

No. 08

ZERO TRUST

Zero Trust Networks

Zero trust security for SAP and enterprise networks, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 08

Zero Trust Networks

Zero trust security for SAP and enterprise networks, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Zero Trust Networks

Zero trust security for SAP and enterprise networks, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why perimeters fail 4
2 Zero trust principles 7
3 The zero trust architecture 10

PART II · THE PILLARS

4 Identity 15
5 Devices 20
6 Networks 23
7 Applications and workloads 27
8 Data 30
9 Visibility, automation and governance 33

PART III · PUTTING IT INTO PRACTICE

10 Zero trust for SAP landscapes 37
11 Maturity and roadmap 41
12 Attack scenarios and how zero trust helps 44
13 Checklists 48

Glossary 51
Further reading 53

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

"Zero trust" is one of the most used — and most misused — phrases in security. Vendors attach it to products; strategies promise it by next year. Behind the noise is a simple and powerful idea: **never grant access just because of where a request comes from. Verify every request, give the least access needed, and assume an attacker may already be inside.**

This book explains zero trust **in plain language, for beginners**, and shows how to apply it — including to SAP landscapes, which hold some of an organization's most valuable data.

Who this book is for

- **Security and network professionals** starting a zero trust program.
- **SAP security and Basis teams** who must fit SAP systems into a zero trust architecture.
- **IT managers and architects** who need to separate zero trust substance from marketing.
- **Auditors and risk managers** who want to assess zero trust claims.

How the book is organized

- **Part I — Foundations** (Chapters 1–3): why perimeter security fails, the zero trust principles, and the reference architecture.
- **Part II — The pillars** (Chapters 4–9): identity, devices, networks, applications and workloads, data, and the cross-cutting capabilities.

FREE SAMPLE · ojayo.com

- **Part III — Putting it into practice** (Chapters 10–13): zero trust for SAP landscapes, maturity and roadmap, attack scenarios, and checklists.

Conventions

TIP

Practical advice you can apply straight away.

IN SAP

How a topic applies to SAP systems.

WATCH OUT

Common mistakes and risks.

Diagrams are original. Screens marked **Illustration** are simplified drawings, not real products, and values in them are examples. People and companies are fictional. The book is vendor-neutral: product types are named, but no product is recommended.

A NOTE ON FRAMEWORKS

This book draws on public frameworks such as NIST Special Publication 800-207 and CISA's Zero Trust Maturity Model. It summarizes their ideas in its own words; read the original documents for authoritative wording and details, and check for newer versions.

FREE SAMPLE · ojayo.com

PART I

Foundations

Why the old perimeter model no longer works, the principles of zero trust, and the architecture that puts them into practice.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why perimeters fail

For decades, networks were built like castles. This chapter explains why that model broke — and what replaced it.

The castle-and-moat model

Traditional network security drew a line between **inside** (trusted) and **outside** (untrusted). Firewalls guarded the line. Once a user or device was inside — in the office, or connected through VPN — it was largely trusted to reach other systems.

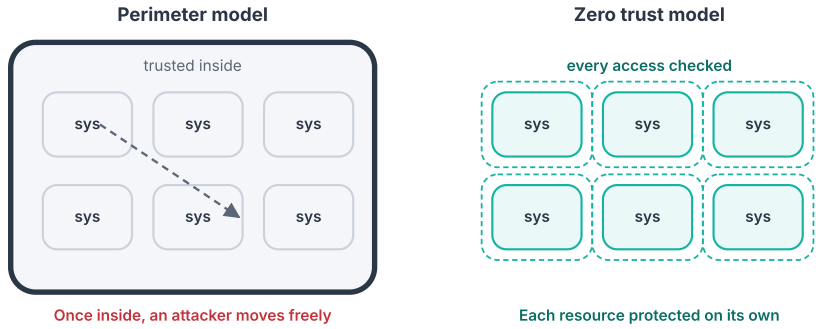


Figure 1.1 In the perimeter model, being inside means being trusted. In zero trust, every resource is protected on its own and every access is checked.

This model made sense when:

- employees worked in offices on company-owned computers;
- applications ran in the company's own data center;
- the number of connections to the outside world was small and known.

FREE SAMPLE · ojayo.com

What changed

None of those assumptions hold today:

- **Remote and hybrid work** put users and devices outside the perimeter most of the time.
- **Cloud services** moved applications and data outside the data center.
- **Partners, suppliers and contractors** need access to some systems.
- **Personal and mobile devices** access company resources.
- **Interconnected systems** — APIs, integrations, SaaS — create many paths in.

The perimeter did not disappear; it dissolved into thousands of small perimeters.

Why "inside = trusted" is dangerous

Many serious breaches follow the same pattern:

1. An attacker gets a **foothold** — a phished password, an infected laptop, a vulnerable internet-facing server.
2. Because the internal network trusts that foothold, the attacker **moves laterally**, scanning and reaching other systems.
3. The attacker **escalates privileges**, often by finding administrator credentials.
4. The attacker reaches **valuable data** or deploys ransomware widely.

In a flat, trusted network, step 2 is easy. Zero trust aims to make every step after the first one hard.

Where zero trust came from

The term "zero trust" is generally credited to **John Kindervag**, then an analyst at Forrester Research, around 2010. **Google's BeyondCorp** program, described in a series of papers from 2014 onward, showed at scale how employees could work without a privileged corporate network, with access decided per request based on user and device.

FREE SAMPLE · ojayo.com

Governments later adopted the idea. In the United States, **NIST** published Special Publication 800-207, *Zero Trust Architecture*, in 2020; **Executive Order 14028** (2021) and the federal zero trust strategy (OMB memorandum M-22-09, 2022) directed agencies toward it; and **CISA** published a Zero Trust Maturity Model, updated to version 2.0 in 2023.

What zero trust is not

- **Not a product.** No single tool "delivers" zero trust. It is an architecture and a way of making access decisions.
- **Not "trust nobody, ever".** Users still get access — but based on verification, not location.
- **Not a one-off project.** It is a journey that improves maturity over years.
- **Not only about networks.** Despite the name, identity, devices, applications and data matter as much as network design.

TIP

When someone says a product is "zero trust", ask: *Which access decisions does it make or enforce, based on which signals?* If there is no clear answer, it is marketing.

KEY TAKEAWAYS

- The **perimeter model** trusts anything inside; modern work and cloud broke it.
- Attackers exploit internal trust through **lateral movement** and **privilege escalation**.
- Zero trust grew from **Forrester** and **Google BeyondCorp**, then **NIST** and **CISA** guidance.
- Zero trust is an **architecture and approach**, not a product.

FREE SAMPLE · ojayo.com

CHAPTER 2

Zero trust principles

Zero trust rests on a short list of principles. Learn these, and the rest of the book is applying them.

The three ideas everyone quotes

Most descriptions of zero trust come down to three ideas:

1. **Verify explicitly.** Decide access using all available signals — who the user is, which device, its health, location, the resource's sensitivity, and behavior — not just network location.
2. **Use least privilege.** Give only the access needed, for only as long as needed.
3. **Assume breach.** Design as if an attacker is already inside: limit what one compromise can reach, encrypt, and watch everything.

The NIST tenets in plain words

NIST SP 800-207 lists seven tenets. In this book's own words, they say:

FREE SAMPLE · ojayo.com

#	Tenet (paraphrased)	What it means in practice
1	Everything is a resource	Data, services, devices and applications are all things to protect — not just "servers"
2	Secure all communication, wherever it happens	Internal traffic is encrypted and authenticated just like internet traffic
3	Grant access per session	Access to one resource does not automatically give access to another
4	Decide with dynamic policy	Decisions consider identity, device state, context and behavior, not fixed rules alone
5	Monitor the security of all assets	Know every device's state and measure it continuously
6	Authenticate and authorize before access, strictly and dynamically	Re-check during sessions; respond to changing risk
7	Collect information to improve	Use logs and telemetry to keep improving policies

Every request is a decision

In a zero trust architecture, each request to a resource is a **decision** made from several questions:

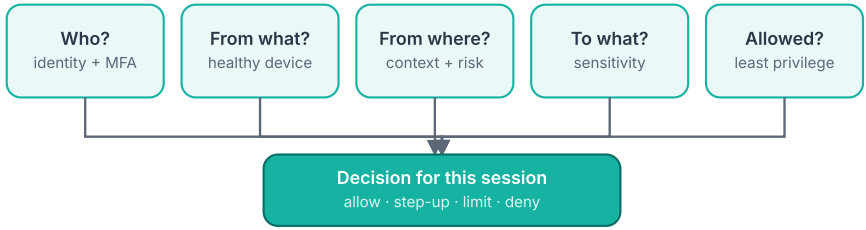


Figure 2.1 The questions behind each access decision. The answer can be more nuanced than yes or no.

The outcome is not only "allow" or "deny". It can be:

- **allow** normally;
- **step up** — ask for stronger authentication;

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks (you are reading this)
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Zero Trust Networks

Enjoyed it? The full book has 58 pages and 13 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.