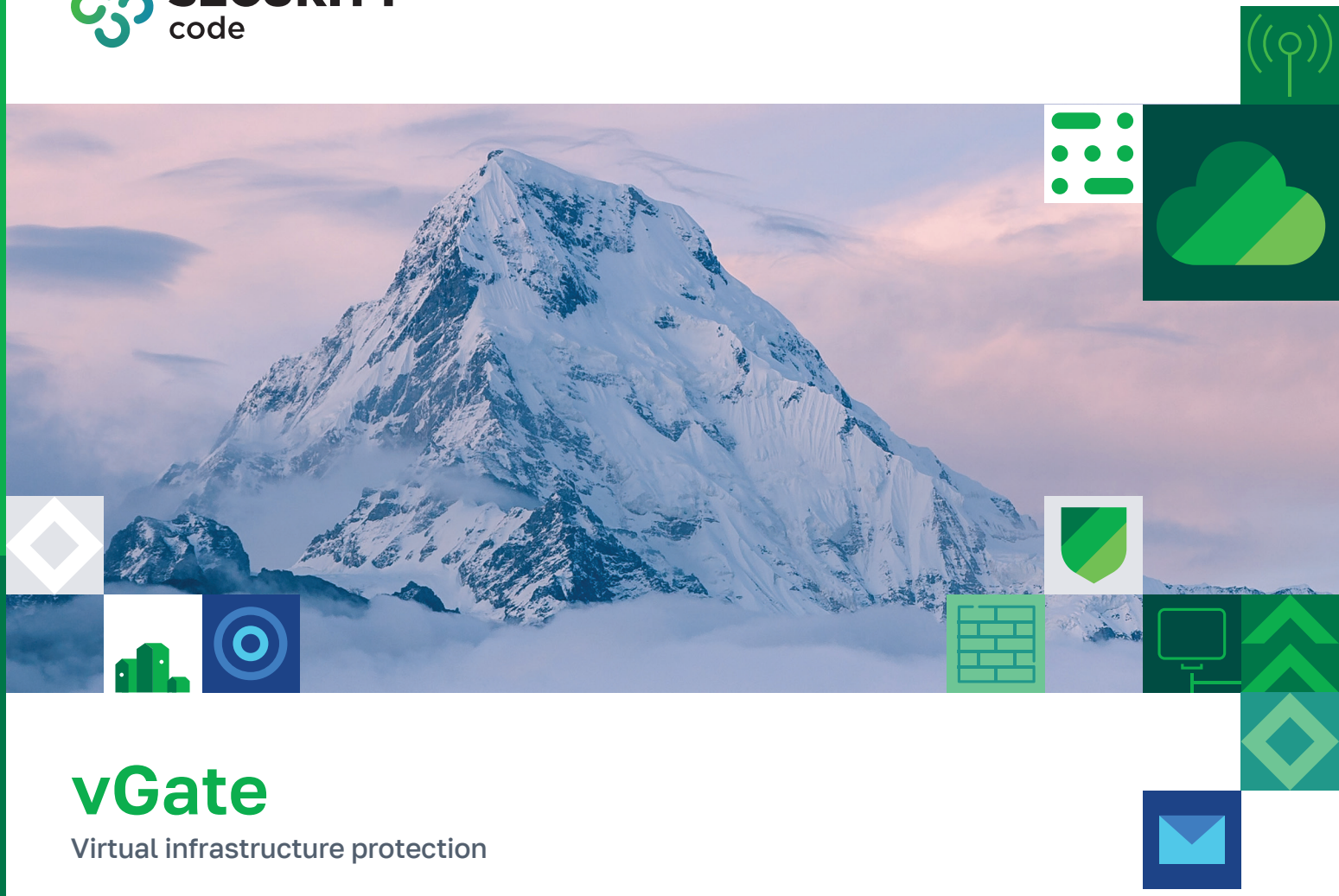
SECURITY code

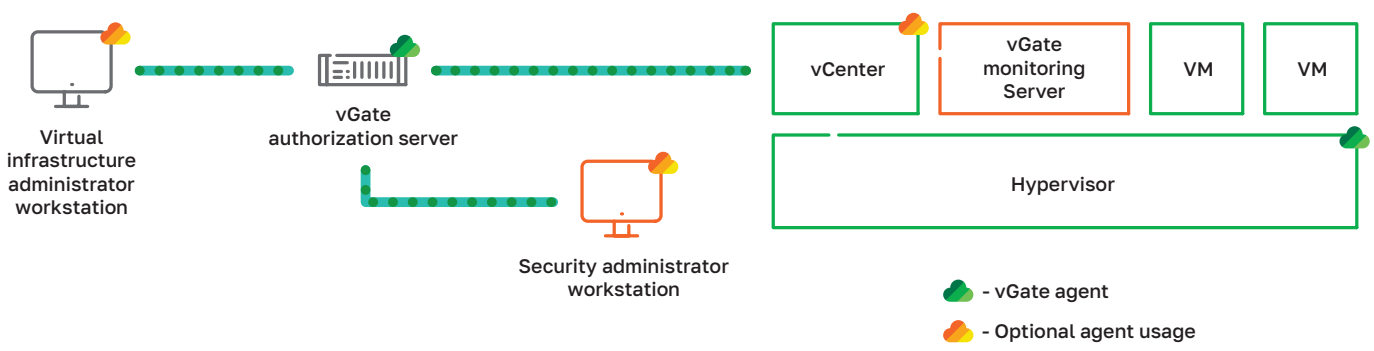


vGate

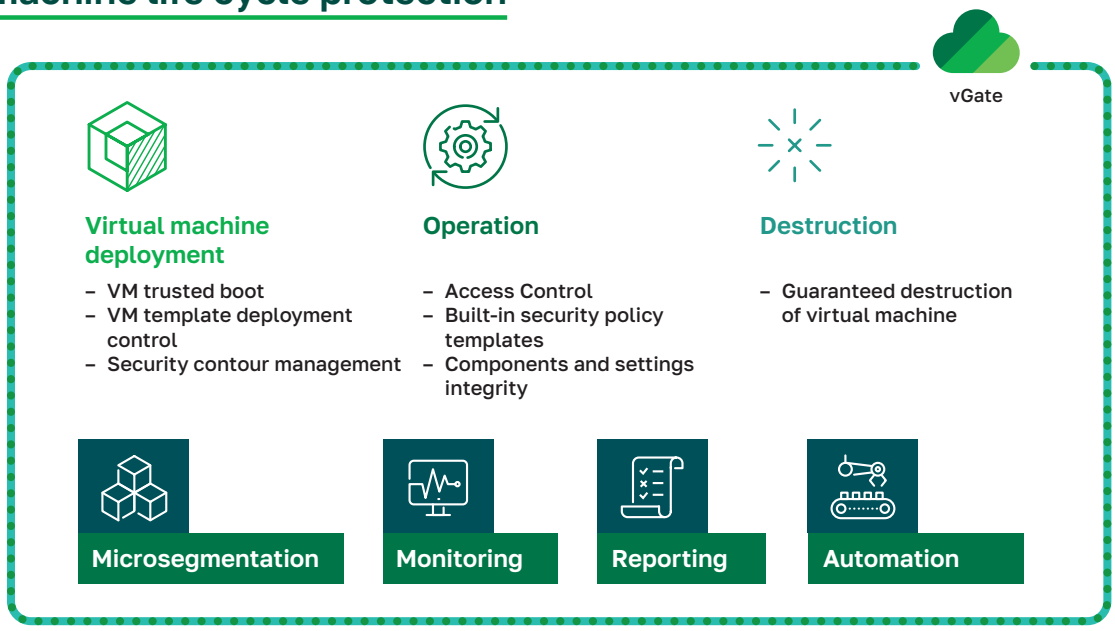
Virtual infrastructure protection

- Microsegmentation
- Automation ready management
- Control over virtualization inrastructure administrators
- Compliance with requirements, standards and best practices
- Comprehensive security analysis of virtualisation infrastructure
- KVM support

vGate architecture



Virtual machine life cycle protection



Key features

VMware technologies support

- High availability cluster of vGate authentication servers.
- vCenter Server Appliance, vCenter HA and vCenter Linked Mode support.
- Works with any guest OS on virtual machine.
- Works on vSphere 6.5, 6.7, 7.0.
- VMware Tanzu containers support.
- VMware Cloud Director support.
- VMware vSAN support.

Access separation for segmentation infrastructure

- Separation of administrative and security roles.
- Security officer can approve changes to virtualisation infrastructure.
- Capability-based access control depending on categories and confidentiality levels.
- Control of administrative access to data processed by virtual machines.
- Integration with Active Directory.
- Custom confidentiality levels.
- Limiting the number of simultaneous virtual infrastructure administrator sessions.
- Role-based Access Control.
- Automation of settings and security policies.
- Security reporting system.
- Separate administrator privilege for editing vGate firewall settings.

Compliance templates

- Security templates for various standards:
  - PCI DSS;
  - VMware vSphere Security Configuration Guide;
  - CIS Benchmark:
    - CIS for ESXi 7.0.
- Local templates could be created upon request.

Logging and reporting

- Enhanced security logging.
- Detailed reports on administrative actions, configurations changes, security status and compliance.
- Continous compliance audit.
- Integration with SIEM.

Hypervisor level firewall

- Layer 2 firewall.
- Network traffic filtering based on:
  - VM name;
  - IP-address;
  - MAC-address.
- Virtual machine migration support.
- Centralised rule-base management.
- Works with any virtual Switch:
  - Standard;
  - Distributed;
  - 3rd Party.
- Compatibility with VMware NSX.
- Real-time control of the active sessions.

Privileged user control

- Separated access to virtualization infrastructure management console.
- Minimised downtime from unintentional damage because of administration faults.
- Reduced risks related to virtualisation infrastructure.

Centralized management

- Account and access management.
- Security components deployment.
- Management automation.
- Virtual machine name based policy enforcement.
- Control access to vSphere Pods.
- Hot spare and cluster mode implementation.
- Integrity control of container images in Harbor built-in registry.

Virtual infrastructure monitoring

- Enhanced security logging.
- Detailed reports on administrative actions, configurations changes, security status and compliance.
- Continous compliance audit.
- Integration with SIEM via syslog.
- Heat map of audit events.
- Real time dashboard panel.
- Event correlation and incident generation.
- Correlation rule templates specifically designed for virtual environments.

www.securitycode.net

115230, Moscow, 1st Nagatinsky proezd 10/1

E-mail: export@securitycode.ru
Tel.: + 7 (495) 982-30-20