Use Case

Defend DevOps Workflows

In Application Development

> “By 2019, only 10% of DevOps initiatives will have achieved the level of security automation required to be considered fully DevSecOps, up from less than 5% in 2017”
>
> Integrating Security Into the DevSecOps Toolchain – Gartner (Nov 2017)

SecureDoc™ by WinMagic

WINMAGIC®

The number of IT professionals working in DevOps increased from 16% in 2014 up to

27%

In 2017, according to the State of DevOps Report[1]

Top DevOps Industries[1]

1. Technology
2. Financial Services
3. Retail
4. Telecommunications
5. Education

> “DevOps stresses automation to achieve scale, but security has traditionally been slow, process heavy and gate-driven – the antithesis of automation, transparency and speed.[2]

Sources

1 2017 State of DevOps Report – Puppet (2017)

2 Integrating Secuirty into the DevSecOps Toolchain – Gartner (Nov 2017)

Transforming IT with DevOps

Today, DevOps is a set of practices and cultural values proven to help organizations of all sizes improve their software release cycles, quality and security. Traditional development models where applications are created, then handed over to operations are less reliable and slower than modern businesses demand. Under a DevOps model, development and operations teams are integrated, not siloed. A more cohesive structure throughout the development process – from design and testing to deployment and operations – enables fast and reliable delivery of applications.

More recently, high demand for applications and services in regulated industries – including financial services and healthcare – has created a greater need to integrate security best practices into infrastructure, development lifecycles, and into applications themselves.

DevOps in the Cloud Era

Virtualization and cloud computing offer DevOps teams the ability to deliver software releases faster than ever. Many organizations withhold mission-critical production workloads to the corporate datacenter or private cloud, but the public cloud is quickly becoming commonplace for DevOps as well. Meanwhile, hyperconvergence has radically simplified private cloud with the power to match IaaS platforms. All of these advancements have transformed the datacenter into a complex, hybrid and highly automated environment.

As hybrid IT becomes standard, security leaders must work to isolate and secure data in DevOps environments through advanced security technologies that can deliver information protection, without significant compromises to transparency and speed – particularly for mission-critical workloads.

95%

Of infrastructure and operations (I&O) services that use DevOps approaches will be subject to contractual obligations and regulatory compliance by 2021

Key Virtualization Risks[2]

- VM Sprawl
- Sensitive Data within a VM
- Offline and Dormant VMs
- Pre-Configured VMs
- Lack of Visibility and Controls over Virtual Networks

> “DevSecOps is the integration of security into emerging agile IT and DevOps development models, ideally without reducing agility or speed and largely transparent to developers.[3]

Sources

1 2017 State of DevOps Report – Puppet (2017)

2 Best Practices for Mitigating Risks in Virtualized Environments – Cloud Security Alliance (2015)

3 Hype Cycle for DevOps, 2017 – Gartner (Jul 2017)

Business Need: **Speed, Transparency & Security**

DevOps emphasizes speed and automation, often leaving security and compliance as afterthoughts. Even if security is a priority, existing solutions pose roadblocks to workflow, preventing DevOps from adopting secure, streamlined development processes – known as DevSecOps.

Developers need to design, test and distribute applications quickly, but security loopholes can be created without implementing data security in the development environment. This rings true particularly in "self-service" environments with high levels of automation, where workloads containing sensitive information or intellectual property can quickly and unintentionally spread to unprotected zones.

The Problem: **Workflow Risk & Interruption**

DevOps is about eliminating bottlenecks, waste and automating the System Development Life Cycle (SDLC). A key component of streamlining DevOps involves quick provisioning through automation scripts and auto-scaling tools to keep pace, as well as self-service provisioning of virtual machines or containers by developers.

DevSecOps starts with securing the infrastructure platform that developers and operations teams leverage for design, testing and production. The developers unit of work – virtual machines (VMs), containers and machine images – must be protected against known threats, whether stored and started up on-prem or in the cloud.

VM Sprawl

Images and VMs can be easily created, cloned and moved from one environment to another. DevOps automated and self-provisioning models can accelerate proliferation of data to unmanageable levels.

SecOps Headaches

OpEx becomes unpredictable with proliferation and Security Operations (SecOps) teams are overwhelmed with efforts to discover, identify and decommission unnecessary or unsecured workloads.

Inconsistent Adoption

Enforcing consistent security is complicated by inevitable human error, misconfiguration, and inconsistent adoption of secure best practices.

Residual Data

In rapid development lifecycles, where instances are frequently spun up and torn down within hours, residual images, backups and snapshots containing intellectual property and/or sensitive data can easily be left behind.

Compliance

Financial services and healthcare have particularly strict requirements for data privacy and security in some areas of production environments.

Workflow Barriers

Virtualization was designed for speed, but unsophisticated encryption solutions can often impede performance and workflow.

The Solution: **Defend DevOps Workflows with SecureDoc CloudVM**

WinMagic's SecureDoc CloudVM delivers high-performance workload encryption to meet security and compliance needs with the speed and transparency expected by DevOps. Our advanced, always-on cryptographic engine ensures that VMs are protected at rest and in transit across public, private and hybrid clouds. It enables leaders in software and application development to focus on what matters most, growing their business.

Protect Production Workloads

Isolate and protect mission-critical or production workloads with FIPS 140-2 validated VM-level encryption.

Prevent VM Sprawl

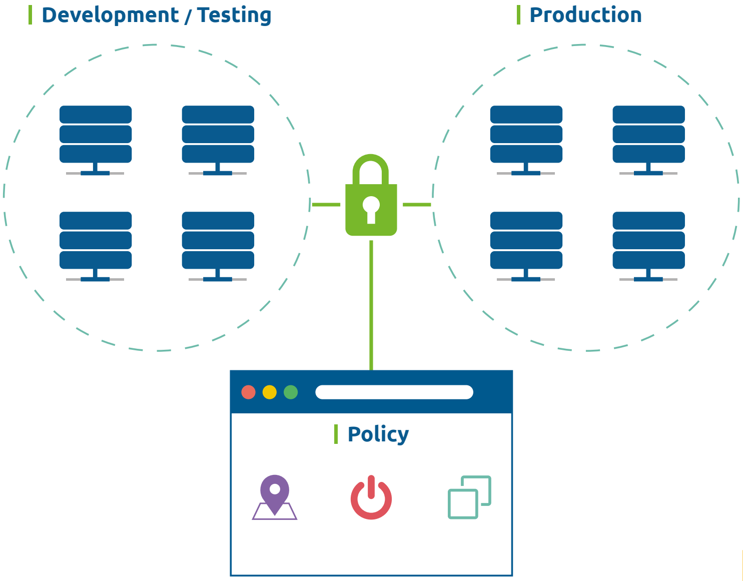
Implement clone controls and geo-fencing policies to restrict unauthorized replication or movement of data.

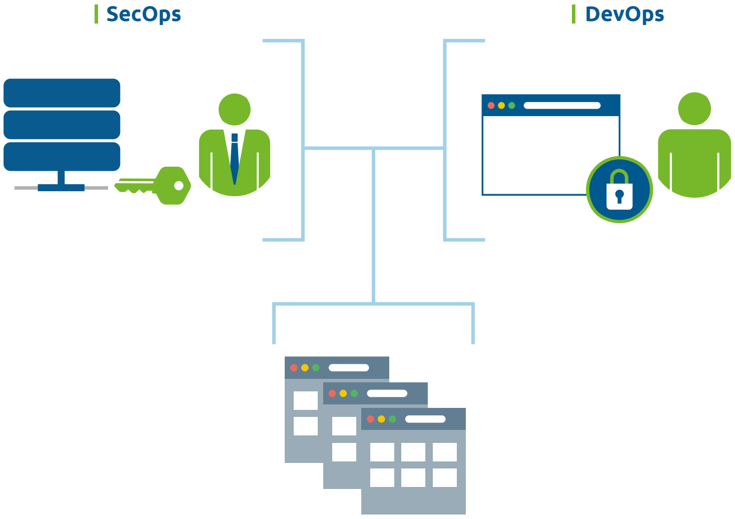
Enforce Time Management

Put in place time-based controls to protect against malicious access attempts after work hours.

Eliminate Residual Risk

Revoke keys to eliminate residual data risk and securely terminate DevOps workloads when they've expired.





Rapid Deployment

Save time, script and embed encryption within VM template libraries and master images for security and policy control by default.

Secure Automation

Workloads are seamlessly protected at rest and in transit – with support for automation tools like auto-scaling, live migration, backup & disaster recovery.

SecOps Management

Separate security from DevOps. Decryption keys are held and controlled by security admins, not developers.

Instant Visibility & Control

Instantly discover, encrypt and report on compliance status of VMs across all cloud accounts, regions and providers – including your private cloud and dedicated servers.

US & Canada	United Kingdom	Germany	Japan	India	APAC
+1 888 879 5879	+44 0148 334 3020	+49 69 175 370 530	+03 5403 6950	+91 124 4696800	+65 9634 5197