Trustwave®

Database Security in a Zero Trust Architecture

.

The lifeblood of today's digital business – data – is constantly under attack from skilled, organized, well-funded cybercriminals. With ever-evolving threats such as ransomware as a service, phishing, advanced botnets and insider threats, organizations must leave behind the flawed assumption that networks are secure. The current security approaches fail to protect data as they are built on the legacy network perimeter-based approach. Today's digital business ecosystem is void of a traditional perimeter and cybersecurity professionals have far less control over networks, applications, devices, and people. This void will continue as organizations continue to adopt multi-cloud infrastructure, remain a remote workforce, and implement technology to meet the distributed demands of the business. Organizations must shift to a data-centric Zero Trust approach which will allow them to transform their security programs to match changes required for operating today and in the future.

What is Zero Trust?

Zero Trust works on the principle of "never trust, always verify". It is an assumption of breach and that risk is an inherent factor both inside and outside the network.

As defined in NIST SP 800-207, "Zero Trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

Fast Fact

John Kindervag, an industry analyst at Forrester popularized the term "Zero Trust" but it was coined by Stephen Paul Marsh for his doctoral thesis on computational security in April 1994.

But what does that mean?

Zero Trust is a security model focused on the premise that trust is never granted implicitly but must be continually evaluated. As a security model it centers on guiding principles to have a coordinated multi-layer defense strategy that focuses on:

- Reducing risk to critical functions and data
- Comprehensive security monitoring to identify malicious activity
- Granular and dynamic risk-based access controls
- The principle of least privilege

Zero Trust brings security to the users, data, applications, APIs, devices, networks, cloud, etc. wherever they are – instead of forcing them onto a "secure" network. In other words, Zero Trust shifts the perceived role of security restricting business to security enabling business.

Why are Organizations Moving to Zero Trust?

It is no secret that many organizations can do better with their security programs. Zero Trust allows for an evolution of an organization's strategy. It also forces organizations to rethink their approach to securing data to meet the requirements of data privacy regulations and expectations from their customers and business partners.

Risk minded organizations see an opportunity to take the Zero Trust mindset and adopt it as best they can to fit their current and future state infrastructure. There is no one size fits all approach and organizations need to be cognizant of this without trying to force certain process or technology changes that may introduce more risk.

> Zero Trust is becoming the security model of choice for enterprises and governments alike. However, security leaders often don't know where to begin to implement it, or they feel daunted by the fundamental shifts in strategy and architecture Zero Trust demands.
>
> A Practical Guide To A Zero Trust Implementation, Forrester March 2021

Data is at the Center of Zero Trust

To realize a Zero Trust approach, organizations need to shift to a Zero Trust Architecture (ZTA). This required shift does not mean you need to rip out all your current security controls and start over. Zero Trust is a long-term goal, but organizations can start benefiting with technology they have today by shifting to the critical principle of limiting access to data.

There are different approaches to a Zero Trust Architecture. Some organizations might look to implement a micro-segmentation approach, while others pay more attention to enhanced identity and access governance. Organizations should adopt the one that best suits their environment but should include core components to address the guiding principles. These components include:

- **Vulnerability and configuration assessment:** This allows organizations to continuously understand the current state of their assets and remediate issues to reduce risk to critical functions and data.
- **Identity access management:** This provides management of user accounts and drives access control policies.
- **Data access policies and enforcement:** This sets the business rules for who and what have the right access to critical data. To properly enforce these policies, constant validation of privileges is necessary.
- **Continuous monitoring and visibility:** This provides detection capabilities and collects valuable information for later analysis. Visibility is needed on users, applications, devices, network, cloud, and especially data.
- **Threat intelligence feeds:** This provides information from internal and external sources to help drive changes needed to policies and configurations.

At the heart of it all is data and it should be one of the main driving forces when considering the organization's roadmap to Zero Trust.

> Apply least privilege. Don't provide more access to data and apps than users need. This is one of the most important principles of solid ZTX IAM practices. You need an annual attestation/access review process whereby managers and app/data owners review user entitlements and grant or revoke them in an identity management and governance (IMG) platform. Similarly, you must ensure that privileged users don't have access to admin functions on systems they don't need to do their job. As users move from job to job and project to project, be sure to retire their access to assets. Overprivileged users — employees, contingent workers, business partners, and customers — and dated access credentials lead to breaches.
>
> A Practical Guide To A Zero Trust Implementation, Forrester March 2021

Where does Database Security fit in Zero Trust?

Database security plays an integral part to a Zero Trust Architecture. Knowing that data is at the heart of Zero Trust, databases need to be considered as critical assets with the appropriate security considerations applied. Focused Zero Trust approaches on micro-segmentation or enhanced identity and access governance do not negate the need for strong database security controls – they only enforce it.

Just like the security focused on applications, devices, users, networks, and cloud, specific purpose-built security should be focused on databases. Data protection like encryption and masking are important technology pieces, but only address certain threats. Like the core components mentioned above, specific focus needs to occur at the database level. Databases are complex with their own authentication subsystems, security configurations, and vulnerabilities. They require specific monitoring that allows them to meet the performance demands of the business.

How does Trustwave DbProtect help?

Trustwave DbProtect proactively assesses threats to databases for organizations to gain visibility into the conditions in their on-premises or cloud databases that could lead to a data breach. It automates the security of critical data by uncovering vulnerabilities that would-be attackers could exploit, limiting user access to the most sensitive data and alerting on suspicious activities, intrusions, and policy violations.

Security teams are already using DbProtect to adhere to the guiding principles whether they are on their journey to Zero Trust or not.

- **Reducing risk to critical functions and data:** DbProtect proactively assesses database security posture uncovering security weaknesses, like vulnerabilities and misconfigurations that can be exploited by attackers and lead to data exfiltration.
- **Comprehensive security monitoring to identify malicious activity:** DbProtect continuously monitors database activity based on specific organization defined policies and will alert on potential suspicious events based on behavior analytics.
- **Granular and dynamic risk-based access controls:** DbProtect provides granular access control privilege analysis to all database accounts. This allows for the constant validation that the administration, application, and service accounts are limited to the critical function and data access required.
- **The principle of least privilege:** DbProtect provides deep analysis of the users, roles, objects, and privileges needed to enforce Zero trust ideals. This information is used by organizations to limit the database accounts to the required necessary access and to adjust and enforce data access policies.

Trustwave DbProtect will help you implement the necessary database security controls to support your journey to a Zero Trust Architecture.

- Risk management approach to database security
- Purpose-built vulnerability assessment for databases
- Customizable database activity monitoring based on intelligent behavioral analytics
- One solution to protect your data on premises or in the cloud
- Focused discovery, analysis, and protection of your sensitive data
- Remediation intelligence provided by Trustwave SpiderLabs dedicated database security research team

Conclusion

As organizations consider their journey to Zero Trust, they must adopt a data-centric approach. With the focus on data and understanding where it lives and who and what is accessing it, it is clear database security is a critical piece to a Zero Trust Architecture. It is essential to have the necessary insights to the risk of data in databases, have visibility to know when malicious activity is happening, and the detailed information to constantly validate that user access is limited to meet the needs of the business.