FORRESTER®

Five Steps To Zero Trust Security

FORRESTER®

SECTION ONE

Perimeter-Based Security, Meet Zero Trust

SECTION TWO

Five Steps To Zero Trust Information Security

SECTION THREE

Track And Measure Your Zero Trust Security Strategy

SECTION FOUR

Zero Trust Will Transform The Role Of Security

FORRESTER®

SECTION ONE

Perimeter-Based Security, Meet Zero Trust

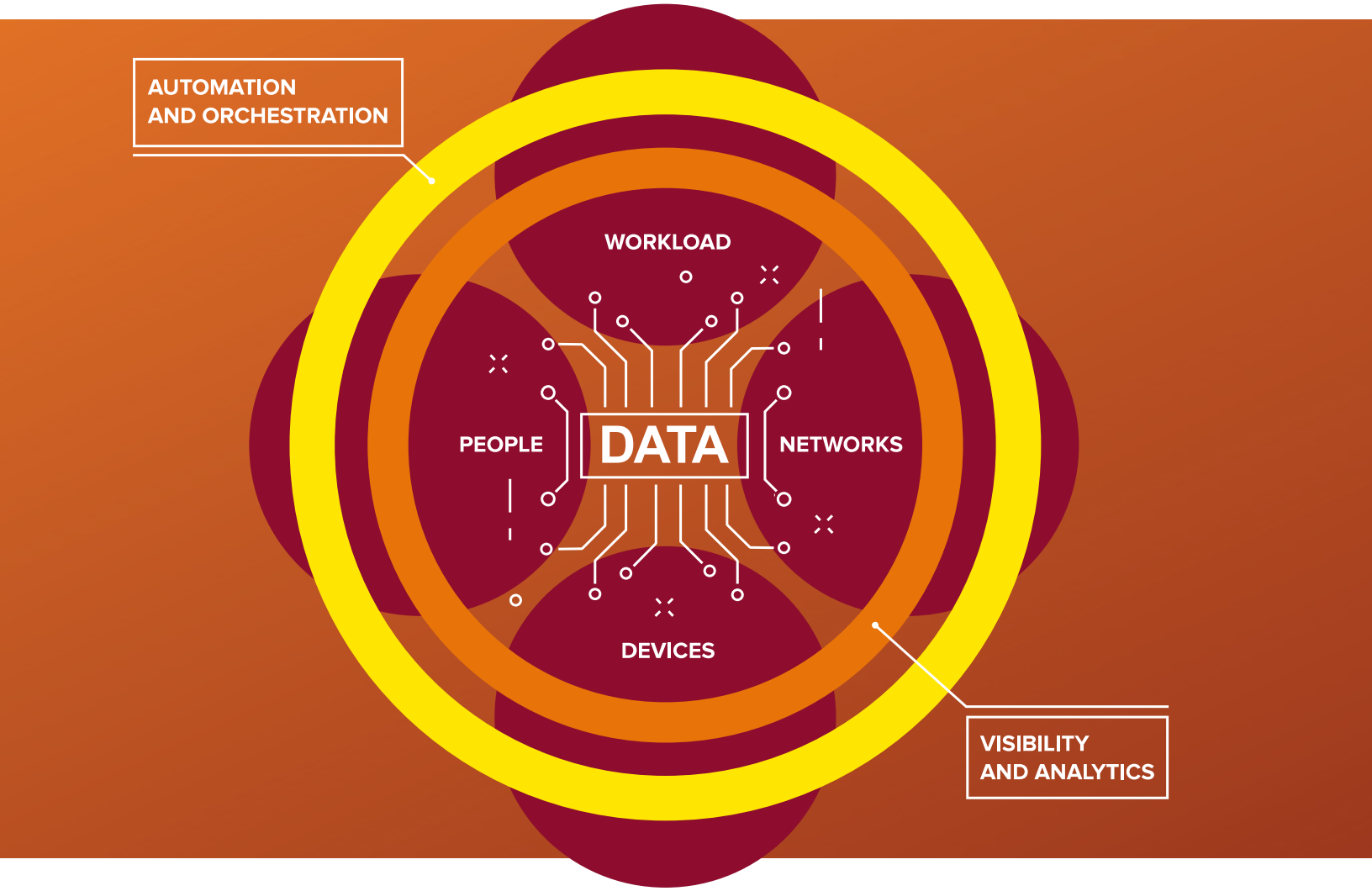
Zero Trust was originally developed by Forrester as a response to the need to move security leaders away from a failed perimeter-centric approach and guide them to a model that keeps data and identity management at its core — and is able to keep up with today's digital businesses.

The model soon came to be associated with network segmentation and next-generation firewalls, but in reality, Zero Trust is much more.

It's a complete and holistic approach to information security that includes processes and technologies for the management of data, networks, people, workloads, devices, visibility and analytics, and automation and orchestration.

FORRESTER®

Forrester's Zero Trust eXtended Framework



Today's cyberenvironment is rife with malicious actors digging for their next easy target — and as we've seen in headlines across the world, they've been successful.

SECTION TWO

Five Steps To Zero Trust Information Security

Zero Trust is the foundation of a secure architecture, and it begins by redesigning network security to be fundamentally data-centric. This is achieved in five steps:

01 Identify your sensitive data.

You can't protect what you can't see. Zero Trust starts with data to ensure your technology investments have a specific purpose and are not guided by expense-in-depth principles.

- Identify and classify sensitive data.
- Segment the network based on data sensitivity.

02 Map the flows of your sensitive data.

You need to understand how data flows across your extended network and between resources and people. Engage multiple stakeholders to map transaction flows.

- Locate and map all dependent network and system objects.
- Design a more optimal flow if necessary.
- Leverage existing data and network flow diagrams, such as the PCI Data Security Standard.

03 Architect your Zero Trust microperimeters.

Base the design of your Zero Trust network on how the transactions flow across your extended business ecosystem and how people and applications access sensitive data. Define and optimize a transaction path that characterizes proper data use and flags transactions when someone is potentially misusing it.

- Define microperimeters around sensitive data.
- Enforce microperimeters with physical or virtual security controls.
- Limit and strictly enforce access to microperimeters.
- Automate the rule and policy base.
- Use auditing and change control tools.

04 Continuously monitor your Zero Trust ecosystem security analytics.

Log and inspect all internal and external traffic for malicious activity and areas of improvement.

- Evaluate where you may already have security analytics.
- Determine the best deployment model for your business.
- Find a vendor that will move you along the automation path.

05 Embrace security automation and orchestration.

Relinquish manual security operations and processes and embrace automation.

- Work with business leaders to define policies for automation.
- Assess and document your SOC processes.
- Check with your security analytics vendor to see what automation options are available.
- Confirm that the security automation and orchestration vendor supports your security infrastructure.

SECTION THREE

Track And Measure Your Zero Trust Security Strategy

Zero Trust metrics measure your firm's ability to protect customer data, retain effective employees, and safeguard the firm's intellectual property. You'll have a range of metrics from strategic to tactical, with a variety of indicators including lagging indicators that highlight the results of past decisions; coincident indicators that provide a snapshot of the current situation; and leading indicators that provide predictive data points. Below you'll find a sample of Zero Trust metrics.

Protect customers' data while preserving their trust.

Customers who suffer identity theft, fraud, or other abuse of their personally identifiable information (PII) will stop doing business with you if they believe that you could have prevented the attack. They might also desert you if your post-breach communication comes late or lacks empathy and specific advice.

Strategic

Changes in customer acquisition, retention, and enrichment rates before and after specific breaches to detect lingering customer trust issues that endanger growth

Tactical

Changes in the adoption of customer two-factor authentication (2FA) and the percentage of customer data that is encrypted to focus your security team's future efforts

Recruit and retain happy, productive employees who appreciate security.

Happy employees lead to happy customers, and happy customers drive financial performance.

Strategic

Changes in the firm's ability to recruit new talent or changes in employee satisfaction and retention rates indicate morale issues that will affect productivity and customer service. Angry, resentful, or disillusioned employees are more likely to steal data for financial profit or as retaliation for a perceived slight.

Tactical

Employee use of 2FA, implementation of a privileged identity management (PIM) solution, and strong processes for identity management and governance (IMG) to identify focus areas for your security staff

Guard the firm's IP and reduce the costs of security incidents.

Intellectual property (IP) includes the trade secrets, formulas, designs, and code that differentiate your firm's products and services from those of competitors. An IP breach threatens your firm's future revenue and perhaps even its viability.

Strategic

Understand if the firm is the target of corporate espionage or nation-state actors and how much IP these actors have already compromised

Tactical

The extent to which the security team has encrypted sensitive data across locations and hosting models tells security staff where they need to concentrate their efforts to discover, classify, and encrypt sensitive IP

SECTION FOUR

Zero Trust Will Transform The Role Of Security

In a Zero Trust network, where apps and data reside in secure enclaves or microperimeters, security pros can quickly support new services, with granular privileges and data protection that don't inhibit business and employee productivity. That’s in stark contrast to perimeter-based approaches to security.

With Zero Trust, security leaders can take a proactive role, helping tech and business leaders adopt digital technologies that create new sources of value for customers and increase the firm's operational agility.

FORRESTER®

WEBINAR

Forrester experts discuss Zero Trust in practice – from implementation to vendor selection and measurement >

EVENTS

Attend our Security & Risk Forum to meet with and learn from industry thought leaders >

BLOGS

Stay up to date on trends and best practices from our security and risk team >

ZERO TRUST CERTIFICATION

Build your understanding of Zero Trust principles and instill confidence in your Zero Trust architecture and strategy >

BECOME A CLIENT

Contact us