kaspersky BRING ON THE FUTURE

Kaspersky Hybrid Cloud Security for DevOps

DevOps steht unter dem ständigen Druck – Druck nach mehr Geschwindigkeit, mehr Genauigkeit, mehr Innovation. Aus diesem Blickwinkel betrachtet können Sicherheitsanforderungen als Hemmschuh angesehen werden, der die Arbeit von DevOps behindert. Aber die Sicherheit aus kritischen Prozessen auszuschließen, kann nicht die Lösung sein. Vielmehr sollte es darum gehen, die Lücke zwischen DevOps und Informationssicherheit zu schließen.

Schulterschluss zwischen DevOps und Informationssicherheit

Die Einführung von DevOps nimmt immer mehr an Fahrt auf, wobei besonderes Augenmerk auf unternehmerische Anforderungen, Markteinführungszeiten, Geschwindigkeit, Flexibilität und komplette Automation gelegt wird. Aber Sicherheit hat die Tendenz, sich negativ auf die eine oder andere dieser Kennzahlen auszuwirken. Für DevOps scheint die einzige Möglichkeit, ihre KPIs zu erfüllen, darin zu bestehen, die Sicherheit zu minimieren oder komplett auszuschalten. Gleichzeitig ringt die IT darum, dynamische und wachsende Schatten-IT zu identifizieren und in das Gesamtgefüge der Unternehmenssicherheit einzugliedern.

Dieser Zwiespalt wird durch eine Reihe von Bedenken auf beiden Seiten noch zusätzlich verschärft. Dass man unterschiedliche Sprachen spricht und andere KPIs verfolgt, ist dabei auch alles andere als hilfreich.

Kaspersky Hybrid Cloud Security dagegen versorgt DevOps mit einem kompletten Toolset und den erforderlichen Schnittstellen, um den Ansatz des „Security-as-Code“ vollumfänglich nutzen zu können. Damit gelingt mit dieser Lösung auch der Schulterschluss zwischen DevOps und IT-Sicherheit, indem DevOps zu DevSecOps wird.

Anforderungen der IT	Anforderungen von DevOps
Informationsrisikoverwaltung	Komplett konfigurierbar
Minimaler Aufwand	Ansatz des „Everything als Code“ – einschließlich Sicherheit
Vernünftige Zunahme an Verwaltungstools	Umfassende Plattformunterstützung
Positives Image als „Business Enabler“	Minimale Auswirkung auf die Leistung
	Dynamisch: Lebenszyklus einer Entität kann Minuten oder sogar nur Sekunden andauern

Übergang zu DevSecOps mit „Security-as-Code“

Kaspersky Hybrid Cloud Security ist ein effizientes, stark konfigurierbares Sicherheitstoolset, mit dem sich eine echte DevSecOps-Kultur in Ihrer Organisation verwirklichen lässt.

- Schützt Linux- und Windows-Plattformen, virtualisierte und Public Cloud-Serverinfrastrukturen sowie Docker- und Windows-Container, damit Angreifer schädliche Container-Komponenten nicht als Einfallstor in die Infrastruktur einer Organisation nutzen können.
- Bietet Sicherheitskontrolle, Transparenz und Risikoverwaltungstools für IT und IT-Sicherheitsadministratoren.

Plattformunterstützung

Betriebssysteme:
- Windows
- Linux

IaaS:
- Google Cloud-Plattform
- AWS
- Microsoft Azure

Containerisierungsplattformen:
- Docker
- Windows-Container

Virtualisierungsplattformen:
- VMWare vSphere und NSX
- Microsoft HyperV
- Citrix Server sowie virtuelle Apps und Desktops
- KVMs (Kernel-basierte virtuelle Maschinen)
- Nutanix AHV

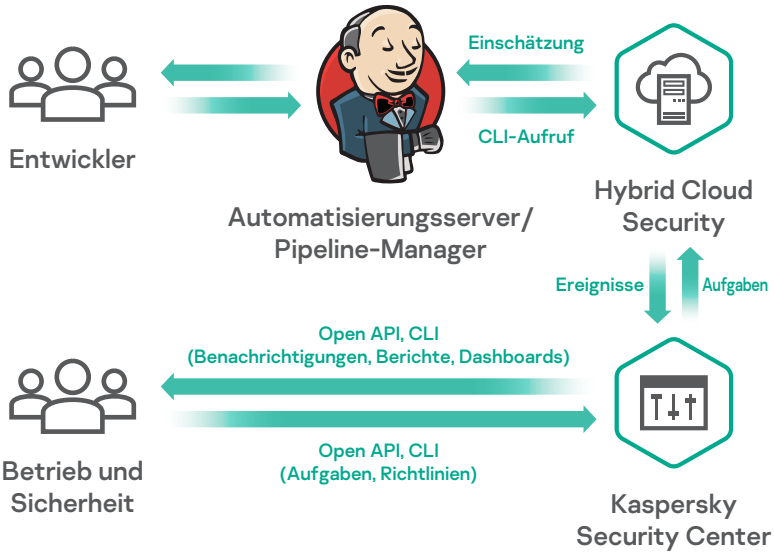
Orchestrierungs- und CI/CD-Pipelines:
- Jenkins
- TeamCity

Benutzeroberflächen:
- CLI
- Open API

Kaspersky Hybrid Cloud Security ermöglicht „Security-as-Code“:

- Laufzeit- und Speicherschutz für Containerisierungsplattformen
- Standardmäßige Sicherheitseinstellungen: Überprüfung von Sicherungen und Containern
- Orchestrierung von Sicherheitstests
- Integration von Sicherheitsroutinen in die Entwicklungsphase von CI/CD-Pipelines
- Umfassende Integrationsfähigkeiten im Sinne eines „Everything-as-a-Code“-Ansatzes

- Vielfältige Berichtfunktionen und Richtlinien-basierter Betrieb.
- Mit Integrationsschnittstellen zur Automation und für den Pipeline-Aufbau, damit DevOps firmeneigene Repositorys sauber halten und die Bereinigung von Entitäten erzwingen kann, die aus öffentlichen Repositorys gezogen wurden.



Vielfältige Integrationsoptionen

Kaspersky Hybrid Cloud Security bietet Unternehmen sichere und kontrollierte Methoden, um schlanke Softwarepraktiken mit zeitnaher Anwendungserstellung, Verpackung und Lieferung zu verbinden, und zwar ohne die Prozesse zu verlangsamen.

- CI/CD-Plattformintegrationen (z. B. Jenkins) vereinfachen den Aufbau und die Automatisierung von Pipelines.
- On-Access- (OAS) und On-Demand-Scanning (ODS) von Containern, Sicherungen, lokalen und Remote-Repositorys erleichtern die Bereinigung von Repositorys für die Belange der Entwickler.
- Namespace-Überwachung, flexible maskenbasierte Kontrolle der Scan-Umfänge und die Möglichkeit zum Scannen unterschiedlicher Container-Layer ermöglichen die Umsetzung von sicheren Best Practices in der Entwicklung.

Verfügbar in Public Cloud-Marketplaces

Kaspersky Hybrid Cloud Security ist in den meisten Public Cloud-Marketplaces erhältlich und bietet eine Reihe von Verbraucheroptionen, von der Verwendung eigener Geräte (BYOL) bis hin zum langfristigen Abonnement. Eine kostenlose Testversion mit automatisierter Bereitstellung ist ebenfalls erhältlich und erleichtert die Bewertung.

Sicherheit für DevOps: kaspersky.com/devops
Sicherheit für AWS: kaspersky.com/aws
Hybrid Cloud Security: kaspersky.com/hybrid
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven.
Transparent.
Independent.