STRONGNETWORK

Virtual Workspace Infrastructure

Secure Cloud IDEs for Global Development Teams

Platform Benefits

- Standardize stacks for code development using software containers
- Deploy development environments (aka workspaces) across your entire team over the web
- Free your developers from their devices by providing them Cloud IDEs (vscode, jetbrains, etc.)
- Access all applications for development (GitHub, GitLab, Jira, etc.) through a secure Chrome-based browser
- Protect your source code and data, application credentials against exfiltration, leaks, and reuse
- Implement a complete Zero-Trust Architecture over your development assets to control and monitor access
- Make your entire development process compliant with ISO 27001's risk controls

Solution Delivery

Enterprise Private SaaS

- Installed on your premises or at your cloud provider
- Fully managed service available

Public SaaS

- For SMEs and start-ups, self-served
- Available at https://strongworkspace.com/

Use Cases

- Streamline the delivery of IT infrastructure for development for cost and security
- Onboard freelancers and contractors while protecting your assets
- Allow your developers and data scientists to BYOD in your company or from home
- All the above together!

Check our website now and contact us for more information!

Platform Features (Enterprise Private SaaS)

Workspace Infrastructure and Teams

- Create and provide access to development workspaces: IDE (vscode, Jetbrain's, vim, emacs, etc), software container and terminal
- Provide monitored access through a Chrome-based browser to SAML-enabled applications such as GitHub, GitLab, BitBucket, Confluence, etc. with Single Sign-On. Prevent credential leaks, access to security sensitive functions (source code downloading, key registration, etc.)
- Import and manage all your development software stacks with containers from any public or private docker registry
- Extensive developer functions that simplify workflows, credential management, etc and improve development environment performances
- Support for organizations and projects to manage the composition of teams and control access to development resources
- Management of user roles and resource access using a Role-based Access Control (RBAC) model, with creation of custom roles
- Full platform API for programmatic control of all platform functions and access to all data analytics, logs, etc.

Secure Management of all Development Resources and Data

- Zero-trust access to GIT applications from workspaces with secure and automated management of all private and public keys
- Support for accessing data buckets from workspaces and version control data across multiple clouds (AWS, Azure, GCP, etc.)
- Creation and management of credentials, tokens and other types of secrets with integration to 3rd-party secret management tools
- Monitored access control from workspaces to HTTPS, SSH and TCP services, including legacy Oracle JDBC, IBM CICS, and others
- ISO 27001's risk control-compliant management of all resources, including confidential data and Personally Identifiable Information (PII)

Identity and Access Management (IAM)

- OAuth with support for Okta, Google and Azure for Single Sign-On (SSO) to the platform in an enterprise setting
- Multi-Factor Authentication
- Support for SSO authentication to SAML-enabled applications used by developers for credential leak/reuse prevention
- Fully ISO 27001-compliant management of IAM functions

Zero-Trust Access Control

- Deploy a 4-level micro-segmentation for Zero-Trust access management across the entire development process and all participants
- Attach network policies to workspaces to log and enforce traffic monitoring, restriction and inspection
- Deploy public-private key credentials automatically and keep them under the control of the organization (unavailable directly to users)

Active Code and Data Protection

- Enable clipboard monitoring and operations logging for workspaces for data leak prevention
- Log and store all data traffic activities (clipboard, network, etc.) for inspection and ISO 27001 compliance with data exfiltration prevention
- Automate the creation of security reviews when users are pasting code originating from outside the IDE (Stackoverflow, etc.)
- Control network access from software containers deployed for development using network policies

Dasboards, Logs and Reporting

- Full security dashboards including extensive security logs with over 100 events
- Team performance dashboards with types of development activities, time duration for real-time process governance

https://strong-network.com @ Strong Network @ Readings Strong Network hello@strong.network +41 76 348 38 61

Y-Parc Swiss Technopole, Rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland