GitLab

6 Key Considerations for Implementing Zero Trust

DEIMOS

Secure your software supply chain end-to-end

The race for government agencies to achieve Zero Trust security goals has officially begun. The Office of Management and Budget (OMB) has mandated that all agencies must be compliant with **The Federal Zero Trust Strategy** by the end of FY 2024. The OMB mandate has a broad reach with a trickle-down effect on state and local governments, including educational institutions in the form of the **CISA Cybersecurity Framework** and available budget for cybersecurity.

Because all agencies, vendors, and education institutions are responsible for protecting data, Zero Trust is mission critical. But what exactly is Zero Trust and how do you begin to implement it?

The concept of Zero Trust has existed in the software industry for some time. It is based on the idea that no device, user, or application attempting to gain access to a system should be assumed to be secure. This aligns with modern application development and DevSecOps, shifting security left to ensure a secure end-to-end software supply chain — *securing the speed to mission.*

Achieve Zero Trust within your DevOps platorm with these six key considerations.

1 Role-Based Access

Ensure teams are structured on a need-to-know basis for information, allowing them to accomplish their tasks. **Permissions and roles** allow users to have different abilities and access depending on their role in a particular group or project.

Authenticate users and Machines 2

Implement an **SSH** protocol to securely communicate and authenticate to a remote server. This provides an additional level of security before allowing access without requiring users to supply a username and password every time. **Two-factor authentication** (2FA) adds another layer of protection by requiring users to present two factors to gain access: their identity (username and password) and the second factor of authentication, typically a device such as a mobile phone or an email account enabled for 2FA.

3 Continuous authentication and authorization

Reinforce development and deployment processes with continuous authentication within a continuous integration and continuous deployment (CI/CD). Users will have a single interface to identify the change, manage monitoring, respond to, and remediate issues that arise postdeployment.

Monitor and Respond 4

Improve visibility of and insight into security vulnerabilities, including how to remediate them, by monitoring the security status of users and machines. **Security Dashboards** provide an overview of trends about vulnerabilities detected by security scanners. Vulnerability reporting provides security teams with the ability to manage vulnerabilities, including triaging, setting priorities, and enable communication within the team.

5 Classify Data

Maintain quality and security standards with Low-to-High workflows. Set and enforce access levels accordingly with isolated development environments that are inaccessible to unauthorized users.

Audits and Reports 6

Ensure adherence to licensing compliance and regulatory frameworks with real-time data access audits and compliance reports. Audit Events make it easy to view all audit events, such as **MR approval auditing** and **compliance framework changes**. **Streaming Audit Events** maintain change records for audits via audit logs and streaming audit events, helping to consolidate audit events in a central Security Information and Event Management (SIEM) tool.

Zero Trust with GitLab

Setting up Zero Trust on your DevSecOps platform is achievable when considering these six factors. GitLab, The One DevOps Platform, supports an ecosystem of Zero Trust principles. GitLab has a history of supporting the DevSecOps initiatives of U.S. federal, state, and local government agencies, vendors, and educational institutions with one end-to-end software development platform that meets strenuous security and compliance requirements.

Talk to Deimos today about how GitLab can help you secure your speed to mission.

GitLab

Lock image courtesy of Unsplash.com

DEIMOS