FORRESTER®

Reinvent Your Security Strategy With Zero Trust

FORRESTER®

SECTION ONE

Digital Business Necessitates Zero Trust

SECTION TWO

Use Zero Trust To Get Business Buy-In

SECTION THREE

Get Started

SECTION FOUR

Act Now — Before It's Too Late

SECTION ONE

Digital Business Necessitates Zero Trust

Data is the lifeblood of today's digital businesses.

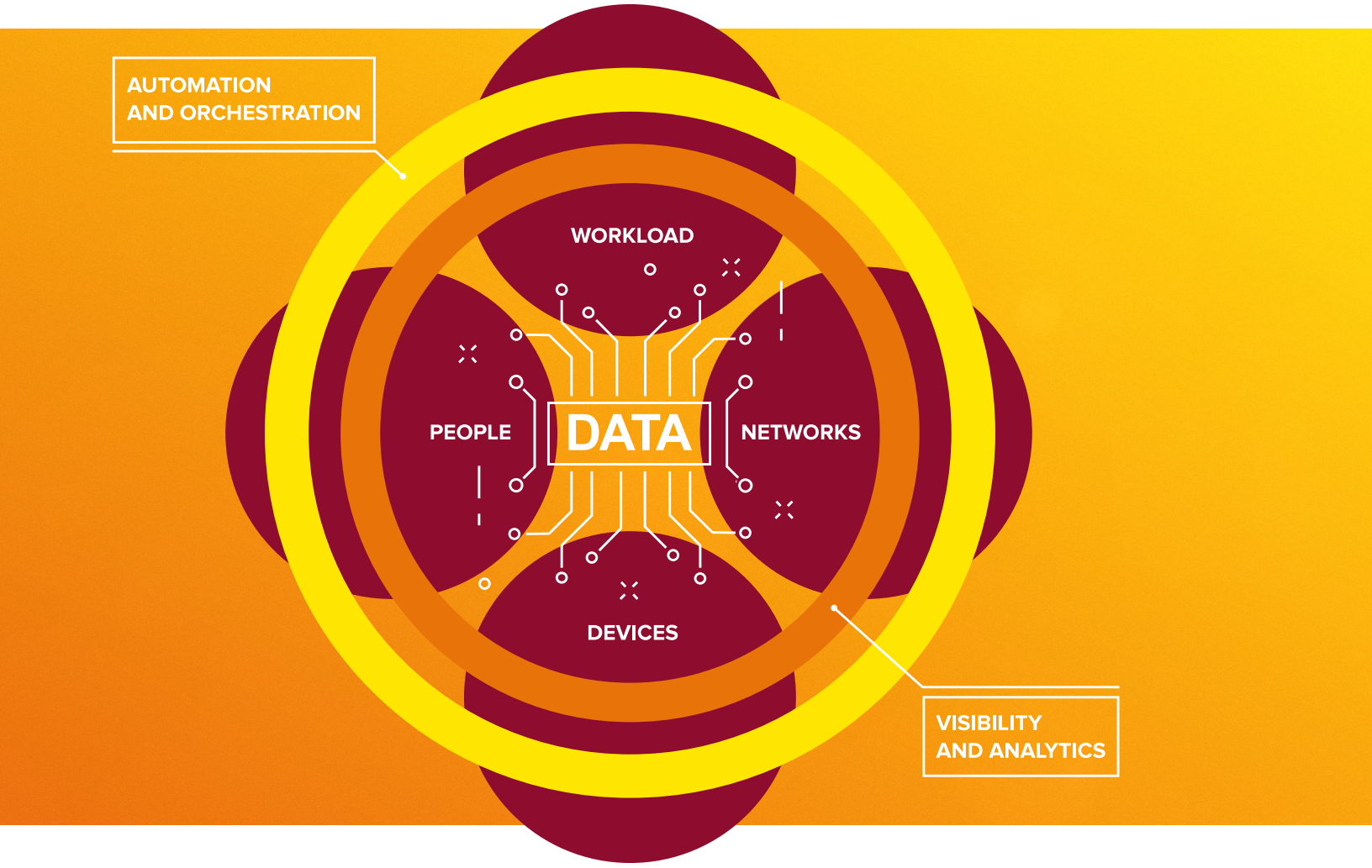
As businesses monetize information and insights across a complex business ecosystem, the idea of a corporate perimeter starts to sound quaint — even dangerous. Just as your business becomes increasingly data-centric, so must your security strategy and architecture.

Zero Trust is a data-first framework to achieve security using microperimeters and microsegmentation. The approach increases data security through obfuscation techniques, limits the risks associated with excessive user privileges, and dramatically improves security detection and response through analytics and automation.

We call our model "Zero Trust" to warn security leaders about the dangers of the numerous trust assumptions made in their architecture — whether that's trusting internal network traffic as legitimate by default or trusting partners to treat access to your systems and your data like it was their own.

The framework establishes security competencies across seven key areas: data, networks, people and workforce (human stakeholders), workloads and applications, devices, security visibility and analytics, and security automation and orchestration.

The ZeroTrust eXtended Framework



A Zero Trust approach to security, security architecture, and operations becomes workload-first, data-driven, and identity-aware rather than static and perimeter-based.

SECTION TWO

Use Zero Trust To Get Business Buy-In

Achieving Zero Trust is a cross-functional effort. To get there, your team will need to collapse the silo walls that separate too many businesses in order to appropriately map data flows and segment your network. Start this conversation by focusing on the business initiatives served by Zero Trust. These include:

Disruption readiness

A Zero Trust environment is agile and able to dynamically adjust to any business initiative at any time. By having knowledge and control of all data at all times, insights are more easily drawn and the business is better able to react quickly to changing customer demands.

Incident response & brand protection

Microperimeters are essential to Zero Trust, not only for the ability to protect the rest of the network in the event of a breach but also so that security teams know exactly when and where data has been stolen or tampered with. This type of control system allows for lightning-fast incident response capabilities, meaning that your business will be able to comply with GDPR requirements as well as remain transparent when communicating with customers.

Communication after a breach has a greater impact on customer trust and loyalty than the breach itself — the longer your firm fails to detect and respond to a breach, the more damaging and costly it will be.

Insights-driven growth

In a market where competitive advantage is achieved through learnings gleaned from customer data, the ability to control and protect that data is critical to success. Both the collection and use of that data depends on your security strategy: Can customers trust you with their data? Are you collecting, storing, and using data in a way that complies with current and future regulations?

A new approach to business support

Traditional perimeter-based approaches to security put up roadblocks for the business, as any access into the corporate perimeter means opening a door to the entire network. Zero Trust erases this risk, allowing security leaders to quickly support new services with granular privileges and data protection that don't inhibit productivity.

A comprehensive Zero Trust strategy can solve for all of the top strategic concerns that security leaders have ranked as a high or critical priority for the next 12 months.

67% Establishing or implementing security strategies for public clouds

65% Complying with security requirements placed upon us by business partners

65% Rolling out effective security training and awareness for employees across the organization

65% Establishing or implementing a formal technology/IT risk management framework

64% Establishing or implementing a framework to tie cybersecurity risk to enterprise risk

Base: 1,937 global security technology decision makers
Source: Forrester Analytics Global Business Technographics® Security Survey, 2018

SECTION THREE

Get Started

Too often security is an afterthought, brought in at the end of the product development life cycle as a bolt-on feature. This risks failure at both the product level and, ultimately, at the business level in the event of a breach.

Zero Trust will be achieved differently for every organization based on how 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 Zero Trust ecosystem for signs of a breach or other malicious activity.

Follow Five Steps To Zero Trust Information Security:

01 **Identify your sensitive data.**

02 **Map the flows of your sensitive data.**

03 **Architect your Zero Trust microperimeters.**

04 **Continuously monitor your Zero Trust ecosystem.**

05 **Embrace security automation and orchestration.**

SECTION FOUR

Act Now — Before It's Too Late

Today, your firm's competitive differentiation relies on your ability to exploit digital technologies and data to their fullest potential. Legacy networks are ill-equipped for reliable protection with most security controls living at the perimeter — meaning that threats in the form of corporate espionage, corporate and industrial sabotage, and cyberwarfare will be catastrophic to your business in the event of an attack.

—

Following Zero Trust will allow you and your teams to embed security throughout the business, yielding benefits not only from increased protection but also from increased potential for growth.

FORRESTER®

EVENTS

Attend our Privacy & Security 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 >

PEER COUNCILS

Connect with like-minded security professionals to learn from mutual challenges and successes >

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 »

FOLLOW FORRESTER