



Virtual Clouds. Why Information Security Matters?

VMware virtual cloud allows datacenter providers build reliable, cost-effective solutions. With this technology they can offer their customers almost unlimited scalability at a reasonable and well-justified price.

However, many companies haven't made the decision yet. Industry experts believe security of business-sensitive, regulated and personal information to be one of major concerns here. According to Gartner, cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing."

When selecting a datacenter provider, enterprise customers do consider not only common operation criteria such as data availability, scalability, and performance, but also all aspects of information security as well.

- **Access control.** The list of people who can assign permissions and have (potential) access to customers' data should be limited and covered by non-disclosure agreements and other legal obligations.
- **Data location.** Even within the cloud, providers must commit to storing and processing data in specific jurisdictions and make contractual commitments to obey specific national regulations.
- **Data integrity.** Customers want to be sure their virtual machines stay valid and all changes are fully controllable.
- **Compliance.** Customers may be subject to certain regulations that should be implemented and enforced for their hosted environment (for example, PCI DSS.)
- **Audit.** All activity must be closely monitored and every suspicious, inappropriate or illegal behavior should be duly reported, no matter whether and how the case had been handled by the provider.

If solution provider cannot adequately handle information security issues, this becomes a serious shortcoming.

But with a dependable technology in place, information security can be turned into a decisive competitive advantage, especially for big enterprise customers and public sector.



Security Code

In fact, virtualization provides unmatched opportunities for building information security-aware solutions. Why? Because in virtual environments you can gain such a firm separation of duties that simply cannot be achieved in physical environments.

Security Code vGate offers a comprehensive approach to information security for virtual infrastructures built around VMware technology.

vGate – Virtual Cloud, Firm Security

Access Control

vGate introduces authentication and access control perimeter – on top of the standard VMware security. Flexible vGate's security model is based on security labels associated with users, virtual machines, ESX & NAS servers, and so on.

Data center IT personnel that maintain the virtual infrastructure can be granted exactly the privileges they require to perform their assigned tasks. At the same time, they cannot access the virtual machines' data and don't have any means to self-privilege. Permissions are granted only by the dedicated high-ranked security officers, which in turn are completely restricted from accessing the virtual infrastructure.

Data Location

Based on security labels, vGate can prevent attempts to move and/or run a labeled virtual machine to/on wrong ESX hosts or store labeled machine's files on an inappropriate NAS.

Data Integrity

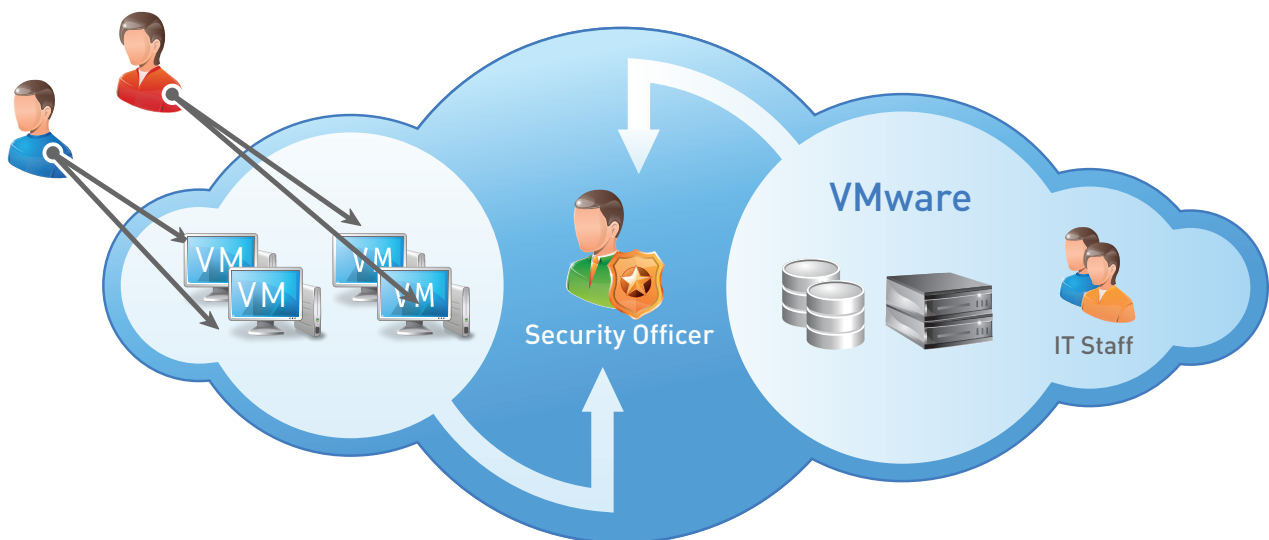
vGate's unparalleled integrity control mechanism works on the individual virtual machine level. The product can report when a machine's integrity is compromised and run a response action (like restore from backup or block virtual machine from booting).

Compliance

Preconfigured policy templates are based on applicable compliance regulations (PCI DSS, CIS Networking, and so on) and can be fine-tuned as needed. Compliance to a certain standard can be verified at any time, and forced if necessary.

Audit

vGate offers versatile auditing that covers both the virtual environment and the vGate infrastructure. Reporting capabilities range from instant environment snapshots to in-depth reports and detailed forensic analysis.



© 2011 Security Code, Inc. All rights reserved. All trademarks and registered trademarks used are property of their respective owners.

Security Code Sales Office Europe

PO Box 40
3632 ZR Loenen a/d Vecht
The Netherlands
Tel: +31 (0) 29 423 4374
Email: info@securitycode.ru



Security Code

PO Box 55, Moscow 127018, Russia
Tel: +7 495 980-2345, Email: info@securitycode.ru
<http://www.vgate.info>