No More Chewy Centers: The Zero Trust Model Of Information Security

Vision: The Security Architecture And Operations Playbook

by John Kindervag

March 23, 2016

Why Read This Report

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For today's digital business, this perimeter-based security model is ineffective against malicious insiders and targeted attacks. Security and risk (S&R) pros must eliminate the soft chewy center and 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. This report explains the vision and key concepts of the model.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

Perimeter-Based Network Security Models Fail To Protect Against Today's Threats

The trust model is broken; there are four critical pitfalls with today's approach to network security: It's impossible to identify trusted interfaces, the mantra "trust but verify" is inadequate, malicious insiders are often in positions of trust, and trust doesn't apply to packets.

Eliminate Chewy Centers With The Zero Trust Model

In Zero Trust, all network traffic is untrusted. This means that security professionals must ensure that all resources are accessed securely regardless of location, adopt a least privilege strategy and strictly enforce access control, and inspect and log all traffic.

Zero Trust Is Not A One-Time Project

Zero Trust is not a project but a new way of thinking about information security. By adopting the concepts of Zero Trust and the architectural components, organizations can become more secure in a way that eases compliance burdens and ultimately reduces costs.

No More Chewy Centers: The Zero Trust Model Of Information Security

Vision: The Security Architecture And Operations Playbook

by John Kindervag
with Stephanie Balaouras, Kelley Mak, and Josh Blackborow
March 23, 2016

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Build Security Into Your Network's DNA: The Zero Trust Network Architecture

Develop Your Road Map For Zero Trust Network Mitigation Technology

FORRESTER®

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

Wake Up: You Must Adapt To Sophisticated And Cunning Adversaries

On July 9, 2010, 10 seemingly ordinary people boarded a plane at New York's LaGuardia Airport bound for Vienna.[1] They weren't tourists heading for the historic old city. They were, in fact, confessed Russian spies expelled from the US for espionage. Unlike James Bond or Jason Bourne, these individuals were not obvious spies — in fact, they were, by my most accounts, extraordinarily ordinary. They were travel agents, consultants, newspaper columnists, and real estate brokers.[2] One spy even tested software for Microsoft.[3] They were so ordinary that one neighbor commented, "They couldn't have been spies. Look what she did with the hydrangeas."[4] There are some important lessons that security professionals can learn from this case:

- **Hackers, like spies, take extraordinary steps to hide their activities.** They may have looked like ordinary middle-class individuals, but they really worked for the Russian Foreign Intelligence Service known as the SVR.[5] According to the US Justice Department, the spies were in the US on long-term, deep-cover assignments, and they worked to hide all connections between themselves and the SVR. Similarly, today's hackers go to extreme measures to avoid detection and suspicion. And they're patient: Their security breaches are no longer audacious but "low and slow," meaning they collect valuable information from the network over long periods — weeks, months, or even years.

- **Example.** In September 2014, Home Depot confirmed that it was investigating a massive customer data breach after the influential security blog Krebs on Security reported that large batches of customers' credit cards had appeared for sale on Internet black markets. Not only did the popular retailer have no idea a breach had occurred until a third party clued it in, the breach had occurred months before.[6] According to Mandiant's M-Trends 2015 report, the average time to detect a breach is 205 days.[7]

- **Hackers, like spies, target specific organizations and individuals.** Press reports indicate that the spies were working to gain access to individuals in influential positions in the US government, including a former legislative counsel for the US Congress and a former high-ranking US government official in national security.[8] One of the agents even applied for work at prominent Washington, D.C., think tanks.[9] The agents had a clear mission: to search for and develop ties in policymaking circles in the US and to send intelligence reports home.[10] Similarly, security attacks are no longer indiscriminate. Hackers often target specific companies and organizations and even target the systems with the information they want — systems that contain personal and financial information or intellectual property.

- **Example.** From September 2014 through October 2015, the five largest breaches (based on the number of breached customer records) accounted for 77% of all breached records. This concentration demonstrates the targeted nature of today's cyberattacks.[11] Hackers carefully pick their victim organization to test for weaknesses and vulnerabilities. For example, between February and May 2015, hackers used in-depth knowledge of the multistep verification process of the IRS's Get Transcript app to gain access to the tax returns of approximately 104,000 individuals — and file $50 million in fraudulent tax returns.[12]

Wolves In Sheep's Clothing: S&R Pros Are Unprepared For Insider Attacks

Even as external threats continuously multiply and knock at our gates, some adversaries are already inside. Two of the most high-profile trust breaches in recent times — Chelsea (formerly Bradley) Manning/WikiLeaks and Edward Snowden/NSA — had international resonance and consequences.[13] The insider threat is not a new phenomenon, but these high-profile breaches have put a spotlight on the holes in our perimeter-based defenses. As enterprises transform themselves for digital businesses, S&R pros must understand the looming insider threat and tackle the data security challenge head on (see Figure 1).[14] How serious is the threat? Well, according to Forrester's Global Business Technographics® Security Survey, 2015, 52% of network security decision-makers who had experienced a breach reported that it was a result of an internal incident, whether it was within the organization or the organization of a business partner or third-party supplier.[15] Insiders have much easier access to critical systems and can often go about their malicious activities without raising any red flags. The main perpetrators are:

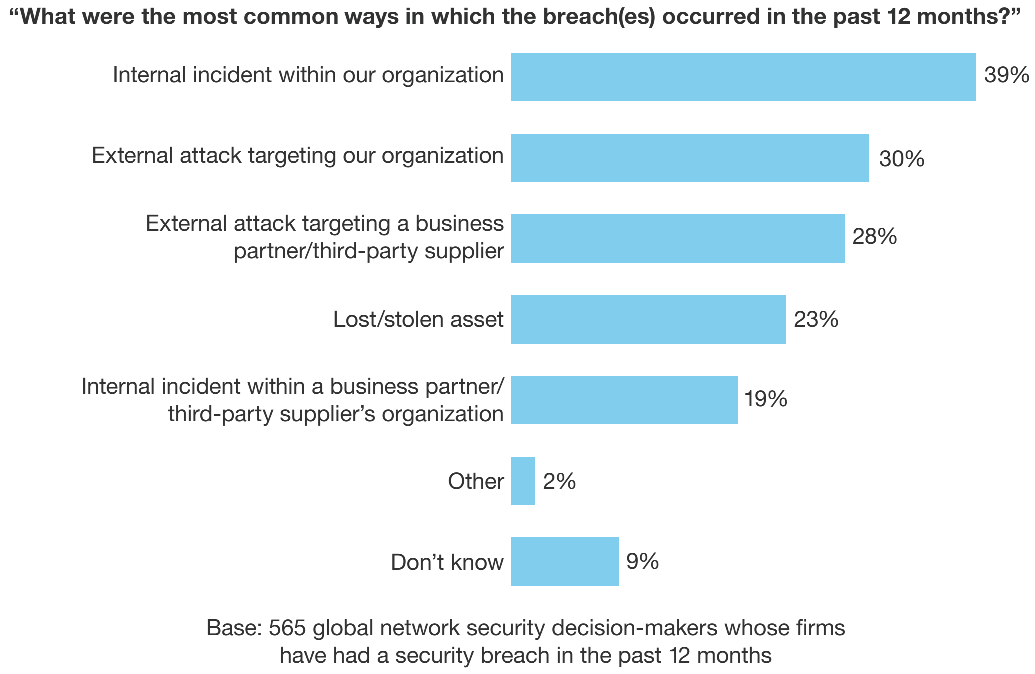
- **Financially incentivized cybercriminals.** Selling personally identifiable information (PII) and intellectual property (IP) is a thriving and lucrative market in the criminal underground.[16] In the past, organized-crime syndicates have enticed insiders to steal valuable customer PII that they could resell in the criminal underground.[17] There are other ways that malicious insiders can collude with external actors to monetize stolen data. In April 2015, the FCC announced that it had reached a $25 million settlement with AT&T to resolve charges stemming from the privacy breach of 280,000 US customers. In the breach, AT&T call center employees accessed and sold customer information to a third party as part of a scheme to unlock stolen or secondhand mobile phones for resale.[18]

- **Disgruntled employees.** Suffering a job loss is hard, and some will seek revenge. Matthew Keys was indicted in 2013 for allegedly providing credentials to the hacktivist group Anonymous after he was fired from Tribune Media. The group used his credentials to deface the Los Angeles Times' website.[19] In 2015, a former employee of Children's Medical Clinics of East Texas copied and shared the personal health information (PHI) of 16,000 with a third party. According to the health provider's investigation into the breach, the employee had "a retaliatory agenda against the clinic."[20]

- **Third parties.** Using legitimate access granted to them, third parties can maneuver into systems undetected and without setting off any alarms. As a US National Security Agency contractor, Edward Snowden leaked thousands of classified material from NSA databases using widely available web-crawling software.[21] Also, cybercriminals can use third parties as a stepping stone into a targeted company. In the 2013 Target breach, attackers gained access to Target's network using stolen credentials from an HVAC company that had worked at Target and other retail locations.[22] In 2015, CVS may have experienced a breach of its photo site. An investigation revealed that it was the firm's partner for credit card transaction processing to the site, PNI Digital Media, which suffered the breach.[23]

- **Employee misuse.** Data breaches are also the result of negligence and/or ignorance of the organization's security policies and regulations. Forrester's Global Business Technographics Security Survey, 2015 shows that 52% of insider breaches were either accidental or the result of inadvertent misuse.[24] In 2014, an employee at Rady Children's Hospital in San Diego accidentally sent out the PHI of 14,100 patients to potential job applicants.[25] Social media is another vector for accidental disclosure of sensitive data or of information that reflects poorly on the company — especially if the firm lacks clear policies, guidance, and education for employees.[26] Even employees that should know better can make mistakes. In November 2014, the CFO of Twitter accidentally tweeted about a potential M&A deal.[27]

FIGURE 1 The Most Common Breach Vector Is From The Inside



Source: Forrester's Global Business Technographics® Security Survey, 2015

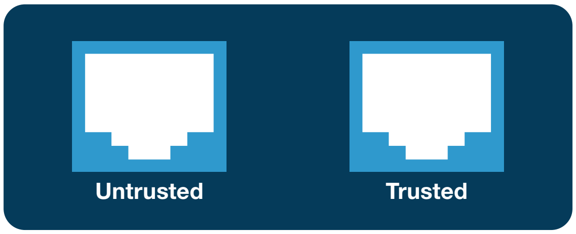
S&R Pros Must Recognize The Pitfalls Of A Broken Trust Model

In light of insider incidents and insider-enabled incidents, clearly something is fundamentally broken in the world of information security. Even though we have a plethora of controls (22 main controls in network threat mitigation alone), attackers continually develop new attacks that our expensive security controls can’t stop. Forrester research shows that a new threat landscape has emerged in which organized crime, nation-states, and hacktivists are creating more significant, targeted attacks.[28] Unfortunately, there are four critical pitfalls with today’s approach to network and information security.

Pitfall No. 1: It’s Impossible To Identify Trusted Interfaces

Almost every security device, such as a firewall, comes with at least one port labeled “untrusted” and another labeled “trusted” (see Figure 2). The assumption that security professionals can easily identify which network interfaces they can trust is a part of the very design of the security device. However, as history illustrates, automatically assuming that you can trust anyone or any device inside your organization’s network perimeter is a mistake. In today’s threat environment, do you connect the Internet into the untrusted port or the trusted port? Do you connect the internal network into the untrusted port or the trusted port?

FIGURE 2 Trusted And Untrusted Interface Ports On Today’s Security Appliances



Pitfall No. 2: The Mantra ‘Trust But Verify’ Is A Joke — Literally

Many security professionals have adopted the mantra “trust but verify.” However, Forrester has found that most security professionals trust a lot but verify very little. By default, we trust people, but it’s hard to perform the verification, so we don’t do it. In addition, there’s a fundamental misunderstanding of the meaning of the phrase. “Trust but verify” comes to our vocabulary from a speech given by President Ronald Reagan to commemorate the signing of a historic nuclear weapons treaty between the United States and the Soviet Union. By reading the transcript of the speech, we can gain a correct understanding of what it meant and how our industry has misunderstood the context:

> “The President (Ronald Reagan): But the importance of this treaty transcends numbers. We have listened to the wisdom in an old Russian maxim. And I’m sure you’re familiar with it, Mr. General Secretary, though my pronunciation may give you difficulty. The maxim is: Dovorey no provorey — trust, but verify.

> The General Secretary (Mikhail Gorbachev): You repeat that at every meeting. [Laughter]
>
> The President: I like it. [Laughter]"[29]

Note that both world leaders laugh as Reagan recites the old Russian proverb. The success of the treaty was not built on trust at all, but on verification. Reagan and Gorbachev clearly understood that each nation would watch the other very closely. There was no trust. In the security world, we have adopted the reverse as our actual security practice — we trust by default and never verify.

Pitfall No. 3: Malicious Insiders Are Often In Positions Of Trust

According to our surveys, 48% of network security decision-makers whose firm had a security breach due to internal incidents in the past 12 months said the breach occurred, at least partially, because of abuse or malicious intent.[30] Security teams treat employees as trusted users by default and without ongoing verification. Unfortunately, malicious insiders can take advantage of this flawed "trust but verify" approach to security. As a result, breaches where a person — a trusted user — has committed a crime or insidious act deliberately have become all too common. Malicious insiders can:

› **Embezzle funds and commit identity theft.** In 2009, the US Justice Department sentenced Cynthia Whitehead, a branch manager for Randstad North America, an international staffing firm, to more than five years in federal prison on charges of wire fraud and related identity theft. We highlight this case from 2009 because it is a classic example of how a malicious insider can exploit a strong position of trust for her own financial benefit and get away with it for years because no one was verifying her activities. Acting US Attorney Sally Quillian Yates identified trust as one of the root causes of this crime. According to the Justice Department:

> "Because of the position of trust Whitehead held with the company, she had access to corporate records, including personal identifiers of former employees and the mechanism for paying wages. Whitehead reactivated the employment status of more than a dozen former employees in the company's data system, made entries which falsely showed that these former employees were currently working for Randstad clients, arranged for the payment of their wages, and accessed the company's payroll accounts to collect those wages for herself. Over a three-year period, Whitehead embezzled approximately $300,000."[31]

› **Steal and disseminate sensitive intellectual property.** Since 2009, the number of breach cases involving the activities of so-called "trusted" insiders have continued to pile up. In 2010, Chelsea Manning, a 22-year-old US Army intelligence analyst stationed in Iraq, used her nearly unrestricted access to the United States Department of Defense Network to download thousands of sensitive military and Department of State documents.[32] Edward Snowden has been leaking sensitive NSA data to the public since 2013.

› **Compromise the privacy of sensitive customer records.** In January 2014, authorities revealed that a security breach had affected the personal information of 40% of the South Korean population, the result of a trusted IT contractor who was able to download millions of customer records to removable media over the course of a year and a half.[33]

Pitfall No. 4: Trust Doesn't Apply To Packets

If we can't always trust the people we have hired or contracted, why would we ever trust data flowing across our network? If you look at a network — packets moving from point A to point B — why are we even talking about trust? Trust is not an idea that we should anthropomorphize for computing. When we do, it reveals several problems:

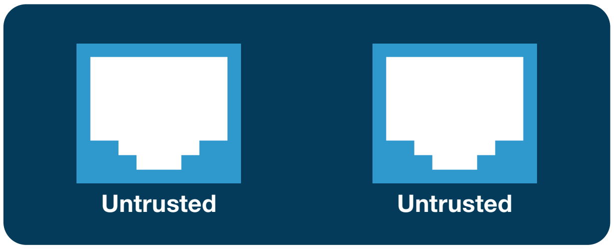
› **It's impossible to know with absolute certainty who is on our networks.** There is a flawed assumption that we know who is originating the traffic on our networks. We call this identity. In computer systems, identity is ultimately unknowable — meaning, you can't be 100% confident about the identity of the users or device. Technology management professionals assert identities based on IP addresses, MAC addresses, and how someone logged into the domain. However, attackers can easily discover IP and MAC addresses, and they can easily hack or guess a user's password.

› **Network identity is limited to the information that one can derive from packets.** Identity at the network level is merely an assertion of certain attributes that may be true or false, forged or real. But all we can truly know about network traffic is what is contained in packets, and packets can't tell us about the veracity of the asserted identity, let alone the intentions or incentives of the entity generating the packets. Therefore, packets can't trust and we can't trust packets. This is the ontological problem that information security professionals must confront.

No More Chewy Centers: Understanding The Zero Trust Model

If the current trust model is broken, how do we fix it? It requires a new way of thinking. The way we fix the old trust model is to look for a new trust model. Forrester calls this new model "Zero Trust." The Zero Trust Model is simple: Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted (see Figure 3). Thus, security professionals: 1) must verify and secure all resources; 2) limit and strictly enforce access control; and 3) inspect and log all network traffic. These are three fundamental concepts of our Zero Trust Model.

FIGURE 3 In Zero Trust, All Interfaces Are Untrusted



Concept No. 1: Ensure All Resources Are Accessed Securely Regardless Of Location

When you eliminate the concept of trust from the network, it becomes natural to ensure that all resources are securely accessed — no matter who creates the traffic or from where it originates. In the Zero Trust Model, security professionals must:

- **Assume that all traffic is threat traffic until determined otherwise . . .** You must make this assumption until you can verify that the traffic is authorized, inspected, and secured. In real-world situations, this will often necessitate using encrypted tunnels for accessing data on both internal and external networks. Cybercriminals can easily sniff unencrypted data; thus, Zero Trust demands that security professionals protect internal data from insider abuse in the same manner as they protect external data on the public Internet.[34]
- **. . . regardless of location or hosting model.** This is especially important as we move to a cloud-enabled technology environment where much of the data sits outside of our traditional data centers. Also, Zero Trust is helpful in enforcing data-residency issues related to the new data privacy regulations emerging around the globe. Zero Trust networks are data-centric and have powerful embedded data control mechanisms.[35]

Concept No. 2: Adopt A Least Privilege Strategy And Strictly Enforce Access Control

The next concept in Zero Trust is access control. When we properly implement and enforce access control, by default we help eliminate the human temptation to access restricted resources. For example, in 2013, prestigious Los Angeles hospital Cedars-Sinai fired six employees after they accessed the PHI of 14 patients, which included one high-profile celebrity.[36] Not only can strict access control help protect against malicious attacks, but it will keep embarrassing and possibly even life-threatening incidents from happening. S&R pros must:

- **Provide role-based access controls for all employees.** Today, role-based access control (RBAC) is a standard technology supported by network access control and infrastructure software, identity and access management systems, and many applications. With RBAC, security professionals place users into a role and based upon that role they are allowed access to certain specific resources. Zero Trust does not explicitly define RBAC as the preferred access control methodology. Other technologies and methodologies will evolve over time. What's important is the concept of minimal privileges and strict access control.[37] It's also important that the security pros have an appropriate identity and access governance strategy in place to periodically review and recertify employees' access rights.
- **Implement privileged identity management (PIM) for access to sensitive systems.** Employees that have administrative access to sensitive applications and systems can wreak havoc for a firm if they have malicious intent. They can delete sensitive data or even entire systems and they can download sensitive data. They are also often the target of hackers hoping to compromise their credentials for their own ends. PIM solutions allow security pros to closely monitor the activities of these users and require them to check out passwords to gain access to sensitive systems.[38]

Concept No. 3: Inspect And Log All Traffic

In Zero Trust, someone will assert their identity and then we will allow them access to a particular resource based upon that assertion. We will restrict users only to the resources they need to perform their job. But Zero Trust does not stop there; it requires S&R pros to:

› **Continuously inspect user traffic for signs of suspicious activity.** Instead of trusting users to do the right thing, we verify that they are doing the right thing. To do this we simply flip the mantra “trust but verify” into “verify and never trust.” By continuously inspecting network traffic, security pros can identify anomalous user behavior or suspicious user activity (e.g., a user performing large downloads or frequently accessing systems or records he normally doesn’t need to for his day-to-day responsibilities).

› **Continuously log and analyze all network traffic.** Zero Trust advocates two methods of gaining network traffic visibility: inspection and logging. Many security professionals do log internal network traffic, but that approach is passive and doesn’t provide the real-time protection capabilities necessary in this new threat environment. Zero Trust promotes the idea that you must inspect traffic as well as log it. Based on our experiences and evidenced by such data breaches as Heartland Payment Systems, the US Military Central Command attack, and even the 2013 Target attack, Forrester believes that there is very little inspection of internal network traffic.[39] Zero Trust network topology makes it easier to send traffic and logs to security analytics tools for deeper analysis.[40]

Zero Trust Requires Network Analysis And Visibility

In Zero Trust, we inspect and log all traffic internally as well as externally, regardless of location or hosting model. We’ve been so worried about the perimeter, we’ve forgotten about the malicious user on our internal network. In today’s network, companies have focused their controls on the perimeter, and now is the time to add controls on the internal network as well as the external network. Once there are appropriate controls deployed throughout the entire network, security professionals must then log that data so we see all the traffic that is traversing our network.

Deploy NAV As Part Of Your Security Analytics System

To do this Forrester recommends deploying network analysis and visibility (NAV) tools in conjunction with your security analytics platform.[41] For many security teams, their traditional security information management (SIM) system is their security analytics platform. NAV includes network discovery tools, tools that analyze flow data, tools that dissect packet captures, tools that look at network metadata, and tools used for network forensic examination.[42] This insight will not only help you identify suspicious traffic, it will also help you understand how sensitive data flows through the enterprise — one of the requirements of Forrester’s Data Security And Control Framework.[43] The purpose of NAV solutions is twofold; it:

- **Gives security professionals insight into the network.** One purpose of NAV is to give security professionals insight into what is actually going on in their network and verify access and behavior on the network. There is an assumption that we need to monitor all applications individually in order to know who is accessing each application and what actions users have taken on the application. However, implementing various controls and agents on each application in a large organization is not scalable. Luckily, in order for an application to work, traffic must traverse the network. It is much easier and more efficient to reconstruct and review what is happening on the application level by analyzing network traffic than it is to try and monitor hundreds or even thousands of individual applications.

- **Sends a message to potential malicious insiders.** Once you deploy NAV, tell people that you're going to be watching what they do. This will change behaviors. If individuals know that security is monitoring their actions, they will be less tempted to take questionable actions. If hospital employees know that the security team is monitoring and logging all user activity, they will be far less tempted to access the medical records of celebrity patients.

- **Will integrate with your security analytics platform to provide better breach detection.** Forrester defines security analytics (SA) as the convergence of the correlation and reporting capabilities of SIM together with information feeds from a variety of security solutions including NAV, user behavior analytics (UBA), data loss prevention (DLP), etc. In the future, as SA platforms continue to mature and increase in functionality, they may supplant standalone NAV solutions. The ability to correlate suspicious traffic together with behavioral anomalies will help security pros identify the tell-tale signs of an in-progress breach.

Zero Trust Enables Digital Business

Most enterprises, from online retailers to hospitals to government agencies, rarely work in isolation and can rarely confine their processes, applications, and data within the traditional perimeter of the organization. The perimeter no longer exists. They must work in a complex ecosystem of powerful customers increasingly concerned about their privacy, digitally native employees, and potentially hundreds of demanding partners and suppliers — all perpetually connected by new systems of engagement and cloud services. Zero Trust allows security pros to:

- **Embrace deperimeterization.** The task for security is not to fight deperimitization but to establish oversight, mitigate risks, and consequently provide consistent, long-term support for today's digital business. Zero Trust is a data- and identity-centric model. In it, we recommend that you segment your networks into microperimeters where you can granularly restrict access, apply additional security controls, and closely monitor network traffic based on the sensitivity of the systems and data within the microperimeter. With this approach, an initial breach of the perimeter doesn't give hackers free reign across the entire environment.

- **Support new business demands.** Zero Trust also gives security pros the flexibility to support new business demands such as providing partner access to certain systems, adopting cloud services to accelerate development, or streamlining customer-facing services. When WestJet wanted to integrate its rewards program, vacations program, advertising mail, and the rest of its guest services into one service, the complexity of managing a huge number of firewall rules and traffic routes in the current network was overwhelming. Therefore, WestJet worked closely with application owners to define and segment the network into microperimeters.[44] It not only solved the current challenge but now technology management and security teams can easily meet future requests.

- **Adapt to future digital disruption.** Organizations are already using Zero Trust networks to address the challenges of the future. Zero Trust is especially useful in protecting the Internet of Things. For example, an APAC utility is using Zero Trust networking to build microperimeters around smart meters. Manufacturers are using Zero Trust networks to protect computers that control manufacturing lines. These systems may be significantly outdated and unfortunately, security teams can't update them because of the specialized nature of the systems they control. Zero Trust builds secure microperimeters around these older systems and segments them away from the organization's highly sensitive data, thereby reducing the chances that one of these systems might be a vector for a larger data breach.

Recommendations

Zero Trust Is Not A One-Time Project

We designed Zero Trust to provide a new conceptual model for information security that includes modern threats and anticipates the need for changes in the future. We designed it to be incremental and nondogmatic. Its purpose is to help create a new dialogue and reframe the challenges regarding the future of information security that can lead to actionable and effective solutions. But to do this we must first attack the fundamental flaw in information security — trust. Thus, Zero Trust is not a project but a new way of thinking about information security. By adopting the concepts of Zero Trust and the architectural components, we believe that S&R professionals can make their organizations more secure in an efficient way that not only eases compliance burdens and ultimately reduces costs, but also helps the business build trusted relationships with its customers and allows it to pursue new business and technology opportunities in a more secure manner. As you embark on the Zero Trust journey, there are two steps that you can take now, both of which are free:

- **Step 1: Change how you and the entire organization think about trust.** This involves changing your thinking about trust models and becoming aware of the misuse of the word "trust" in relation to networking and security. Once attuned to how inappropriate trust is in the infosec realm, you can share the Zero Trust concept throughout the organization. The basic idea is simple and resonates with both infrastructure and operations and security and risk professionals. Use Zero Trust to begin dialogues among teams about the core concepts, but to make it a reality requires a cross-functional team that consists of architects and technicians from the network, security, and application teams.

› **Step 2: Integrate Zero Trust into future planning.** Forrester's clients are looking at issues such as network segmentation, cloud security, and compliance, which can all benefit from the ideas implicit in Zero Trust. Budgets intended for traditional security upgrades may well be more attractive and effective if done within the concept of Zero Trust. The network is at an inflection point, where compliance pressures and new technologies are creating a need to rethink current network and security deployments. Your cross-functional team needs to develop a Zero Trust strategy, road map, and technical details that you can present to the office of the CIO for final validation and funding.

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

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

Supplemental Material

Survey Methodology

Forrester conducted Forrester's Global Business Technographics® Security Survey, 2015, a mixed-methodology (phone and online) survey fielded in April and May 2014 of 3,305 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.

Each calendar year, Forrester's Business Technographics fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. 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. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

We have illustrated only a portion of survey results in this document. To inquire about receiving full data results for an additional fee, please contact data@forrester.com or your Forrester account manager.

Endnotes

[1] Source: Jim Heintz, Veronika Oleksyn, and Vanessa Gera, "Cold War redux: US, Russia swap 14 spies in Vienna," boston.com, July 9, 2010 (http://www.boston.com/news/world/europe/articles/2010/07/09/us_russian_planes_swap_14_spies_in_vienna/).

[2] Source: John M. Guilfoil, "How Russian spies blended into Cambridge," The Boston Globe, November 2, 2011 (https://www.bostonglobe.com/metro/2011/11/01/how-russian-spies-blended-into-cambridge/LpnMO6TyqHSEGJgtfkr0PN/story.html).

[3] Source: Charles Arthur, "Russian spy worked for Microsoft," The Guardian, July 14, 2010 (http://www.guardian.co.uk/technology/2010/jul/14/russian-spy-worked-for-microsoft).

[4] Source: Scott Shane and Charlie Savage, "In Ordinary Lives, U.S. Sees the Work of Russian Agents," The New York Times, June 28, 2010 (http://www.nytimes.com/2010/06/29/world/europe/29spy.html).

[5] In Russian: Sluzhba Vneshney Razvedki.

[6] Source: Brian Krebs, "Banks: Credit Card Breach at Home Depot," Krebs on Security, September 2, 2014 (http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/).

[7] Source: "M-Trends 2015: A View From The Front Lines," Mandiant, 2015 (https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf).

[8] "According to the FBI, some of the people the accused spies met with include a former legislative counsel for US Congress, a former high ranking US government national security official, a person working on bunker busting nuclear warheads, and a New York financier who is prominent in politics and a major fundraiser for an un-named political party." Source: Jason Ryan and Megan Chuchmach, "Russian Spy Ring Suspects Busted! 10 Alleged Secret Agents Arrested in U.S.," ABC News, June 28, 2010 (http://abcnews.go.com/Blotter/russian-spy-ring-10-accused-russian-spies-arrested/story?id=11037360&page=1).

[9] Source: Toby Harnden and Michele Walk, "Russian spy applied for jobs at think tanks with links to Obama," The Telegraph, July 8, 2010 (http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7879850/Russian-spy-applied-for-jobs-at-think-tanks-with-links-to-Obama.html).

[10] Source: "United States Of America -v- Anna Chapman, and Mikhail Semenko, Defendants," US Department of Justice, June 27, 2010 (http://www.justice.gov/opa/documents/062810complaint1.pdf).

[11] Breaking news of a massive customer breach dominates headlines for days. However, months and even years later, affected customers still struggle with the aftermath and firms are still absorbing the costs. By reflecting on these breaches, we can glean long-term lessons that help security and risk (S&R) pros improve their firm's overall security posture, its breach response, and its appreciation of privacy law and customer trust. To learn more, see the "Lessons Learned From The World's Biggest Customer Data Breaches And Privacy Incidents, 2015" Forrester report.

[12] On May 27, the US Internal Revenue Service (IRS) disclosed that cybercriminals had gained access to the tax returns of approximately 104,000 individuals. This breach is notable because it demonstrates how cybercriminals couple their business and financial savvy with in-depth knowledge of compromised consumer identities to commit high-value fraud, and to build on that foundation with more elaborate identity theft and fraud. To learn more, see the "Quick Take: Fifteen Lessons For Security & Risk Pros From The IRS Get Transcript Breach" Forrester report.

[13] Source: "Edward Snowden: Leaks that exposed US spy programme," BBC, January 17, 2014 (http://www.bbc.com/news/world-us-canada-23123964) and "Bradley Manning sentenced to 35 years in Wikileaks case," BBC, August 21, 2013 (http://www.bbc.com/news/world-us-canada-23784288).

[14] For more information, see the "The Mobile Mind Shift Index: Global" Forrester report.

[15] Source: Forrester's Global Business Technographics® Security Survey, 2015.

[16] For more information, see the "The Cybercriminal's Prize: Your Customer Data And Intellectual Property" Forrester report.

[17] During his employment at TeleData Communications (TCI), a provider of software for credit bureaus like Equifax, TransUnion, and Experian Information Solutions, Philip Cummings was offered $60 for each credit report provided to members of a Nigerian organized crime syndicate. The crime continued for years after Cummings was no longer an employee, and the financial impact was enormous. The US government estimates that Cummings and his criminal counterparts stole approximately 30,000 identities, resulting in a direct financial loss of at least $2.7 million. Source: "The Infamous History Of Identity Theft," Guard Privacy & Online Security (http://www.guard-privacy-and-online-security.com/history-of-identity-theft.html).

[18] Breaking news of a massive customer breach dominates headlines for days. However, months and even years later, affected customers still struggle with the aftermath and firms are still absorbing the costs. By reflecting on these breaches, we can glean long-term lessons that help security and risk (S&R) pros improve their firm's overall security posture, its breach response, and its appreciation of privacy law and customer trust. To learn more, see the "Lessons Learned From The World's Biggest Customer Data Breaches And Privacy Incidents, 2015" Forrester report.

[19] Source: Kim Zetter, "Judge Refuses to Dismiss Confession, Evidence in Reuters Employee Hacking Case," Wired, March 24, 2014 (http://www.wired.com/2014/03/matthew-keys-case/).

[20] Source: "16K children's medical records potentially stolen in east Texas," HIPAA Journal, November 11, 2015 (http://www.hipaajournal.com/16k-childrens-medical-records-potentially-stolen-in-east-texas-8178/).

[21] Source: Rory Carroll, "Snowden used simple technology to mine NSA computer networks," The Guardian, February 9, 2014 (http://www.theguardian.com/world/2014/feb/09/edward-snowden-used-simple-technology-nsa).

[22] Source: Brian Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 5, 2014 (http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/).

[23] Source: "CVS Photo Breach Points to Third-Party Vendor," Identity Theft Resource Center, July 24, 2015 (http://www.idtheftcenter.org/Data-Breaches/cvsphoto-breach-points-to-third-party-vendor.html).

[24] Source: Forrester's Global Business Technographics Security Survey, 2015.

[25] Source: Consumer Bob, "Data Breach at Rady Children's Hospital Exposes Thousands," NBC 7 San Diego, June 18, 2014 (http://www.nbcsandiego.com/news/local/Data-Breach-at-Rady-Childrens-Hospital-263738941.html).

[26] For more information on social risk and compliance, see the "The Forrester Wave™: Social Risk And Compliance Solutions, Q2 2014" Forrester report.

[27] Source: Sarah Frier, "Oops. Twitter CFO Inadvertently Leaks M&A Deal Intent in Tweet," Carrier Management, November 25, 2014 (http://www.carriermanagement.com/news/2014/11/25/132367.htm).

[28] For more information on recently emerged threat landscapes, see the "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities" Forrester report.

[29] Source: "Remarks on Signing the Intermediate-Range Nuclear Forces Treaty," Ronald Reagan Presidential Library, December 8, 1987 (http://www.reagan.utexas.edu/archives/speeches/1987/120887c.htm).

[30] Source: Forrester's Global Business Technographics Security Survey, 2015.

[31] Source: "Former Randstad Branch Manager Sentenced to Federal Prison for Embezzlement," US Department of Justice press release, September 16, 2009 (https://www.justice.gov/archive/usao/gan/press/2009/09-16-09c.pdf).

[32] Forrester's Zero Trust model of information security demands that organizations know what types of activities take place on their internal network as well as on their external network. Forrester has defined a new functional space called network analysis and visibility (NAV) to provide this type of deep insight into internal and external networks. For more information, see the "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" Forrester report.

[33] Source: Sophia Yan and K.J. Kwon, "Massive data theft hits 40% of South Koreans," CNN Money, January 21, 2014 (http://money.cnn.com/2014/01/21/technology/korea-data-hack/).

[34] Zero Trust builds upon the deperimeter ideas first socialized by the Jericho Forum. For more information, go to The Open Group website. Source: The Open Group (https://www.opengroup.org/jericho/index.htm).

[35] To help security and risk professionals navigate the complex landscape of privacy laws around the world, Forrester created a data privacy heat map that highlights the data protection guidelines and practices for 54 different countries. It also covers other relevant issues like government surveillance, cross-border data transfers, and regulatory enforcement. To learn more, see the "Forrester's 2015 Data Privacy Heat Map" Forrester report.

[36] Source: Anna Gorman and Abby Sewell, "Six people fired from Cedars-Sinai over patient privacy breaches," Los Angeles Times, July 12, 2013 (http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713).

[37] Increasingly, identity and access management (IAM) has become a tool not just for security but also business agility. Competitive challenges push businesses into the cloud and encourage mobile device use even without full-fledged access controls in place. These trends create pressing provisioning, authentication, and authorization challenges for S&R pros while compliance requirements and breaches and other security threats continue to swell. S&R pros should apply a Zero Trust information security model to IAM to unify and improve access control across the extended enterprise. See the "Navigate The Future Of Identity And Access Management" Forrester report.

[38] To learn more about important and emerging IAM technologies, see the "TechRadar™: Identity And Access Management (IAM), Q1 2016" Forrester report.

[39] A recent article in The Washington Post reports that the US Military's Central Command network was infected by "malicious code placed on the [flash] drive by a foreign intelligence agency [that] uploaded itself onto a network run by the US Military's Central Command." The story quotes a US Defense Department official saying the "code spread undetected on both classified and unclassified systems." Source: Ellen Nakashima, "Defense official discloses cyberattack," The Washington Post, August 24, 2010 (http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html?hpid=topnews).

[40] Forrester segments the problem of securing and controlling data into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data. We refer to this as our Data Security And Control Framework. To learn more, see the "Dissect Data To Gain Actionable INTEL" Forrester report.

[41] To learn more about important and emerging IAM technologies, see the "TechRadar™: Data Security, Q1 2016" Forrester report.

[42] The Zero Trust concept of NAV shares similarities with, and is indebted to, the idea of network security monitoring (NSM) as advocated by Richard Bejtlich in his book The Tao of Network Security Monitoring: Beyond Intrusion Detection. In the book, Bejtlich defines NSM as "the collection, analysis, and escalation of indications and warnings (I&W) to detect and respond to intrusions." Zero Trust adds packet inspection of all internal traffic to NSM and looks

beyond intrusion alerting to proactive discovery of all types of network abuse. Source: Richard Bejtlich, "Network Security Monitoring History," TaoSecurity, April 11, 2007 (http://taosecurity.blogspot.com/2007/04/network-security-monitoring-history.html).

[43] For more information on Forrester's Data Security And Control Framework, see the "Dissect Data To Gain Actionable INTEL" Forrester report.

[44] For a Zero Trust case study on WestJet, see the "Case Study: WestJet Redefines Its Security With Forrester's Zero Trust Model" Forrester report.

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.