kaspersky BRING ON THE FUTURE

Kaspersky Hybrid Cloud Security per DevOps

I team DevOps sono costantemente sotto pressione, perché devono garantire velocità, precisione e innovazione. Considerando tutto ciò, i requisiti di sicurezza possono apparire come un elemento frenante, che rischia di compromettere i risultati del delicato lavoro svolto. Tuttavia, escludere la sicurezza dai processi critici non rappresenta di sicuro la risposta più appropriata: occorre una soluzione in grado di colmare le abituali distanze fra team di sviluppo DevOps ed esperti di sicurezza IT.

Colmare le distanze fra team DevOps e Cybersecurity

Le attività DevOps sono in rapida e costante crescita: si focalizzano sulle specifiche esigenze aziendali, sul time to market, su velocità, flessibilità e completa automazione. Tuttavia, le tematiche di sicurezza IT tendono a produrre un impatto negativo su uno o più di tali parametri. Per i DevOps, a quanto pare, l'unico modo per soddisfare i propri indicatori KPI è quello di ridurre al minimo il fattore sicurezza, o bypassarlo del tutto, mentre l'Information Technology si trova in chiara difficoltà nell'identificare lo Shadow IT, fenomeno in costante crescita, e nel ricondurre lo stesso nell'ambito della sicurezza aziendale.

Le distanze attualmente esistenti vengono ulteriormente ampliate da una serie di problemi e preoccupazioni che creano problemi a entrambe le parti. Il fatto di parlare lingue diverse e perseguire KPI diversi non aiuta di certo a migliorare la situazione: si tratta di un evidente punto debole.

Fornendo ai team DevOps un set di strumenti completo e le interfacce necessarie per sfruttare tutto il potenziale di un approccio "Security as code", la soluzione Kaspersky Hybrid Cloud Security colma le distanze fra team di sviluppo DevOps ed esperti di sicurezza IT, trasformando i DevOps in veri e propri DevSecOps.

Esigenze IT	Esigenze DevOps
Gestione dei rischi a livello di sicurezza IT	Configurabilità totale
Minimo sovraccarico	Un approccio "Everything as code", compresa la sicurezza
Ragionevole aumento del numero di strumenti di gestione	Ampia gamma di piattaforme supportate
Immagine di "business enabler"	Impatto minimo sulle performance
	Dinamica: il ciclo di vita di un'entità si può risolvere in minuti o addirittura pochi secondi

Adozione di un approccio DevSecOps grazie al modello "Security as code"

Kaspersky Hybrid Cloud Security è un'efficace soluzione end-to-end altamente configurabile, in grado di creare una vera e propria cultura DevSecOps in ambito aziendale.

- Protegge le piattaforme Linux e Windows, le infrastrutture server virtualizzate e public cloud, nonché i container Docker e Windows, per impedire agli autori degli attacchi di utilizzare un livello container vulnerabile o nocivo come gateway di accesso all'infrastruttura aziendale.
- Fornisce agli amministratori IT e ai responsabili della Cybersecurity efficaci strumenti per il controllo della sicurezza, la visibilità e la gestione dei rischi.

Piattaforme supportate

Sistemi operativi:
- Windows
- Linux

IaaS:
- Google Cloud Platform
- AWS
- Microsoft Azure

Piattaforme di containerizzazione:
- Docker
- Container Windows

Piattaforme di virtualizzazione:
- VMWare vSphere e NSX
- Microsoft HyperV
- Citrix Server e Citrix Virtual Apps and Desktops
- KVM (Kernel-based Virtual Machine)
- Nutanix AHV

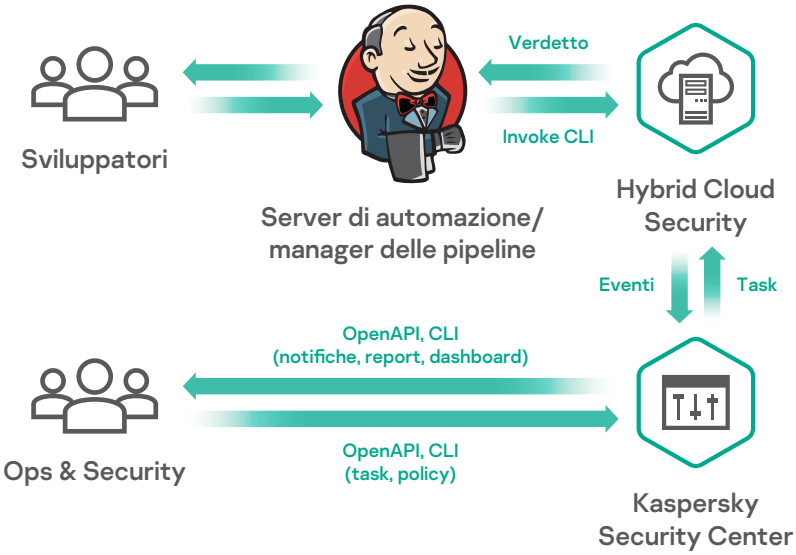
Pipeline di orchestrazione e CI/CD:
- Jenkins
- TeamCity

Interfacce:
- CLI
- API aperta

Kaspersky Hybrid Cloud Security crea un approccio "Security as code":

- Runtime della piattaforma di containerizzazione e protezione della memoria
- Controllo di immagini e container "secure by default"
- Avanzate funzionalità di Security Testing Orchestration
- "Shift left": perfetta integrazione delle routine di sicurezza nella fase di sviluppo delle pipeline CI/CD
- Funzionalità di integrazione avanzate per un approccio "Everything as code"

- Offre avanzate funzionalità per la generazione dei report e un funzionamento basato su policy.
- Presenta utili interfacce di integrazione per sofisticate funzionalità di automazione e creazione della pipeline, consentendo ai team DevOps di garantire la pulizia dei repository aziendali e disinfettare le entità provenienti dai repository pubblici.



Opzioni di integrazione avanzate

Kaspersky Hybrid Cloud Security consente ugualmente di combinare in modo controllato e sicuro procedure software lean con la generazione, il packaging e la delivery delle applicazioni just-in-time, senza alcun rallentamento dei processi.

- Le integrazioni della piattaforma CI/CD (ad esempio, Jenkins) semplificano la creazione e l'automazione delle pipeline.
- La scansione di container, immagini e repository locali e remoti all'accesso (OAS, On-Access Scanning) e on-demand (ODS, On-Demand Scanning) consente di mantenere questi ultimi protetti e pronti per le attività degli sviluppatori.
- Il monitoraggio dello spazio dei nomi, il controllo flessibile dello scope di scansione basato su maschera e la possibilità di eseguire la scansione di diversi livelli di container permettono di applicare best practice di sviluppo sicure.

Disponibile sui marketplace dei cloud pubblici

Kaspersky Hybrid Cloud Security è disponibile sulla maggior parte dei marketplace del cloud pubblico e offre varie opzioni in termini di consumo, dal modello BYOL alla subscription a lungo termine. È disponibile anche la prova gratuita: il deployment automatizzato facilita inoltre la relativa valutazione.

Sicurezza per le attività DevOps: kaspersky.com/devops
Sicurezza per AWS: kaspersky.com/aws
Hybrid Cloud Security: kaspersky.com/hybrid
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security

www.kaspersky.it

We are proven. Siamo indipendenti. Siamo trasparenti. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia possa migliorare le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Bring on cybersecurity for a safer tomorrow.

Per saperne di più: kaspersky.it/transparency

Proven. Transparent. Independent.