Five Steps To A Zero Trust Network
Road Map: The Security Architecture And Operations Playbook
by Stephanie Balaouras, Chase Cunningham, and Peter Cerrato
October 1, 2018

Why Read This Report
A Zero Trust (ZT) architecture abolishes the idea of a trusted network inside a defined corporate perimeter. ZT mandates that enterprises create microperimeters of control around their sensitive data assets to gain visibility into how they use data across their ecosystem to win, serve, and retain customers. This report gives security and risk (S&R) leaders best practices and a five-step road map to realize the benefits of a Zero Trust strategy more quickly.

Key Takeaways

Zero Trust Is The Blueprint For Your Security Architecture
A secure structure needs a solid foundation. When building their security architecture, S&R pros must start with their fundamental needs and move outward. Use Forrester’s Zero Trust Model as the foundation for this security architecture.

Identify Your Data And Map Its Flow
Zero Trust starts with the data. The first steps to building a ZT security architecture are identifying your sensitive data and mapping its flow. Learning the who, what, when, where, why, and how of your firm’s data is imperative to create a more robust and nimble security architecture.

Create And Monitor Your Zero Trust Ecosystem
Base the design of your Zero Trust extended network on the way your transactions flow through your business ecosystem and how employees, customers, and applications access data. Use this information to isolate and protect your extended network, enforce access control and inspection policies, and continuously monitor your ZT ecosystem for signs of a breach or other malicious activity.
Five Steps To A Zero Trust Network
Road Map: The Security Architecture And Operations Playbook

by Stephanie Balaouras, Chase Cunningham, and Peter Cerrato
with Laura Koetzle, Madeline Cyr, Bill Barringham, and Peggy Dostie
October 1, 2018

Table Of Contents

2 Zero Trust Is The Blueprint For Your Security Architecture

4 Five Steps To Zero Trust Information Security
   Step 1: Identify Your Sensitive Data
   Step 2: Map The Flows Of Your Sensitive Data
   Step 3: Architect Your Zero Trust Microperimeters
   Step 4: Continuously Monitor Your Zero Trust Ecosystem With Security Analytics
   Step 5: Embrace Security Automation And Orchestration

Recommendations

10 Use Zero Trust To Unite Technology And Business Stakeholders

Related Research Documents

The Eight Business And Security Benefits Of Zero Trust
The Future Of Data Security And Privacy: Growth And Competitive Differentiation
Future-Proof Your Digital Business With Zero Trust Security
The Zero Trust eXtended (ZTX) Ecosystem: People

Share reports with colleagues.
Enhance your membership with Research Share.
Zero Trust Is The Blueprint For Your Security Architecture

Too many security teams fail to address the basic vulnerabilities that cyberadversaries target in their attacks. Foundational needs include a security strategy, dedication to recruiting and retaining staff, a focus on fundamental security, and an integrated security portfolio that enables orchestration. S&R leaders should:

› **Ensure you have a documented security strategy.** Your security strategy must document the scope of the security organization’s functional and technical responsibilities, structure, and staffing; describe the overall technical security architecture; and lay out the road map for capital and operating investments.

› **Use Forrester’s Zero Trust Model as the security architecture blueprint.** ZT is an architectural model for building secure microperimeters, using obfuscation to increase data security, curbing excessive user privileges to limit risk, and employing automation and analytics to improve security detection and response. It requires S&R pros to discard the idea of a trusted internal network and an untrusted external network. It demands that security teams verify and secure all resources regardless of location; limit and strictly enforce access control for all users, devices, channels, and hosting models; and log and inspect all internal and external traffic (see Figure 1).

› **... and apply it to the entire business ecosystem.** Apply ZT throughout the extended business ecosystem, including all hosting models, locations, users, and devices. If you don’t address mobile device and app proliferation, cloud service adoption, social media use, and third-party dependencies, you have no hope of detecting or responding to a targeted attack. An architectural approach will help you focus on the security of your data, workforce, and workloads (whether they run on-premises or in the public cloud).
Data-centric security is supported by integrated security functions and consolidated controls that form a security ecosystem.

- **Data control** — the ability to apply universal security policies to protect sensitive data regardless of location, device type, hosting model, or user population. This requires the ability to:
  - Inventory and classify data across networks, devices, and apps.
  - Encrypt data in flight to and at rest in any application, device, or network regardless of location.
  - Enforce access control across user populations, apps, and devices.
  - Apply and enforce declarative policy dynamically via APIs.

- **Intelligence** — combining real-time analysis and visibility with contextual information to identify threats, address vulnerabilities, and uncover incidents in progress. This requires:
  - Real-time analysis and visibility across networks, devices, apps, users, and data.
  - Contextual information about the user, transaction risk, and overall security state, such as traffic flows, device state, user identity and biometrics, behavior, app state, app classification, data classification, location, and time.
Five Steps To Zero Trust Information Security

While Zero Trust begins by redesigning network security, it’s fundamentally a data-centric model. Today, cyberadversaries steal data to sell in underground markets and intellectual property to sell to unscrupulous competitors. As digital businesses amass data on customers, markets, and their own operations to personalize marketing, develop new products and services, and make better decisions, data becomes both an opportunity and a threat. As society better understands the threat to individual privacy, lawmakers will enact regulations restricting data use. As business becomes more data-centric, so must security strategy, architecture, and networks. That’s why each of our five steps to Zero Trust focuses on data in some way.

Step 1: Identify Your Sensitive Data

You can’t protect what you can’t see. If you don’t know where your firm stores data; how employees, partners, and customers use it; who specifically uses it; and how sensitive it is; you’re depending on blind luck to protect you from a data breach. Before investing in security controls, identify the data you need to protect. Zero Trust starts at the data to ensure that S&R pros’ technology investments have a specific purpose and are not guided by expense-in-depth principles. S&R leaders must:

› **Identify and classify sensitive data.** By defining your data, you can identify sensitive data sources to protect. Forrester’s data security and control framework can help you get a handle on sensitive data and create a strategy for becoming more data-centric. Next, simplify your data classification. Many data classification policies are based on complex analog models of classifying documents that are impossible to implement. Prevent this by using Forrester’s simplified data classification model, which sorts data into three categories: public, internal, and confidential. Classifying data according to the way you will protect it can make your data classification project a reality (see Figure 2).

› **Segment the network based on data sensitivity.** When designing ZT networks, it’s important to do it in consumable chunks. Zero Trust is an object-oriented network design. The goal is to create small segments of network elements — microperimeters — that you can bind together to create a larger ZT network. When creating your first ZT microperimeter, start with a well-understood data type or system such as the HR system, which contains highly sensitive data in the form of employees’ personally identifiable information. If you’re a hospital or medical provider, start with your clinical systems; a pharmaceutical company, your drug discovery systems.
Step 2: Map The Flows Of Your Sensitive Data

You need to understand how data flows across your extended network and between resources and people: employees, partners, and customers (see Figure 3). To map transaction flows, engage multiple stakeholders: application architects to see how the application interacts with users; network architects to understand network interconnections; enterprise architects to pull everything together; and business reps to identify the business value of the application. Designing an HR ZT network, for example, would use a typical three-tiered application architecture: The web server tier provides the application interface to users; the app server tier translates web server requests into business logic; and the database server tier holds the sensitive data necessary for the application to function. As you begin mapping, the cross-functional ZT design team must:

› **Locate and map all dependent network and system objects.** In an HR system, for example, this means locating all of the network and system objects that a successful application needs. It’s not uncommon to discover legacy hardware or software in the flow. Mapping the application flow is useful for disaster recovery planning and can reveal sanctioned and unsanctioned third-party and cloud-service dependencies. In an HR system, this might include third-party identity verification services and employee due diligence services. The data flow mapping exercise can’t stop at the corporate perimeter: Sensitive data flowing to a third party requires security controls including encryption in flight and at rest.11
› **Design a more optimal flow if necessary.** Application flow mapping will show you how the application works today. The design team must take that version of the transaction flow and design an optimized version that disregards the current network state. Remember, you’re building a new micronetwork for this application that you will join with other elements to make a functioning application or technology service.\(^\text{12}\)

› **Leverage existing data and network flow diagrams.** The Payment Card Industry (PCI) Data Security Standard requires firms to create diagrams to help understand cardholder data flows and ensure that network segmentation isolates the cardholder data environment.\(^\text{13}\) You can use PCI cardholder data flow diagrams to help map your own sensitive data transaction flows. Many firms also undertake data flow mapping exercises as part of their efforts to comply with the EU’s General Data Protection Regulation, which took effect in May 2018. Data protection authorities across the EU have geared up to enforce these new data privacy protections for EU residents — including fines of up to 4% of a violator’s global revenues.\(^\text{14}\)

---

**FIGURE 3 Example Data Flow Mapping**

---

**Step 3: Architect Your Zero Trust Microperimeters**

Security architects will base the actual design of a Zero Trust network on how the transactions flow across the extended business ecosystem and how people and applications access sensitive data. Individuals can only use, abuse, or misuse data — so define and optimize a transaction path that characterizes proper data use and flags or denies transactions when someone is potentially abusing or misusing it. To do this:

› **Define microperimeters around sensitive data.** Once you determine the optimal flow, identify where to place the microperimeters. As the primary goal is to protect sensitive data, S&R pros usually create microperimeters around sensitive data repositories and systems of record (see Figure 4). The ability to create virtual networks via software-defined networking is useful in ZT design, but
it’s important to enforce the segmentation with a security control. Virtual networks are designed to optimize network performance; they can’t by themselves prevent malware propagation, lateral movement, or unauthorized access to sensitive data.

› **Enforce microperimeters with physical or virtual security controls.** There are multiple ways to enforce microperimeters. In some instances, you’ll want to use a physical or virtual NGFW from a vendor like Check Point, Cisco, Fortinet, or Palo Alto Networks. If you’ve adopted a network virtualization platform because you have a highly virtualized compute environment, opt for a virtual NGFW to insert into the virtualization layer of your network. You don’t always need a NGFW to enforce network segmentation; there are software-based approaches to microsegmentation from vendors such as Edgewise Networks, Illumio, Safe-T, ShieldX, and even established vendors such as Akamai and VMware.\(^\text{15}\)

› **Limit and strictly enforce access to microperimeters.** The Zero Trust approach requires you to minimize and strictly control this access. To define rules, the ZT design team must have a detailed understanding of user entitlements — fine-grained authorizations that dictate what kind of access a user has to a resource after authentication. Security teams also need a commercial solution for identity management and governance to frequently review and recertify these entitlements.\(^\text{16}\)

› **Automate the rule and policy base.** Zero Trust requires firms to define and enforce data security and access policies across hosting models, locations, users, and devices, requiring you to carefully define rules and policies within key security controls such as NGFWs, email and cloud security gateways, and DLP.\(^\text{17}\) These controls combine to enforce microperimeters that transcend hosting models and locations. While today you may have to go to each solution’s management console to do this, vendors are working on product integrations that automatically update policy and centralized consoles that define and update policies across products. Cisco’s Defense Orchestrator unifies policies across its NGFWs, web security appliances, and solutions that are part of Cisco Umbrella. Most security portfolio vendors are taking a similar approach.

› **Use auditing and change control tools.** If you’re using heterogeneous firewalls, one best practice is to use a firewall auditing and change control solution such as AlgoSec, FireMon, Red Seal, Skybox Security, or Tufin to continuously audit and optimize your NGFW rule base. Many security teams have a change control mechanism that provides a process for adding firewall rules but doesn’t delete expired rules. Don’t forget to look for unused rules in your policy; malicious actors could exploit these.
Step 4: Continuously Monitor Your Zero Trust Ecosystem With Security Analytics

Another core tenet of Zero Trust is to log and inspect all internal and external traffic for malicious activity and areas of improvement. S&R pros can use a variety of solutions to monitor the entire ecosystem for signs of malicious activity. Many security information management (SIM) solutions have evolved into robust security analytics (SA) solutions that can ingest and correlate not only logs but also data from disparate sources such as networks, applications, endpoints, and DLP and IAM solutions. Instead of relying solely on rules, SA uses data science techniques to detect unknown threats and complex attacks; the deeper context, built-in workflows, and embedded remediation capabilities dramatically improve investigations and response. To better monitor ZT environments:

› **Evaluate where you may already have SA.** Are you making the most of tools you already own? SIM vendors now include features like network analysis and visibility and security user behavior analytics (SUBA) — so ask your SIM vendor what functionality is available through your current solution. If you can avoid adding yet another product or interface, your security operations team will thank you.

› **Determine the best deployment model for your business.** If much of your business has already moved to the cloud, a cloud deployment from a vendor like AlienVault (recently acquired by AT&T), IBM, Securonix, or Splunk may be a better fit for you, especially if your security team is already overtaxed. On-premises deployments can be a better fit in sensitive environments or where data volumes are a concern. Hybrid deployments, where some monitoring is performed in the cloud and some with on-premises equipment, are also popular.
› **Find a vendor that will move you along the automation path.** SA vendors are building automation into their solutions and integrating with tools like IAM, NGFWs, intrusion prevention, and endpoint detection and response to give security operations center (SOC) analysts the ability to initiate remediation from the SA console. The next step is to automate remediation to take immediate action based on confidence level and business impact. Challenge your vendor to demonstrate how it’s automating SOC processes.

**Step 5: Embrace Security Automation And Orchestration**

Technology is increasingly automated, but security teams at many firms still use manual processes, relying on spreadsheets and email for much of their investigative work and collaboration. Manual security operations slow breach detection and response, leaving data and systems vulnerable to attacks or giving attackers more time to exfiltrate data and cause lasting damage to the environment. To embrace automation:

› **Work with business leaders to define policies for automation.** In the past, security teams were hesitant to automate anything for fear of blocking a legitimate transaction or affecting the customer or employee experience. Today, the potential business impact of a security breach or incident is so great that both business leaders and S&R teams are embracing automation — which requires defining the firm’s tolerance for risk. If a monitoring solution like SA has a high degree of confidence that an employee’s behavior is malicious, a predefined policy or SOC analyst automatically triggers a reset of that user’s password and the isolation of his devices from the network. The confidence threshold could be lower for privileged users with the potential to inflict significant damage.

› **Assess and document your SOC processes.** Many security teams lack defined workflows and SOC processes. Automating poor processes will only allow you to make bad decisions faster. Before fully embracing security automation and orchestration (SAO), assess the maturity of your processes, document them, and standardize them across the security team. You may be surprised to learn how many steps your analysts go through to conduct an investigation or close a ticket.

› **Check with your SA vendor to see what automation options are available.** SA vendors like IBM and Splunk already have or are adding SAO to their solutions. Splunk recently acquired one of the better-known dedicated SOA vendors, Phantom. Before investing in yet another security tool, ask your existing vendor if it can support your needs. Depending on the capabilities and road map of your current SA vendor, you may decide to go with a dedicated SAO solution like those from Demisto, Siemplify, and SwimLane.

› **Confirm that the SAO vendor supports your security infrastructure.** A SAO tool will do you no good if it doesn’t work with your current technology stack. Before deploying, ask for a proof of concept to demonstrate that the solution works with your infrastructure.
Use Zero Trust To Unite Technology And Business Stakeholders

You can’t achieve Zero Trust in a vacuum. Because it’s cross-functional, ZT provides incentives for different business and technology organizations to collaborate and helps to collapse the silos that inhibit growth. A ZT environment is agile and can dynamically adjust to business initiatives such as underpinning customer-facing mobile services, supporting geographic business expansion, adopting cloud services, integrating suppliers, and opening up R&D facilities. To realize Zero Trust across the organization, security leaders must:

› **Work with I&O leaders to define microperimeters and enable automation.** At many firms, the infrastructure and operations (I&O) team controls much of the technology budget; develops strategy; manages cloud initiatives and core infrastructure for computing, network, and storage; and is at the forefront of initiatives like DevOps, infrastructure-as-code, and the internet of things. Traditionally, I&O and security teams have operated as distinct silos, but now they must fuse their talents and automation initiatives to deliver efficient risk management with unprecedented speed, agility, and dependability.

› **Engage business leaders in data inventory, classification, and mapping.** Data is the currency of digital businesses, and a data breach is a catastrophic event. Because ZT is data-centric, it can play a key role not only in shoring up an enterprise’s reputation for security, privacy, and trust with its customers, but also in aligning the objectives of the CMO, CIO, and CISO. By understanding the critical data that drives a company’s business, Zero Trust efforts can help these execs prevent a data breach that drives customers away and costs millions. It can also aid chief privacy and data protection officers to ensure the firm not only meets but exceeds the spirit of consumer privacy objectives in regulations like GDPR and the recently passed California Consumer Privacy Act of 2018.

› **Extend Zero Trust thinking to include their people.** Use security awareness training as an opportunity to increase the security IQ of your employees, engage them in identifying and compartmentalizing sensitive data, and leverage them as a first line of defense to recognize when sensitive data is flowing outside of appropriate channels. Once your people are engaged in these processes, they will be more comfortable as you roll out SUBA to detect anomalous activity in your network and act on it before it becomes a breach.
Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

**Analyst Inquiry**
To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

**Analyst Advisory**
Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

**Webinar**
Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester’s research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

---

**Endnotes**

1 Cyberthreats, complex technology environments, and the struggle to hire experienced staff are finally forcing S&R pros to seek out security automation solutions. See the Forrester report “Breakout Vendors: Security Automation And Orchestration (SAO).”

2 Forrester’s CISO Strategic Canvas guides security leaders in developing a strategy that aligns with business objectives. Expand outside security if you want to anticipate where the business is going and how to help get it there. See the Forrester report “Use Forrester’s CISO Strategic Canvas To Align Security With Business.”

3 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. See the Forrester report “No More Chewy Centers: The Zero Trust Model Of Information Security.”

4 See the Forrester report “The Zero Trust eXtended (ZTX) Ecosystem: People.”

5 As the threat landscape continues to evolve, S&R leaders must adjust their risk management strategies to counter the next frontier: intellectual property theft. Theft of IP, such as trade secrets, new product designs, financial information, and source code, can lead to a permanent loss of competitive advantage. See the Forrester report “The Cybercriminal’s Prize: Your Customer Data And Intellectual Property.”
To help S&R professionals navigate the complex landscape of privacy laws around the world, Forrester created the Data Privacy Heat Map, which explains the data protection guidelines and practices for 54 countries. See the Forrester report “Forrester’s 2017 Interactive Data Privacy Heat Map.”

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.”

Forrester’s Data Security And Control Framework breaks down the problem of controlling and securing data into three areas: defining the data; dissecting and analyzing the data; and defending and protecting the data. See the Forrester report “The Future Of Data Security And Privacy: Growth And Competitive Differentiation.”

S&R pros can’t expect to adequately protect customer, employee, and sensitive corporate data and IP if they don’t know what data exists, where it resides, how valuable it is to the firm, and who can use it. See the Forrester report “Rethinking Data Discovery And Classification Strategies.”

See the Forrester report “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture” and see the Forrester report “Jump-Start Zero Trust With Forrester’s Reference Architecture.”

Due to growing concerns regarding data theft, privacy, and government surveillance, security pros are increasingly using all forms of encryption (cloud gateway, file, full disk, app-level, database-level, etc.) throughout their digital businesses. See the Forrester report “TechRadar™: Data Security And Privacy, Q4 2017.”


“Infringements . . . shall . . . 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/).

See the Forrester report “The Five Milestones To GDPR Success.”

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

See the Forrester report “The Forrester Identity Management And Governance Maturity Model” and see the Forrester report “The Forrester Wave™: Identity Management And Governance, Q2 2016.”

DLP: data loss prevention.

IAM: identity and access management.

See the Forrester report “Counteract Cyberattacks With Security Analytics.”

In our 36-criteria evaluation of security analytics providers, we identified the 11 most significant ones and researched, analyzed, and scored them. See the Forrester report “The Forrester Wave™: Security Analytics Platforms, Q1 2017.”

SA solutions promise to provide an array of functionality to give security professionals better visibility, improved detection, and enhanced workflows. See the Forrester report “Vendor Landscape: Security Analytics (SA).”

Security analytics is the decision-making layer for Forrester’s declarative security model. Using a response index based on confidence level and impact, security systems can take automated actions to stop malicious behavior, saving precious time in the event of an incident. See the Forrester report “Rules Of Engagement: A Call To Action To Automate Breach Response.”

See the Forrester report “Now Tech: Security Automation And Orchestration (SAO), Q3 2018.”
24 See the Forrester report “Become A Unicorn With Infrastructure-As-Code” and see the Forrester report “Pick The Right IoT Network Strategy.”

25 See the Forrester report “Reduce Risk And Improve Security Through Infrastructure Automation.”

26 See the Forrester report “Maintain Your Security Edge.”
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.