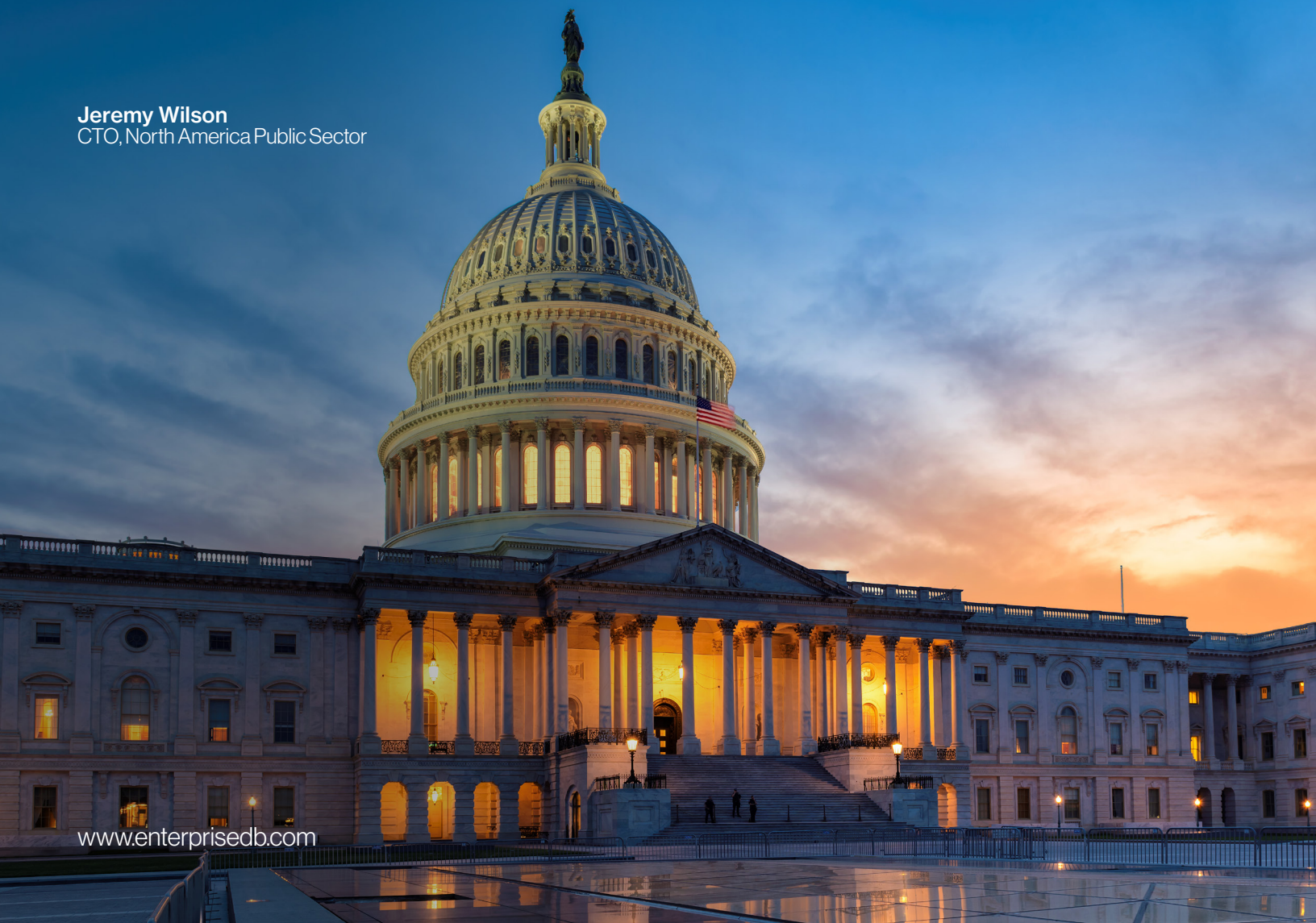
EDB
Postgres® for the AI Generation

# How EDB Can Help Organizations Along Their Zero Trust Journey

It all starts at the core – and the core is the database.

**Jeremy Wilson**
CTO, North America Public Sector



www.enterprisedb.com

## TABLE OF CONTENTS



# Introduction

In the digital age, data is the new currency. Organizations of all sizes need to manage a vast amount of data to remain competitive. Databases are the backbone of any organization's information, storing critical data such as customer information, financial data, and intellectual property. As such, databases are a prime target for cybercriminals who use a variety of techniques to gain unauthorized access to databases, including SQL injection, cross-site scripting, and brute force attacks. Database security is therefore critical, and requires the implementation of security measures to protect sensitive data stored in the database from unauthorized access, modification, or destruction.

On May 12, 2021, the Biden administration issued an Executive Order on Improving the Nation's Cybersecurity, with a strategic focus on the implementation of a Zero Trust security model. The executive order mandates that all federal agencies implement a Zero Trust model by the end of fiscal year 2024 in order to reinforce the government's defenses against increasingly sophisticated and persistent threat campaigns. The move toward a Zero Trust model is a significant shift in cybersecurity strategy that emphasizes continuous verification and strict access controls, and the executive order is seen as a critical step toward enhancing the security of federal networks and data.

## What is a Zero Trust model and what does it impact?

First, let us address what the Zero Trust model means and how EDB can help organizations along their Zero Trust journey. The term Zero Trust refers to a security model that is designed to prevent cyberattacks by assuming that every request to access a system, network, or application could potentially be a threat. This approach assumes that no user or device can be fully trusted, regardless of whether they are inside or outside the organization's network perimeter. As a result, it requires continuous verification of every user's identity, device, and access privileges before granting them access to resources.

Traditionally, most organizations have relied on perimeter-based security models, where they establish a secure boundary around their network and allow users to access resources within that boundary without requiring additional authentication. With this model, organizations focus on firewall security to protect the boundary and lean on asset management practices to ensure that only managed workstations and servers are able to operate within the environment. The model inflated the confidence in environmental security, lowering authentication barriers to access internal resources. But this approach is no longer effective in today's threat landscape, where cyberattacks are becoming more sophisticated and users are accessing resources from various locations and devices.

A key tenet of the Zero Trust model is the principle of least privilege, which means that users and accounts are granted only the minimum level of access necessary to perform their job functions. Additionally, regular access certifications ensure access isn't accumulated over time or mistakenly approved. Through proper scoping of account access and ongoing oversight, the abuse of privileges by a threat actor is made more difficult.

Network segmentation is an additional form of least privileged access control. Organizations and network engineering teams often opt for flat network designs, which allow for easier maintenance and higher levels of availability. Network segments often are defined as VLANs, for client and server networks, but rarely enforce logical restrictions on traffic that is allowed to traverse each segment. In a Zero Trust model, critical systems and components are divided into micro-segments, with strict ingress and egress managed through logical access controls. Much like account access, this hardening of network access limits the ability to move laterally across the network.

Strong forms of authentication help with increasing the confidence that someone connecting to a system is in fact the authorized user. Multi-factor authentication (MFA) requires users to provide two or more forms of identification, such as a password and a hardware key, before they can access a resource. Logging and monitoring practices help identify potential abuses and can prevent even a user leveraging strong forms of authentication from accessing the network. In the Zero Trust model, user activity and network traffic is continuously monitored to detect and prevent unauthorized access. Security analytics, machine learning, and increasingly, artificial intelligence can help identify abnormal user behavior and potential threats.

# Principles of the Zero Trust model

### Never trust, always verify

The foundational principle of Zero Trust is to "never trust, always verify." Unlike conventional security models that enforce security measures primarily at the perimeter level, Zero Trust dictates that trust should not be assumed even if the access request originates from within the organization's network. Every access request must be authenticated, authorized, and continuously validated for security configuration and posture before granting access and privileges. This principle is applied through strong management of user identities, workstations, and micro-segmented networks that allow for conditional access when each has been sufficiently verified at the time of accessing a resource.

### Assume breach

Under the Zero Trust framework, security teams operate under the assumption that their IT environments may already be compromised. This pragmatic assumption compels organizations to adopt a more rigorous and proactive security stance. Organizations implement stringent access control measures and micro-segmentation to minimize the impact of a breach. By segmenting networks and applying strict access controls, the movement within the network by malicious actors is limited, reducing the blast radius of any attack.

### Verify explicitly

Every access request must be explicitly verified using all available data points, including user identity, location, device health, service or workload, data classification, and scoring any anomalies. Explicit verification is typically achieved through the deployment of policy engines and security policies that make real-time decisions based on comprehensive contextual information and can enforce access restrictions with control points within the environment.

### Use least privilege access

This principle involves limiting user access with just-enough-access (JEA) and just-in-time-access (JIT) principles, which provide users only the access necessary to perform their job functions. The practical implementation of least privilege can involve role-based access control (RBAC), where users are given access rights based on their job role, and conditional access policies that enforce restrictions based on the user's context and accumulated risk score.

### Enforce microsegmentation

Microsegmentation is a method of creating secure zones in data centers and cloud environments to isolate workloads and components from one another and secure them individually. It helps protect sensitive data by limiting lateral movement within a network, which can prevent the spread of unauthorized access from one segment of the network to another through the use of privilege escalation.

### Monitor and maintain security posture

Constant monitoring of all network and information assets is crucial in Zero Trust. This involves detecting and responding to threats in real time, maintaining and improving the security posture, and using advanced analytics to understand and predict security risks. This can be managed by deploying security information and event management (SIEM) systems, anomaly detection tools, and endpoint detection and response (EDR) solutions.

### Emphasize device security

Device security is paramount in the Zero Trust model. Every device attempting to access a resource is treated as a potential threat vector. Organizations enforce security policies that ensure devices are properly configured, updated, and free of vulnerabilities before they can connect to network resources. Factored into the policy engines should be the risk score of a workstation, and at the time of authentication and thereafter, a low-scoring device loses its ability to access resources.

## How EDB Postgres plays a critical role in a Zero Trust model

Postgres plays a critical role in a Zero Trust model by providing a foundational platform that provides secure and auditable data storage with a flexible API that can be integrated with many other Zero Trust security components. Examples of some of these security components include identity and access management (IAM), data loss protection (DLP), analytics, automation, data management, application and network security, and many others.

Additionally, Postgres has built-in security features that can help ensure that all data stored in the database is secure. Postgres supports row-level security (and column-level security upcoming), which allows administrators to restrict access to specific rows in a table based on the user's role or other attributes. This feature ensures that only authorized users can access sensitive data. Postgres also supports SSL/TLS encryption for secure communication between the client and the server.

## Core areas where Postgres augments a Zero Trust model

### Access control

Postgres supports RBAC, which allows administrators to define specific permissions for each user or role, and MFA, which requires users to provide two or more authentication factors, such as a password and fingerprint, before gaining access to the database.

### Encryption

Postgres also supports various forms of data encryption, including transparent data encryption (TDE), which encrypts data at rest, and SSL/TLS encryption, which encrypts data in transit. File system encryption, columnar encryption, and full disk encryption are also supported. These encryption technologies can help protect sensitive data and ensure that it is only accessible to authorized users.

### Auditing

Postgres provides detailed logging and auditing capabilities, allowing administrators to monitor and analyze database activity. This can help detect and respond to suspicious or unauthorized access attempts, providing an additional layer of security in a Zero Trust environment.

### Backup and recovery

Finally, it is important to ensure that the database is regularly backed up and that a disaster recovery plan is in place. This can be achieved by implementing a backup and recovery solution that can quickly restore the database to a previous state in the event of a security breach or other disaster. Additionally, it is equally important to ensure backups are encrypted to protect sensitive data from unauthorized access and ensure compliance with policy and regulations.

## Steps to integrate Postgres into a Zero Trust model

Integrating Postgres into a Zero Trust model requires careful planning and execution to ensure that sensitive data is protected. Here are the general steps to integrate Postgres into a Zero Trust model:

1. **Define the scope:** Start by defining the scope of the project. Identify the databases that need to be integrated into the Zero Trust model and the sensitive data they contain.

2. **Identify access requirements:** Determine what application service accounts are required and tailor access to the connection application function, segmenting when sensible. Determine which users need administrative access and create secondary administrative accounts for those users for operational purposes. Lastly, determine which end users need access to the databases and scope their access using least privileged access. This will help you create the necessary security policies and controls to restrict access to only those who need it.

3. **Implement network segmentation:** Segment the network to isolate the databases from the rest of the network. Use firewalls or VPCs, leveraging access control lists to restrict traffic to only traffic locations. For example, if only three applications require a data client connection, the resulting ruleset should only allow ingress from the application network segments, and limit outbound network access to the internet.

4. **Implement identity and access management:** Implement an identity and access policy engine that ensures that only users with strong forms of authentication, healthy and compliant workstations, and allowed network segments can access the databases. Use MFA and RBAC to limit access to only the necessary users, and regularly review access for all users.

5. **Data encryption:** Encrypt the data at rest and in transit to protect it from unauthorized access. Use strong encryption algorithms and key management practices to ensure that the encryption keys are secure.

## Your Zero Trust journey starts with Postgres and EDB

In summary, EDB Postgres is designed to support a Zero Trust model by providing a secure and controlled environment and utilizing strong access control and encryption mechanisms to prevent unauthorized access to sensitive data. Strong authentication protocols such as RBAC and MFA are also supported to ensure that only authorized users can access the database. A Zero Trust model also requires constant monitoring and auditing of database access activities to detect any suspicious behavior or anomalies. EDB Postgres supports robust monitoring and auditing tools to help quickly identify any potential threats and take appropriate measures to mitigate them.

As government organizations continue to adopt a Zero Trust model, the need for robust and efficient database management solutions becomes more critical than ever before. By implementing strong access controls, encryption mechanisms, auditing and monitoring tools, and a backup and recovery plan, organizations can significantly improve their overall security posture and ensure their data is secure and protected from unauthorized access or data breaches.


EDB provides a data and AI platform that enables organizations to harness the full power of Postgres for transactional, analytical, and AI workloads across any cloud, any time.

For more information, visit www.enterprisedb.com.