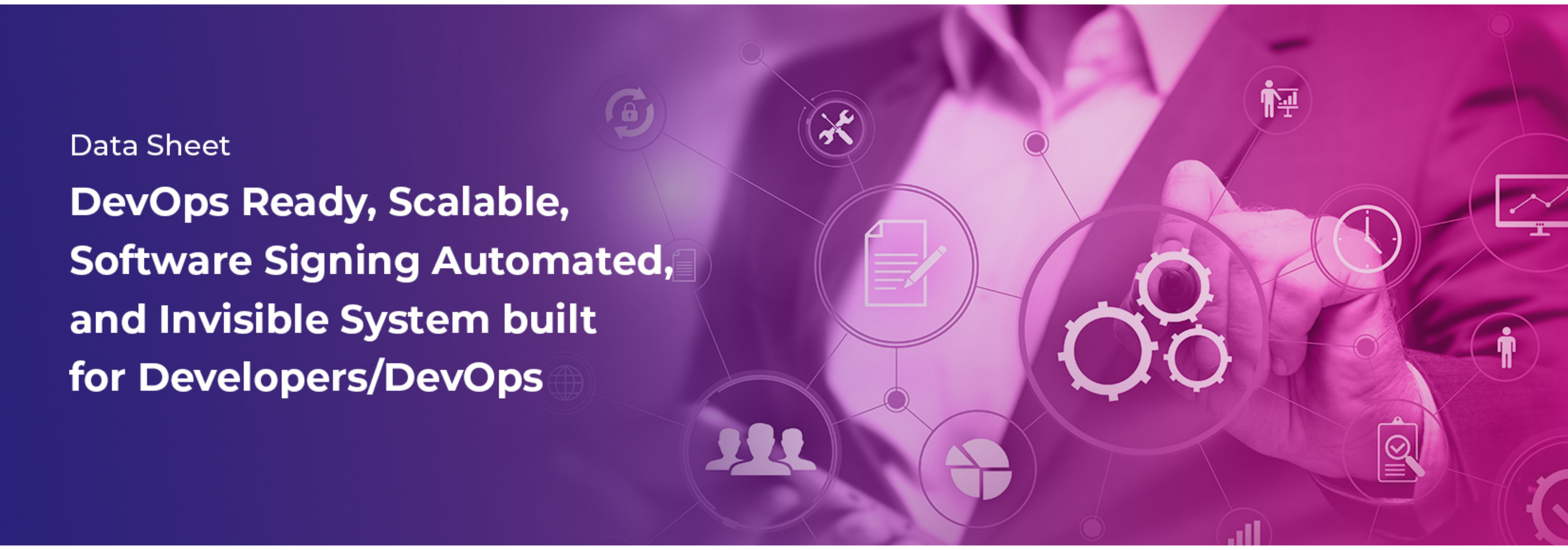
AUJAS CYBERSECURITY

NSE NSEIT



Data Sheet

DevOps Ready, Scalable, Software Signing Automated, and Invisible System built for Developers/DevOps

Key Features

- Tightly integrated with build process, signing process is leak free.
- Enterprise-grade malware scanner to inspect files for malware.
- Cross platform and multiple certificate (standard, EV and self-signed certificates) support.
- Over 50 filetypes supported. Plugin based support for new file types.
- Includes Basic signing, GPG signing, Hash sign, Force signing, Append signing, MAGE, WHQL and many more.
- Use any CA, including your own.
- support for HSMs & secure key manage-ment.
- Built-in workflows and audit trail of approvals and signing actions.
- Highly scalable signing more than 12 million files per year.

CodeSign by Aujas is a secure, automated, and DevOps ready solution that ensures the integrity of software applications, protects the signing keys, with full audit trails, and helps combat malware. It allows unmatched versatility to sign all file types across all platforms.

Why CodeSign

Unified and Centralized

- Automated code signing platform that consolidates the process at organization level; establishes a unified way of signing.
- Tightly integrated with build process, signing process is leak-free.

Secure

- Enterprise-grade malware scanner to inspect files for malware.
- Cloud HSM for secure storage of signing keys, moves the keys away from organization; implies more security, increases the trust.
- Role-based approval provides complete control over every code signing activity.
- Automated audit trails make the process transparent for Infosec team.

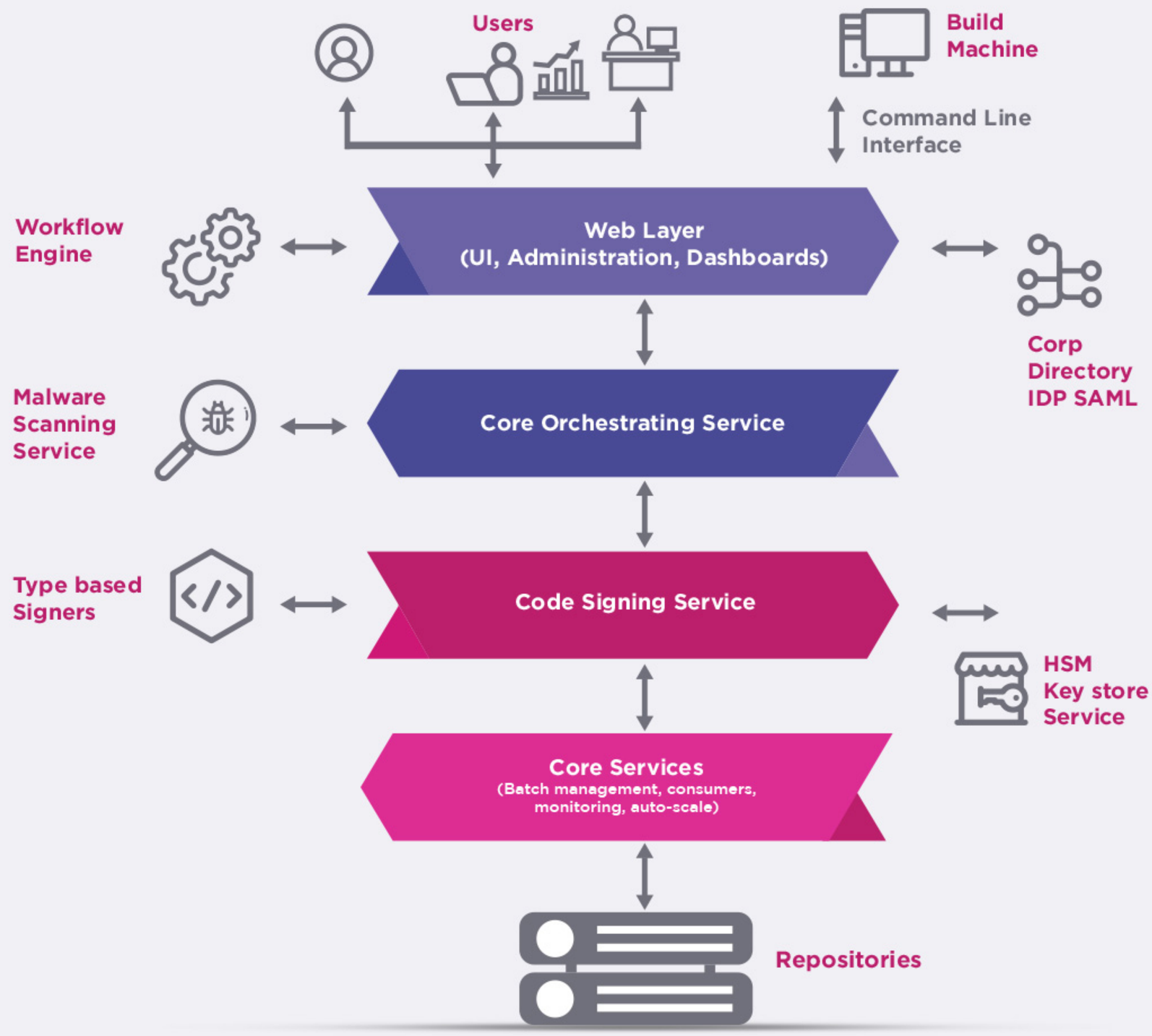
Development Friendly

- Easy CLI integration with options to submit file signing parallelly.
- Can easily become part of DevOps pipeline.

Easy to Buy

- Pay as use, flexible payment model, number of signing based licensing.

Functional Architecture



CodeSign provides a role-based approval process with workflow engine in place along with integration with corporate directory, to ensure secure signing process and enforce code signing policies. Code signing keys are securely stored in HSM or secure keystore. CodeSign is a secure, automated, and highly scalable signing solution.

Key Specifications

Architecture Style

i. Micro Services – Improved modularity, high scalability

File Type Support

1	Windows	dll, exe, js, sys, msi, vbs, msp, ocx,cp1,ps1,wsf,cab
2	Java	jar, war, ear,hpi
3	Android	apk
4	RPMV3, RPMV4	rpm
5	GPG	Any Linux file types
6	Docker	Docker Images
7	IOS/MAC	dmg, ipa, pkg, app
8	XAR	xar, safariextz
9	MAGE	manifest, exe.manifest,application
10	HLK/WHQL or Driver	sys, cat, dll, HLKX
11	VSIX	vsix
12	Debian	Deb
13	HELM Chart	HELM Chart

*Plugin based approach to support and add new file type signing

Certificate Types

i. Self-Signed Certificates
ii. Standard Code Sign certificate issued by any CA
iii. Extended Validation/ EV certificate

Mode of Signing

i. Hash Signing (This mode will not support file scanning process)
ii. Remote Signing

Product Hosting

i. On premise: software runs in Customer Data Center
ii. Public Cloud: software runs in Public Cloud Services Data Center (Amazon, Azure)
iii. Managed Cloud: software runs in Private Data Center (Company Data Center)

Key Value

Code signing is a proven security practice to protect and extend the trust-based usage of software systems and applications. Organizations that publish as well as consume software, need a secure code signing mechanism to ensure software authenticity. It is very important to have a secured, well-monitored, and consolidated code signing process to achieve most reliability.

CodeSign by Aujas not only makes the signing software, updates or executable easy but also takes care of **policy enforcement, access control, certificate management, secure key storage, and provides a one-stop solution for application code signing.**

Contact

Email: codesign@aujas.com

For more details, please visit codesign.aujas.com