

[14] For today’s digital business, perimeter-based security models are ineffective against malicious insiders and targeted attacks. Security and risk (S&R) pros must 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. See the Forrester report “No More Chewy Centers: The Zero Trust Model Of Information Security.”

[15] See the Forrester report “Lessons Learned From The World’s Biggest Data Breaches And Privacy Abuses, 2016.”

[16] Building a Zero Trust network is becoming easier because of several new technological innovations that have happened in the past few years. The network and security landscapes are quickly and dramatically changing. See the Forrester report “Three Technical Innovations Will Ignite Zero Trust.”

[17] Source: “Document Library,” Official PCI Security Standards Council Site (https://www.pcisecuritystandards.org/document_library).

[18] One of our goals with Zero Trust is to optimize the security architectures and technologies for future flexibility. As we move toward a data-centric world with shifting threats and perimeters, we look at new network designs that integrate connectivity, transport, and security around potentially toxic data. See the Forrester report “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture.”

[19] Too often, security and risk leaders create data policies without a clear understanding of feasibility and purpose within their business because they themselves are in the dark about their data. In today’s evolving data economy, data identity is the missing link that S&R leaders must define to create actionable policy. See the Forrester report “Develop Effective Security And Privacy Policies.”

Defining data via data discovery and classification is an often overlooked, but critical, component of data security and privacy. See the Forrester report “Rethinking Data Discovery And Classification Strategies.”

[20] See the Forrester report "Build A Data Privacy Organization That Balances Marketing Innovation And Customer Expectations."

"Privacy is dead": It's a trope so often repeated you might actually think it's true. But in the age of smartphones and sensors, privacy is not only possible, it's essential for building trust. See the Forrester report "The New Privacy: It's All About Context."

[21] Source: Fatemeh Khatibloo, "Countdown To The GDPR," Forrester Blogs, May 25, 2017 (https://go.forrester.com/blogs/17-05-25-countdown_to_the_gdpr_0/). See the Forrester report "Brief: You Need An Action Plan For The GDPR" and see the Forrester report "The Five Milestones To GDPR Success."

"Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher." Source: "Art. 83 GDPR – General conditions for imposing administrative fines," General Data Protection Regulation (GDPR) (https://gdpr-info.eu/art-83-gdpr/).

[22] See the Forrester report "Develop Effective Security And Privacy Policies."

[23] Source: Evan Perez and Wesley Bruer, "OPM Director Katherine Archuleta steps down," CNN Politics, July 11, 2015 (https://edition.cnn.com/2015/07/10/politics/opm-director-resigns-katherine-archuleta/index.html).

[24] Source: "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach," Federal Trade Commission press release, July 22, 2019 (https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related).

See the Forrester report "Estimate Breach Impact And Costs To Drive Investments."

[25] Source: Marcus Weisgerber, "China's Copycat Jet Raises Questions About F-35," Defense One, September 23, 2015 (https://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/).

[26] Base: 763 security decision makers with network, data center, app security, or security ops responsibilities whose firm had experienced a breach in the past 12 months. Source: Forrester Analytics Global Business Technographics® Security Survey, 2019.

[27] Source: "UPDATE 1-Australian metal detector company counts cost of Chinese hacking," Reuters, June 25, 2015 (https://www.reuters.com/article/china-cybersecurity-australia-pix-graphi-idUSL3N0ZB15O20150625).

[28] Source: Ben Elgin, Dune Lawrence, and Michael Riley, "Coke Gets Hacked And Doesn't Tell Anyone," Bloomberg, November 5, 2012 (https://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell?utm_source=Sinocism+Newsletter&utm_campaign=7b539f90bb-The_Sinocism_China_Newsletter_For_11_05_2012&utm_medium=email).

[29] See the Forrester report "Planning For Failure: How To Survive A Breach."

[30] Source: Seth Fiegerman, "End of an era: Yahoo is no longer an independent company," CNN Business, June 13, 2017 (https://money.cnn.com/2017/06/13/technology/business/yahoo-verizon-deal-closes/index.html).

[31] See the Forrester report "Future-Proof Your Digital Business With Zero Trust Security."

[32] Agility was the main goal of the organization. Zero Trust promotes agility because security is baked in from the get-go. As WestJet technologist Richard Sillito put it, "If you need to talk to that service, then hook up to that service. Why? Because we already put a security bubble around that service that is appropriate for its functionality." See the Forrester report "Case Study: WestJet Redefines Its Security With Forrester's Zero Trust Model."

[33] See the Forrester report "Vendor Landscape: Identity And Access Management Solutions For The Internet Of Things" and see the Forrester report "Top Cybersecurity Threats In 2017."

[34] See the Forrester report "The IoT Attack Surface Transcends The Digital-Physical Divide."

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.