THE ESSENTIAL SECURITY GUIDES SERIES

JUST TELL ME WHAT I NEED TO KNOW...

ZERO TRUST

NEVER TRUST. ALWAYS VERIFY. REDUCE RISK. PROTECT EVERYTHING.

VERIFY EXPLICITLY
Strong identity verification for every user and device.

USE LEAST PRIVILEGE ACCESS
Limit user access with just-in-time and just-enough access.

ASSUME BREACH
Design for failure. Continuously detect and respond to threats.

MICROSEGMENT EVERYTHING
Isolate resources and enforce granular access controls.

DEVICE HEALTH & COMPLIANCE
Ensure devices meet security standards before access is granted.

CONTINUOUS MONITORING
Analyze behavior and context to adapt and respond in real time.

ZERO TRUST PILLARS

IDENTITIES
Secure and verify all users and service identities.

DEVICES
Validate and assess device trust and security posture.

NETWORK
Encrypt and protect all connections everywhere.

APPLICATIONS
Control access to applications based on trust and context.

DATA
Classify and protect data across all anvironments.

ZERO TRUST IN ACTION

IDENTIFY
Know who and what is trying to connect.

AUTHENTICATE
Verify identity with strong, phishing-resistant authentication.

AUTHORIZE
Evaluate context and grant least privilege access.

ENCRYPT & PROTECT
Secure all data in transit and at rest.

MONITOR
Continuously monitor activity and detect anomalies.

ADAPT & RESPOND
Automatically adjust access and respond to changes.

Just Tell Me What I Need To Know

Zero Trust

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

Table of Contents

Introduction

The days of trusting everything inside the corporate network are over.

Today's organizations operate in a world of cloud computing, remote work, mobile devices, Software as a Service (SaaS), APIs, containers, and increasingly sophisticated cyber threats. Users connect from anywhere, applications run across multiple environments, and critical data is no longer confined to a single data center. In this new reality, traditional perimeter-based security is no longer enough.

The answer isn't simply adding more firewalls or deploying another security product. It requires a different way of thinking.

That way of thinking is Zero Trust.

Despite its growing popularity, Zero Trust is one of the most misunderstood concepts in cybersecurity. Some believe it's a product they can purchase. Others assume it's nothing more than multi-factor authentication or a remote access solution. In reality, Zero Trust is a security architecture and operating philosophy that assumes no user, device, application, workload, or network should be trusted by default. Every access request must be continuously verified based on identity, device health, context, risk, and policy.

That's where this book comes in.

The Just Tell Me What I Need to Know… series is designed to cut through the complexity and focus on the knowledge professionals actually need. Rather than overwhelming you with vendor-specific implementations or theoretical models, each book delivers practical, real-world concepts in a clear, concise, and easy-to-understand format.

This book focuses on Zero Trust—the principles, architectures, and technologies used to build secure, modern enterprises. You'll learn how identity becomes the new security perimeter, how continuous verification replaces implicit trust, and how organizations use least privilege, microsegmentation, strong authentication, workload identities, device trust, and data-centric security to reduce risk across cloud, hybrid, and on-premises environments.

Unlike books that focus exclusively on a single vendor or identity platform, this book takes a vendor-neutral approach. Whether your organization uses Microsoft Entra ID, Active Directory, Okta, Ping Identity, AWS, Google Cloud, Azure, or another platform, the architectural principles remain the same. The emphasis is on understanding how the components work together to create a resilient Zero Trust architecture.

The purpose of the book is to learn how to design, implement, and mature enterprise Zero Trust architectures using identity-centric security, continuous verification, least privilege, microsegmentation, workload identity, and policy-based access control to secure modern on-premises, cloud, hybrid, and multi-cloud environments. This book is the enterprise Zero Trust architecture reference for the series, focusing on practical implementation rather than vendor-specific products.

Whether you're an engineer, architect, cybersecurity professional, ISSO, manager, executive, student, or technology leader, understanding Zero Trust has become essential for designing and protecting modern enterprise systems.

Our goal is simple:

Give you the knowledge you need, without making you read three books to get it.

So, let's get started.

TRUST IS NO LONGER A PLACE. IT'S A DECISION THAT MUST BE EARNED EVERY TIME.

The traditional network perimeter has disappeared. Employees work remotely, applications span multiple clouds, devices connect from anywhere, and attackers routinely exploit stolen credentials to move through enterprise environments. Protecting modern organizations requires a new approach—one that assumes no user, device, application, or workload should ever be trusted by default.

The problem? Most Zero Trust books focus on a single vendor, identity platform, or technology. Others are so theoretical that it's difficult to understand how Zero Trust actually works in a real enterprise.

This book is different.

Just Tell Me What I Need To Know... Zero Trust provides a practical, business-focused guide to designing and implementing modern Zero Trust architectures. You'll learn how identity becomes the new security perimeter, how continuous verification replaces implicit trust, and how least privilege, microsegmentation, device trust, workload identities, policy-based access, and continuous monitoring work together to protect today's cloud, hybrid, and on-premises environments. Rather than promoting a specific vendor or product, this book explains the architectural principles, technologies, and best practices that apply across any enterprise.

ZERO TRUST BY THE NUMBERS

80%	of organizations are already underway with Zero Trust initiatives.
90%	of cyber attacks start with credential compromise.
75%	of enterprises run workloads across multiple clouds.
60%+	of the workforce is remote or hybrid.
3x	less risk of breach with mature Zero Trust implementations.

Source: Gartner, Forrester, IBM, Verizon DBIR

INSIDE YOU'LL LEARN HOW TO:

- Understand the principles and architecture of Zero Trust
- Design identity-centric security for modern enterprises
- Implement least privilege, continuous verification, and adaptive access
- Secure users, devices, workloads, applications, APIs, and data
- Apply Zero Trust across cloud, hybrid, and multi-cloud environments
- Build policy-driven architectures using industry best practices
- Measure Zero Trust maturity and develop a practical implementation roadmap
- Build a resilient enterprise security architecture that continuously adapts to evolving threats

HOW ZERO TRUST WORKS

IDENTIFY
Know who and what is requesting access.

VERIFY
Validate context, risk, and policy before granting access.

AUTHORIZE
Grant least privilege access based on policy.

MONITOR
Continuously monitor behavior and session activity.

ADAPT
Dynamically adjust access as risk and context change.

NEVER TRUST. ALWAYS VERIFY.

ZERO TRUST PROTECTS EVERYTHING

USERS | DEVICES | APPLICATIONS | WORKLOADS | APIS | DATA

THE SIX PILLARS OF ZERO TRUST

IDENTITY
Verifying users and workloads continuously.

DEVICES
Ensuring device health and compliance.

NETWORK
Eliminating implicit trust through microsegmentation.

APPLICATIONS
Protecting apps and APIs with least privilege.

DATA
Classifying and securing data wherever it lives.

VISIBILITY & ANALYTICS
Gaining real-time insight and detecting risk continuously.

ZERO TRUST MATURITY MODEL

1 INITIAL
Ad-hoc controls and limited visibility.

2 DEVELOPING
Foundational policies and basic controls.

3 DEFINED
Consistent policies and expanded coverage.

4 ADVANCED
Automated policies and integrated technologies.

YOUR ZERO TRUST ROADMAP

ASSESS
Evaluate current state, risks, and gaps.

DESIGN
Define target architecture and capabilities.

IMPLEMENT
Deploy solutions and integrate systems.

MEASURE
Track outcomes and drive improvement.

EVOLVE
Continuously mature and adapt.

Whether you're a security architect, engineer, CISO, ISSO, cloud professional, consultant, project manager, or aspiring cybersecurity professional, this book provides the practical knowledge you need to understand, implement, and mature Zero Trust—helping your organization reduce risk while enabling secure business operations in today's increasingly connected world.

ZERO TRUST ISN'T JUST A STRATEGY. IT'S A MINDSET.
BUILD TRUST. REDUCE RISK. ENABLE THE BUSINESS.

BELSHAW CONSULTING