BEMI
IT SOLUTIONS

BEMI TECH SOLUTIONS · CYBERSECURITY TRAINING SERIES

Zero Trust Security

The Complete Guide

> Never Trust. Always Verify. — From fundamentals to enterprise implementation.

10	50+	5	4
Chapters	Pages	Pillars Covered	Implementation Steps

This guide covers the complete Zero Trust Security model — from its foundations and core principles to enterprise-grade implementation. Whether you're a security professional, IT manager, or someone starting your cybersecurity journey, this guide gives you the knowledge and practical roadmap to understand and apply Zero Trust in any environment.

Ransford Slater · Bemi Tech Solutions · bemitechsolutions.com · Arlington, TX

TABLE OF CONTENTS

What's Inside

01

What Is Zero Trust Security?

Never Trust. Always Verify.

BEMI IT SOLUTIONS

Zero Trust Security is a cybersecurity model built on one foundational principle: never trust, always verify. Unlike traditional security that assumed everything inside the network was safe, Zero Trust treats every user, device, and request as potentially hostile — regardless of where it comes from.

THE CORE PRINCIPLE

John Kindervag, a Forrester Research analyst, developed the Zero Trust model in 2010 after observing that organizations were investing heavily in perimeter defenses while doing little to protect what was already inside. His insight: the concept of a trusted internal network was fundamentally flawed.

The Zero Trust model eliminates the idea of a trusted zone entirely. Every access request — whether from an employee in the office, a remote worker, a cloud application, or a partner — is verified against identity, device compliance, location, and behavioral context before access is granted.

ZERO TRUST DEFINED

- A security model that requires strict verification of every user and device
- No implicit trust is granted based on network location
- Access is granted on a least-privilege basis after continuous verification
- Designed to contain breaches and limit lateral movement

WHY 'ZERO TRUST'?

The name reflects the model's core assumption: zero implicit trust is given to anyone or anything, even if they appear to be inside your organization's network. Traditional security operated on an 'inside is safe' assumption. Zero Trust operates on an 'always verify' assumption.

Traditional Security

Trust everything inside the firewall. Authenticate once at the perimeter.

Zero Trust Security

Trust nothing by default. Continuously verify every request.

WHO MANDATES ZERO TRUST?

- NIST Special Publication 800-207 — the authoritative Zero Trust architecture standard
- CISA Zero Trust Maturity Model — US federal government adoption framework
- Executive Order 14028 (2021) — US federal agencies required to adopt Zero Trust

- ISO/IEC 27001:2022 — information security management aligned with Zero Trust principles
- SOC 2 Type II — continuous monitoring requirements map directly to Zero Trust controls

Zero Trust is no longer optional for organizations handling sensitive data. Whether you operate in healthcare, finance, government, or technology — regulators, customers, and insurance providers now expect Zero Trust-aligned security controls.

02

Why Zero Trust Exists

The Perimeter Is Dead

BEMI IT SOLUTIONS

Zero Trust did not emerge from a theoretical exercise. It emerged because the traditional security model failed — repeatedly, catastrophically, and at scale. To understand why Zero Trust is necessary, you must first understand why the old model broke down.

THE DEATH OF THE PERIMETER

For decades, enterprise security was built around a simple idea: defend the perimeter. Build a strong firewall. Control what enters and exits. Everything inside is trusted. This model worked reasonably well when employees sat in offices connected to on-premises servers.

Then everything changed. Cloud computing, remote work, mobile devices, SaaS applications, and third-party integrations destroyed the concept of a defined perimeter. Today, your data lives in AWS, your employees work from coffee shops, your applications run across dozens of vendors — and your 'perimeter' is everywhere and nowhere.

80%	287	$4.45M	98%
Breaches use compromised credentials	Days avg. attacker dwell time	Avg. cost of a data breach (2023)	Orgs breached via third party

THE INSIDER THREAT PROBLEM

Traditional security assumed external attackers were the primary threat. This assumption was wrong. Insider threats — whether malicious employees, negligent users, or compromised accounts — account for a significant portion of security incidents. A firewall does nothing to stop someone who is already inside.

WHY TRADITIONAL SECURITY FAILED

- Perimeter-only defense left the interior completely unprotected
- Once inside, attackers moved freely — lateral movement was undetected
- Single authentication at login gave full access for entire session
- VPNs extended the perimeter to remote workers — and their home networks
- Shadow IT and cloud adoption created invisible attack surfaces

THE CREDENTIAL CRISIS

80% of data breaches involve stolen or weak credentials. This single statistic explains why Zero Trust exists. When an attacker has valid credentials, they look exactly like a legitimate user to traditional security systems. They log in normally. They move freely. They exfiltrate data for months before detection.

Zero Trust addresses this by making credentials only one factor in a continuous verification chain. Even with valid credentials, an attacker still must pass device compliance checks, behavioral analytics, conditional access policies, and micro-segmentation controls.

Credential Theft

Phishing, password spraying, and credential stuffing compromise valid accounts.

Lateral Movement

Once inside, attackers pivot from system to system until they reach high-value targets.

03

The 3 Core Principles

Verify · Limit · Assume Breach

BEMI IT SOLUTIONS

Zero Trust architecture is built on three core principles defined by NIST SP 800-207. Every design decision, policy, and control in a Zero Trust environment traces back to one of these principles. Understanding them deeply is essential before attempting implementation.

PRINCIPLE 1: VERIFY EXPLICITLY

Every access request must be authenticated and authorized using all available data points — not just a username and password. Verification must be continuous, not just at login.

WHAT VERIFY EXPLICITLY MEANS

- Authenticate every user with MFA — not just a password
- Verify device health and compliance status before granting access
- Evaluate location, IP reputation, and time-of-day context
- Apply behavioral analytics to detect anomalous access patterns
- Re-authenticate for sensitive operations — not just at session start

PRINCIPLE 2: USE LEAST PRIVILEGE ACCESS

Users, applications, and systems should have access only to the specific resources they need to do their job — nothing more. Permissions should be time-bound, scoped to the minimum required, and regularly reviewed.

Role-Based Access

Grant access based on job role — only the permissions that role requires.

Just-in-Time Access

Temporary elevated access granted for a specific task and automatically revoked.

Least privilege dramatically reduces the blast radius of a compromised account. If an attacker takes over a developer account with read-only access to a single repository, they cannot pivot to payment systems, HR data, or administrative consoles.

PRINCIPLE 3: ASSUME BREACH

Design your security architecture as if an attacker is already inside your network. This mindset shift drives fundamentally different security decisions. Instead of asking 'how do we keep attackers out?' you ask 'what happens when they get in — and how do we contain it?'

ASSUME BREACH CONTROLS

- Micro-segment networks so breach of one zone doesn't spread to others
- Encrypt all data in transit and at rest — even on internal networks
- Implement comprehensive logging and monitoring of all traffic
- Define incident response playbooks before a breach occurs
- Regularly test your detection and response capabilities

Together, these three principles create a security posture that is fundamentally different from traditional defense. Rather than a strong outer wall with an unprotected interior, Zero Trust creates layered verification at every access point, with minimal blast radius if any layer fails.

04

Zero Trust vs Traditional Security

Old Model vs New Reality

BEMI IT SOLUTIONS

Understanding the shift from traditional perimeter security to Zero Trust requires a direct comparison of the two models. The differences are not subtle — they represent a fundamental change in how security is conceptualized, designed, and operated.

THE TRADITIONAL MODEL

Traditional security, often called 'castle-and-moat' security, focused all defenses at the perimeter. A strong firewall kept external threats out. Once inside the perimeter — whether you were an employee, a device, or an application — you were implicitly trusted. Internal traffic was largely unmonitored.

TRADITIONAL SECURITY ASSUMPTIONS

- The internal network is trusted — external is untrusted
- Authentication happens once at the perimeter (VPN login, office door)
- Verified users can move freely within the internal network
- Firewalls and perimeter controls provide sufficient protection
- Internal monitoring is minimal — threats come from outside

THE ZERO TRUST MODEL

Zero Trust eliminates the concept of a trusted zone. Every request — internal or external, from any user or device — is verified against identity, device posture, context, and policy. Trust is never assumed; it is earned through continuous verification and granted only for the minimum required access.

ZERO TRUST ASSUMPTIONS

- No implicit trust — the network location does not determine trust
- Every access request is authenticated and authorized every time
- Access is granted to specific resources only — not the entire network
- All traffic is monitored — east-west internal traffic included
- Assume breach — design to contain rather than solely to prevent

SIDE-BY-SIDE COMPARISON

- Trust model: Implicit trust inside perimeter !’ Explicit verification always

- Access model: Broad network access granted !’ Least-privilege per resource
- Authentication: Once at login !’ Continuous per session and per request
- Monitoring: Perimeter-focused !’ All traffic including internal east-west
- Breach response: Contain after detection !’ Assume breach by design
- Remote work: VPN extends trust zone !’ ZTNA verifies per request
- Cloud security: IP-based controls !’ Identity-based controls

05

The 5 Pillars of Zero Trust

Identity · Devices · Networks · Apps · Data

BEMI IT SOLUTIONS

CISA's Zero Trust Maturity Model organizes the Zero Trust architecture into five pillars. Each pillar represents a critical area of your environment that must be secured under Zero Trust principles. Progress across all five pillars simultaneously — no single pillar is sufficient on its own.

PILLAR 1: IDENTITY

Identity is the foundation of Zero Trust. Every user, service account, and application must have a verified, trusted identity before any access is granted. Identity security goes far beyond usernames and passwords.

MFA | **SSO** | **Conditional Access** | **Identity Governance** | **Behavioral Analytics** | **Privileged Identity Management**

PILLAR 2: DEVICES

A verified identity is not enough if the device is compromised. Every endpoint — laptop, mobile, server, IoT device — must be enrolled in device management and must pass compliance checks before access is granted. An unknown or non-compliant device should be denied or placed in a restricted segment.

DEVICE SECURITY CONTROLS

- Mobile Device Management (MDM) — enforces compliance policies on endpoints
- Endpoint Detection & Response (EDR) — detects and responds to threats on devices
- Device health attestation — verifies OS version, patch level, encryption status
- Certificate-based authentication — ties access to specific registered devices

PILLAR 3: NETWORKS

Traditional flat networks allow unrestricted lateral movement. Zero Trust networks are segmented into small, isolated zones with strict access controls between them. Traffic between zones is treated as potentially hostile and requires explicit authorization.

PILLAR 4: APPLICATIONS

Every application must enforce access controls at the application layer. Users see only the apps they need. App-level micro-segmentation ensures that even a compromised account cannot pivot from one application to another. API security, OAuth scopes, and application firewalls are key controls.

PILLAR 5: DATA

Data is the ultimate target of every attack. Zero Trust data security requires classifying all data by sensitivity, encrypting it at rest and in transit, applying data loss prevention controls, and monitoring access continuously. Data should be protected even after it leaves your environment.

5	100%	0	"
Pillars to protect	Traffic monitored	Implicit trust	Continuous verification

06

Identity Is the New Perimeter

MFA, Conditional Access & PAM

BEMI IT SOLUTIONS

In a Zero Trust architecture, identity replaces the network as the primary security boundary. Where you connect from matters far less than who you are, what device you're using, and whether your behavior matches expected patterns.

MULTI-FACTOR AUTHENTICATION (MFA)

MFA is the single most impactful control you can deploy. Microsoft's research shows that MFA blocks 99.9% of automated credential attacks. Even if an attacker steals a valid password, they cannot authenticate without the second factor.

MFA FACTOR TYPES

- Something you know — password or PIN (weakest factor alone)
- Something you have — authenticator app, hardware token, smart card
- Something you are — biometrics: fingerprint, face, voice recognition
- Phishing-resistant MFA — FIDO2/WebAuthn hardware keys (strongest)

CONDITIONAL ACCESS POLICIES

Conditional access evaluates the full context of every sign-in request before granting access. Instead of binary allow/deny, it can enforce step-up authentication, block access from risky locations, or limit access to specific applications based on device compliance.

Signals Evaluated

User identity, device compliance, location, IP risk, application sensitivity, time of day.

Access Outcomes

Allow, require MFA, require compliant device, block, limit to read-only.

PRIVILEGED ACCESS MANAGEMENT (PAM)

Privileged accounts — system administrators, database administrators, executives — are the primary targets of attackers. PAM solutions enforce the strictest controls on these accounts: just-in-time access, session recording, password vaulting, and approval workflows.

CyberArk | BeyondTrust | Delinea | HashiCorp Vault | Azure PIM | AWS IAM | Okta | Microsoft Entra ID

IDENTITY GOVERNANCE

Identity governance ensures that access rights are granted correctly, reviewed regularly, and revoked promptly. Access certification campaigns require managers to review and reapprove employee permissions periodically — preventing privilege creep where users accumulate excessive access over time.

07

Micro-Segmentation

Contain the Blast Radius

BEMI IT SOLUTIONS

Micro-segmentation is the practice of dividing a network into small, isolated zones with strict access controls between them. It is one of the most powerful tools in a Zero Trust architecture — directly addressing the lateral movement problem that makes breaches so devastating.

THE LATERAL MOVEMENT PROBLEM

When an attacker compromises a single endpoint in a flat network, they can move freely to every other system on that network. They can reach financial databases, HR systems, source code repositories, and administrative consoles — all from one initial compromise. Micro-segmentation eliminates this freedom.

WHAT MICRO-SEGMENTATION ACHIEVES

- Limits blast radius — a breach stays contained within its segment
- Eliminates unrestricted lateral movement across the network
- Forces east-west traffic through security inspection and policy enforcement
- Enables granular, application-level access control between workloads
- Supports Zero Trust principle of 'assume breach' by design

IMPLEMENTATION APPROACHES

Micro-segmentation can be implemented at several layers of the network stack, each with different granularity and control capabilities.

Network-Based

VLANs, firewall rules, and ACLs create network-level isolation between segments.

Host-Based

Software firewalls on each host enforce policies at the workload level.

SDN / Overlay

Software-defined networking creates virtual network segments independent of physical topology.

Service Mesh

mTLS between microservices enforces mutual authentication and encryption at the application layer.

EAST-WEST TRAFFIC MONITORING

Traditional security focused on north-south traffic — traffic entering and leaving the network perimeter. Zero Trust requires equal attention to east-west traffic — traffic moving between internal systems. Most attackers, once inside, generate east-west traffic as they move laterally. Without visibility into this traffic, breaches go undetected for months.

VMware NSX **Illumio** **Akamai Guardicore** **Cisco ACI**

Palo Alto Prisma **Zscaler** **AWS Security Groups** **Azure NSGs**

08

Zero Trust in the Cloud

CASB · SASE · ZTNA

BEMI IT SOLUTIONS

Cloud environments were not designed with a traditional perimeter. Data, applications, and workloads are distributed across multiple providers, regions, and services — accessible from any location by any device. This makes Zero Trust not just compatible with cloud security, but essential to it.

WHY CLOUD DEMANDS ZERO TRUST

When your infrastructure lives in AWS, your applications run in Azure, and your employees work from anywhere, IP-based trust controls become meaningless. A user in Chicago and an attacker in another country can both present the same IP range if they're using the same cloud region. Identity-based verification replaces location-based trust entirely.

CLOUD SECURITY CHALLENGES ZERO TRUST ADDRESSES

- No defined perimeter — resources are accessible from anywhere
- Dynamic workloads — servers spin up and down automatically
- Shared responsibility model — cloud providers secure infrastructure, you secure data
- Multi-cloud environments — each provider has different security models
- Shadow IT — employees adopt cloud services without IT approval

CLOUD ACCESS SECURITY BROKER (CASB)

A CASB sits between your users and cloud applications, enforcing security policies on cloud service usage. It provides visibility into which cloud apps are being used, controls data movement to and from cloud services, enforces compliance policies, and detects threats like account compromise and data exfiltration.

SECURE ACCESS SERVICE EDGE (SASE)

SASE converges network security and wide-area networking into a single cloud-delivered service. It combines SD-WAN, CASB, ZTNA, Secure Web Gateway, and Firewall-as-a-Service into one platform — applying Zero Trust policies consistently regardless of where users, devices, and applications are located.

ZERO TRUST NETWORK ACCESS (ZTNA)

ZTNA is the modern replacement for VPN. Instead of granting network-level access and trusting the user to access only what they should, ZTNA grants access to specific applications only — based on identity verification and device compliance. Users never touch the network directly; they access only the resources they need.

VPN

Extends network access to remote users. Grants broad network-level trust after authentication.

ZTNA

Grants access to specific apps only. Verifies identity, device, and context continuously.

- **Zscaler ZPA**
- **Cloudflare Access**
- **Palo Alto Prisma Access**
- **Cisco Duo**
- **Okta Workforce**
- **Microsoft Entra**
- **CrowdStrike Falcon**

09

How to Implement Zero Trust

A Practical 4-Step Roadmap

BEMI IT SOLUTIONS

Zero Trust implementation can feel overwhelming — especially for organizations with complex existing infrastructure. The key is to follow a structured approach, start with the highest-value controls, and build iteratively rather than attempting a complete transformation at once.

STEP 1: DEFINE YOUR PROTECT SURFACE

The protect surface is not your entire attack surface — it is the subset of your environment that matters most. It includes your most sensitive data, your most critical applications, the assets that keep your business running, and the services your customers depend on. Unlike the attack surface, the protect surface is manageable and finite.

PROTECT SURFACE CATEGORIES (DAAS MODEL)

- Data — what data is most sensitive? PII, financial records, IP, credentials
- Applications — which apps process or store sensitive data?
- Assets — which physical and virtual assets support critical functions?
- Services — which services (DNS, DHCP, Active Directory) are critical?

STEP 2: MAP TRANSACTION FLOWS

Before you can protect something, you must understand how it works. Map how data flows through your environment — who accesses it, from what devices, from what locations, through what applications, and for what purposes. This map is the foundation of your Zero Trust policy. You cannot write good policy for traffic you don't understand.

STEP 3: ARCHITECT ZERO TRUST CONTROLS

With your protect surface defined and transaction flows mapped, you can now architect Zero Trust controls tightly around that protect surface. This includes deploying a next-generation firewall or segmentation gateway at the protect surface boundary, enabling identity-based access controls, and implementing the micro-segmentation that protects internal resources.

Phase 1 — Identity

Deploy MFA everywhere. Implement SSO. Enable conditional access. Enforce least privilege.

Phase 2 — Devices

Enroll all endpoints in MDM. Enforce compliance checks before access is granted.

Phase 3 — Networks

Segment the network. Enforce east-west controls. Deploy ZTNA to replace VPN.

Phase 4 — Data & Apps

Classify and encrypt data. Apply app-level access controls. Deploy CASB.

STEP 4: MONITOR AND IMPROVE

Zero Trust is not a project — it is a continuous practice. Deploy a SIEM to aggregate and analyze security logs. Implement UEBA to detect behavioral anomalies. Run regular access reviews to remove excessive permissions. Conduct tabletop exercises and penetration tests to validate your controls. Measure your maturity against CISA's Zero Trust Maturity Model and improve systematically.

SIEM SOAR UEBA DLP PAM MDM CASB ZTNA SASE EDR XDR

10

Zero Trust Is a Journey

Start Today. Improve Every Day.

BEMI IT SOLUTIONS

The most important thing to understand about Zero Trust is that it is not a destination — it is a continuous improvement journey. No organization achieves perfect Zero Trust. The goal is to continuously reduce implicit trust, improve visibility, tighten access controls, and shrink the blast radius of any potential breach.

CISA ZERO TRUST MATURITY MODEL

CISA defines three levels of Zero Trust maturity — Traditional, Advanced, and Optimal — across each of the five pillars. Most organizations begin at Traditional, where security relies heavily on perimeter controls and manual processes. The journey to Optimal involves automating trust decisions, eliminating implicit trust across all pillars, and continuously evaluating security posture in real time.

MATURITY LEVEL OVERVIEW

- Traditional — perimeter-based, manual processes, limited visibility
- Advanced — identity-centric controls, some automation, improved monitoring
- Optimal — fully automated, real-time posture assessment, no implicit trust

WHERE TO START: THE HIGHEST ROI STEPS

If you are beginning your Zero Trust journey, prioritize these actions. They deliver the greatest security improvement for the least complexity and cost:

- Deploy MFA for all users, especially privileged accounts — blocks 99.9% of credential attacks
- Implement single sign-on (SSO) with conditional access policies — centralizes identity enforcement
- Enroll all endpoints in MDM with compliance policies — stops non-compliant devices at the door
- Audit and remove excessive permissions — reduce standing privileges to absolute minimum
- Enable logging and monitoring for all authentication events — creates visibility for detection
- Segment your network — even basic segmentation dramatically reduces lateral movement

BUILDING YOUR ZERO TRUST ROADMAP

A practical Zero Trust roadmap spans 12–24 months for most organizations. Begin with identity and device controls in the first 90 days — these deliver immediate protection. Extend to network segmentation and application controls in months 3–12. Mature your data classification, DLP, and continuous monitoring in the second year.

Days 1–90

MFA everywhere. SSO deployment. MDM enrollment. Conditional access baseline policies.

Months 3–12

Network micro-segmentation. ZTNA deployment. PAM implementation. App-layer controls.

Year 2

Data classification and DLP. CASB deployment. SIEM/UEBA. Continuous monitoring maturity.

Ongoing

Access reviews. Penetration testing. Maturity assessment. Policy refinement.

THE ZERO TRUST MINDSET

Beyond the technology and the controls, Zero Trust is a mindset. It requires security teams, IT teams, executives, and end users to operate with the assumption that threats are everywhere and that verification must be continuous. This mindset shift — from 'we have a firewall, we're safe' to 'we verify everything, always' — is the real transformation that Zero Trust requires.

The organizations that successfully adopt Zero Trust are not the ones with the biggest budgets. They are the ones with a clear vision, a phased roadmap, and the discipline to improve one control at a time. Start today. Every control you add makes lateral movement harder, reduces your blast radius, and brings you closer to a security posture that attackers find genuinely difficult to overcome.

CONTINUE YOUR CYBERSECURITY JOURNEY

More Training at Bemi Tech Solutions

%¶ YouTube Training
youtube.com/@insightswithrayslater

Ø<ß Website & Courses
bemitechsolutions.com

Ø=ÜÚ More Ebooks
kokumorix.gumroad.com

Ø=Üe Community & Mentorship
skool.com/@ransford-slater-2081