POWER TO POSTGRES

Accelerate Government's Zero Trust Journey with EDB Postgres

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

Jeremy Wilson
CTO, NA Public Sector, EDB

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

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 system and database security is a critical aspect. It involves the implementation of security measures to protect sensitive data stored in the database from unauthorized access, modification, or destruction. They store critical data such as customer information, financial data, and intellectual property. As such, databases are a prime target for cybercriminals. Hackers use a variety of techniques to gain unauthorized access to databases, including SQL injection, cross-site scripting, and brute-force attacks.

On May 12, 2021, the Biden administration issued an Executive Order on Improving the Nation's Cybersecurity, which includes a section on Zero Trust 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 towards 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 towards enhancing the security of federal networks and data.

"The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in the philosophy of how we secure our infrastructure, networks, and data, from verifying once at the perimeter to continual verification of each user, device, application, and transaction."

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

First, let us address what the Zero Trust model means and additionally how EDB can help organizations along their Zero Trust journey. The term Zero Trust refers to a security model that is designed to prevent cyber attacks 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. However, this approach is no longer effective in today's threat landscape, where cyber attacks are becoming more sophisticated, and users are accessing resources from various locations and devices.

The Zero Trust model operates on the principle of least privilege, which means that users are granted only the minimum level of access necessary to perform their job functions. This is achieved by implementing strict access controls, such as multi-factor authentication (MFA), role-based access control (RBAC), and network segmentation.

MFA requires users to provide two or more forms of identification, such as a password and fingerprint, before they can access a resource. RBAC ensures that users are granted access only to the resources that are necessary for their job functions. Network segmentation divides the network into smaller, isolated segments, which reduces the potential impact of a cyber attack and limits lateral movement within the network.

The Zero Trust model also involves continuous monitoring of user activity and network traffic to detect and prevent unauthorized access. This is achieved through the use of security analytics, which uses machine learning and artificial intelligence to identify abnormal user behavior and potential threats.

The Zero Trust model is based on the following principles:

Verify explicitly: Every single access request must be authenticated, authorized, and verified before access is granted.

Least privilege: Users and devices must only have access to the resources they need to perform their tasks or duties.

Assume breach: The Zero Trust model assumes that attackers are already inside the network and are trying to move laterally to gain access to sensitive data.

Segmentation: The network is segmented into smaller, more manageable parts, and access is granted based on the need-to-know principle.

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 & 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.

Here are some 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 level 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.

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 who needs access to the databases and what level of access they require. This will help you create the necessary security policies and controls to restrict access to only those who need it.

3. **Implement identity and access management:** Implement an identity and access management solution to ensure that only authorized users can access the databases. Use multi-factor authentication and role-based access controls to limit access to only the necessary users.

4. **Implement network segmentation:** Segment the network to isolate the databases from the rest of the network. Use firewalls and access controls to restrict traffic to only authorized users and applications.

5. **Encrypt data:** 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.

6. **Monitor and audit access:** Monitor access to the databases and audit all activity to detect any unauthorized access or data breaches. Use security information and event management (SIEM) solutions to monitor activity and alert any suspicious behavior

7. **Continuously review security policies:** Regularly review and update your security policies and controls to ensure that they are effective and up-to-date. Stay informed of the latest threats and vulnerabilities and adjust your security measures accordingly.

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. Also supported, is strong authentication protocols, such as RBAC and MFA 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 having a backup and recovery plan in place, organizations can significantly improve their overall security posture and ensure their data is secure and protected from unauthorized access or data breaches.

About EDB

EDB provides enterprise-class software and services that enable businesses and governments to harness the full power of Postgres, the world's leading open source database. With offices worldwide, EDB serves more than 1,500 customers, including leading financial services, government, media and communications and information technology organizations. As one of the leading contributors to the vibrant and fast-growing Postgres community, EDB is committed to driving technology innovation. With deep database expertise, EDB ensures extreme high availability, reliability, security, 24x7 global support and advanced professional services, on-premises, in the cloud or a hybrid. This empowers enterprises to control risk, manage costs and scale efficiently. For more information, visit **www.enterprisedb.com**

POWER TO POSTGRES

Accelerate Government's Zero Trust Journey with EDB Postgres

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

Updated on May 5, 2023
EnterpriseDB Corporation
34 Crosby Drive
Suite 201
Bedford, MA 01730