SECURITY code

vGate

SECURITY code

About the product

vGate

Protection of virtualization platforms based on VMware vSphere, Scala-P, KVM and oVirt:

- Protection of virtual machines from unauthorized copying, cloning, and destruction
- Protection against threats specific to virtual environments
- Control of privileged users
- Micro-segmentation of infrastructure
- Monitoring of security events and investigation of information security incidents
- Automation of compliance and best practices

SECURITY code

Advantages

Supports Russian and foreign virtualization platforms, such as VMware vSphere, Microsoft Hyper-V, Skala-R.

Automated compliance with industry standards and security requirements.

Agentless firewall at the hypervisor level.

Virtual infrastructure of security events monitoring.

SECURITY code

Comprehensive approach to virtualization security

vGate

Virtual machine deployment

- VM trusted boot
- VM template deployment control
- Security contour management

Operation

- Access Control
- Built-in security policy templates
- Components and settings integrity control

Destruction

- Guaranteed destruction of virtual machine data

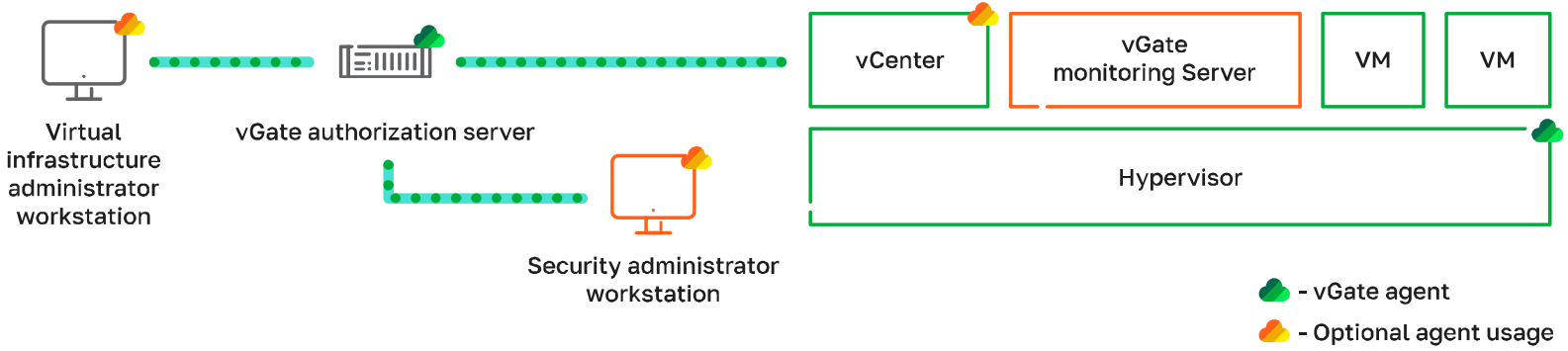
Microsegmentation

Monitoring

Reporting

Automation

Architecture



SECURITY code

Key features

SECURITY code

Administrative function differentiation

Virtual infrastructure administrator

Information security administrator

SECURITY code

Admin access control

Predefined roles

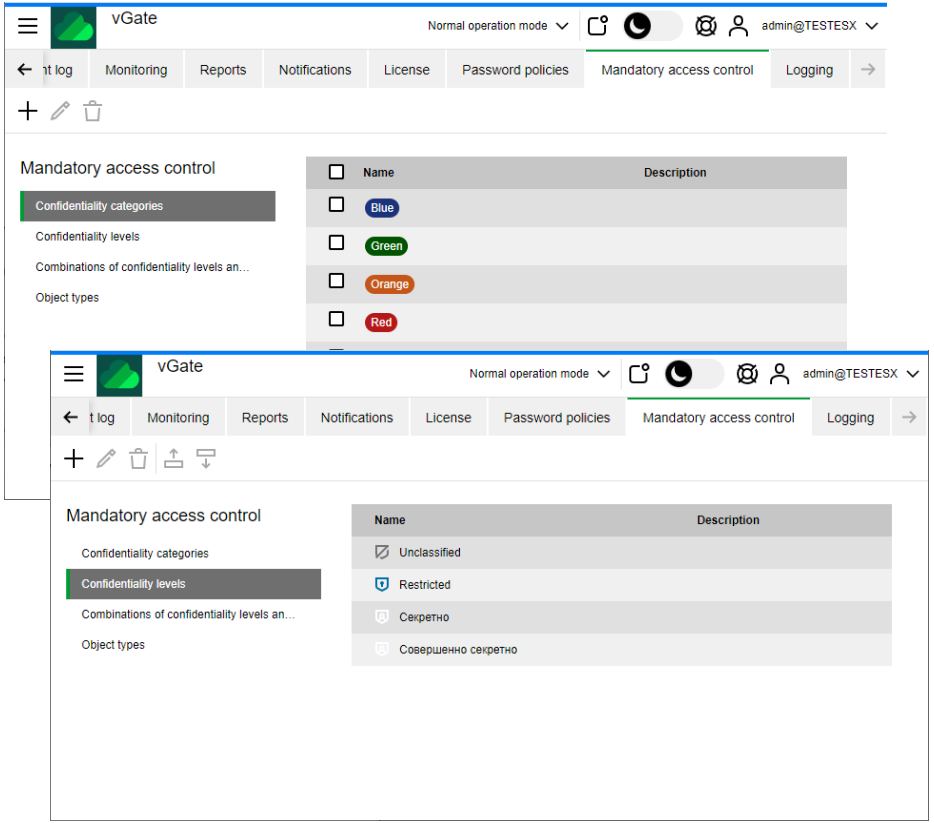
- Virtual infrastructure administrator
- VM administrator
- vNetwork administrator
- vDatastore administrator
- VM user
- Auditor

Strong authentication

Mandatory control of access to confidential resources

Security labels are assigned to the following resources:

- ESXi server
- vCenter server
- KVM server
- Skala-R server
- Skala-R data storage
- vSphere data storage
- vSphere virtual machine
- KVM virtual machine
- vSphere network adapter
- vSphere virtual network
- distributed virtual switch
- user
- object group
- Cloud Director organization



SECURITY code

Virtual machine security

- Snapshot restriction
- Clone restriction
- Storage data erasure
- Device control
- Console access restriction
- File download restriction

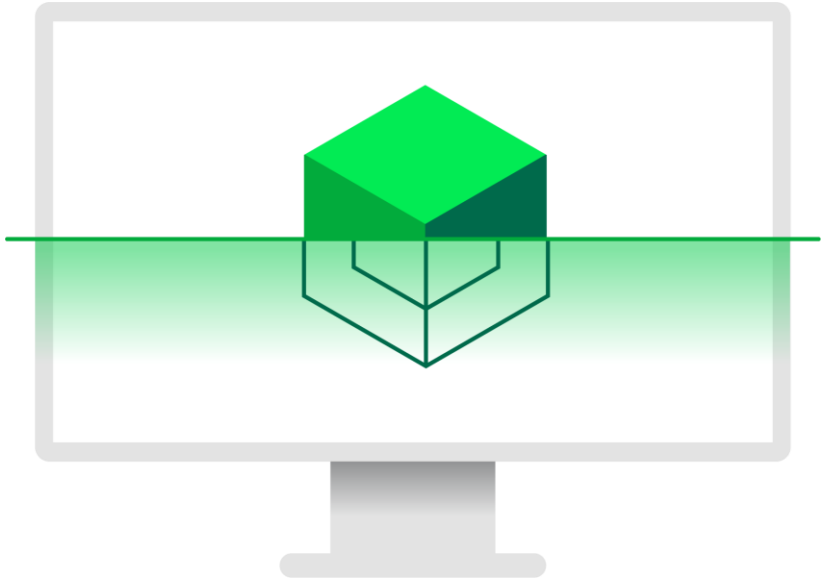
SECURITY code

Hypervisor hardening

- Host Lockdown mode enforcing
- USB drive mount restriction
- Host SSH restriction
- VM log restriction
- Host application whitelisting
- Segregation between management and production networks

SECURITY code

VM integrity control



VM hardware integrity check

- CPU
- RAM
- HDD
- NIC
- etc

VM hardware configuration change confirmation

- Change will not be committed until security approval

SECURITY code

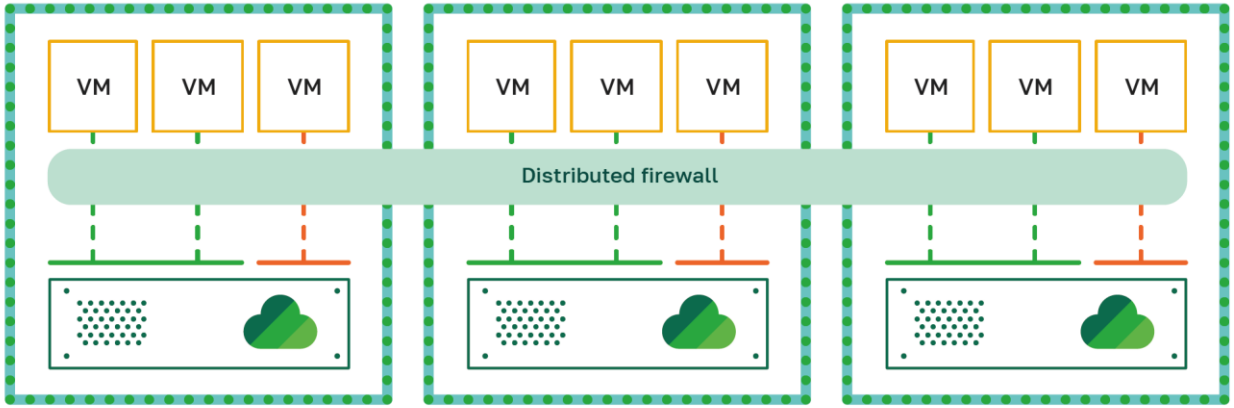
Reports

- Configuration changes
- Non-work hours access
- Most active users
- VM boot statistics
- Security policy statistics
- Account management
  - VMware
  - vGate

SECURITY code

Segmentation network. Firewall

- Network firewalling allows you to filter the traffic on the virtual machine's network, including those located on different virtualization servers.
- Filtering rules can be created for a specific virtual machine or for a group of virtual machines.
- Stateful packet inspection (SPI) and Deep packet inspection (DPI).



SECURITY code

Firewall. Rules

vGate

Normal operation mode | admin@TESTESX

Refresh | Statistics | Services | Copy | Enable | Disable | Reset statistics

Firewall rules

Items count: 50

Column options

Priority	State	Outgoing traffic	Incoming traffic	Outgoing packets	Incoming packets	Name	Source
1395	Enabled	50.8 MB	101.7 MB	34660	37332	test_rule_6	seg3
1394	Enabled	50.8 MB	101.7 MB	29328	32000	test_rule_5	SEg2
1393	Enabled	50.8 MB	101.7 MB	23996	26668	test_rule_4	seg3
1392	Enabled	50.8 MB	101.7 MB	18664	21336	test_rule_3	SEG4
1391	Enabled	50.8 MB	101.7 MB	13332	16004	test_rule_2	sEg1
1390	Enabled	50.8 MB	101.7 MB	5334	8006	test_rule_1	sEg1
1389	Enabled	14 B	20 B	2	8	test_rule	SEG2
596	Enabled	14 B	20 B	2	8	46	Any
595	Enabled	14 B	20 B	2	8	45	Any
594	Enabled	14 B	20 B	2	8	44	Any

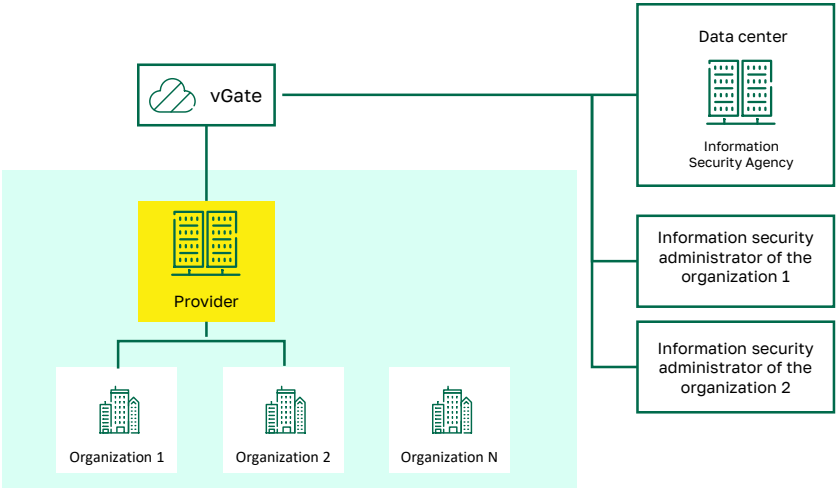
Recent tasks

SECURITY code

Protection of KVM servers

- Storing account data for connection to KVM servers.
- Adding KVM servers to the list of servers protected by vGate.
- Installing vGate Agents on KVM servers.
- Control of the VM loading.
- Integrity control of VM when loading.
- Cleaning up the residual information after VM deletion.
- Assigning security labels and security policies to the virtual machines.
- Adding KVM servers to the groups (includes automatic adding).
- Export and import of the KVM servers configuration.
- Synchronization of vGate settings on KVM servers between vGate Servers.

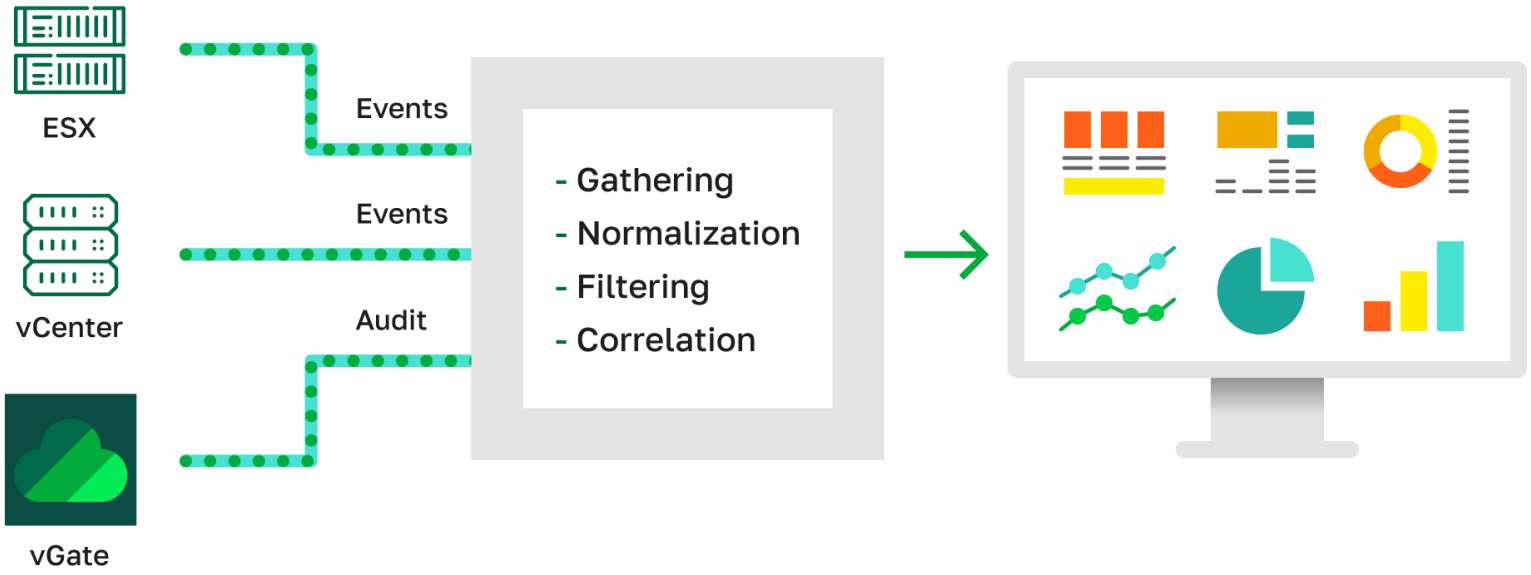
Multi-tenancy



- The separation of powers between the data center security administrator and the security administrators of the organizations being served.
- Protected objects of protected organizations are only visible to the relevant security administrators.
- The data center security administrator does not have access to the organization's facilities.

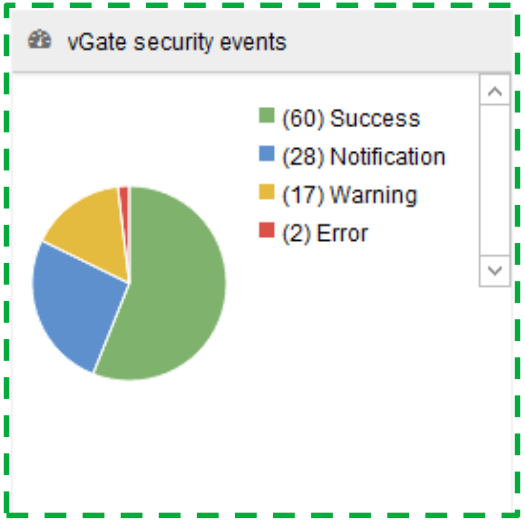
SECURITY code

Virtual infrastructure security monitoring

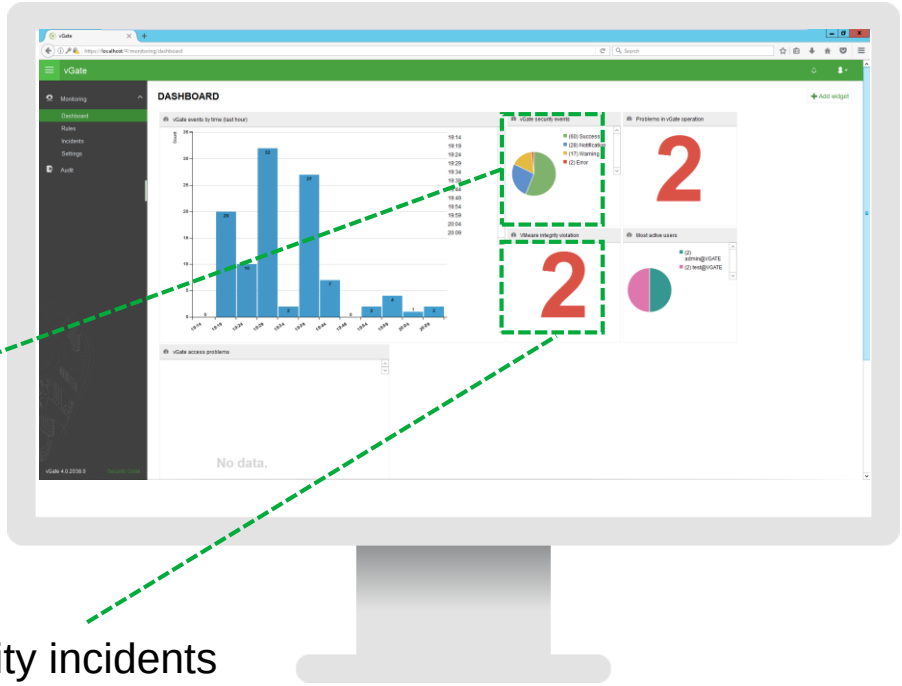


Reporting dashboard

Drill-down reports



vGate events pie chart



Integrity incidents

Supported platforms

- Proxmox 7.4.1, 8.0.2
- VMware Tanzu
- vCenter HA и Linked Mode
- VMware vSAN
- VMware vSphere 6.5, 6.7, 7.0
- Microsoft Windows Server 2012, 2012 R2, 2016.
- Microsoft Hyper-V Server 2012 R2, 2016.
- Microsoft System Center Virtual Machine Manager 2012 R2, 2016
- Ubuntu 18.04.6/20.04.3 LTS

SECURITY code

Use Cases

SECURITY code

Use cases: Admin activity control

Key value

- Restricted access to sensitive data in private cloud
- Reduced risks of downtime due to the virtual infrastructure damage
- Reduced risks of financial losses due to related information leakages.

Key features

- Independent virtual infrastructure management for access control
- Protection against private cloud admin account compromise
- Independent audit trail of private cloud admin’s actions

SECURITY code

Use cases: Security posture management

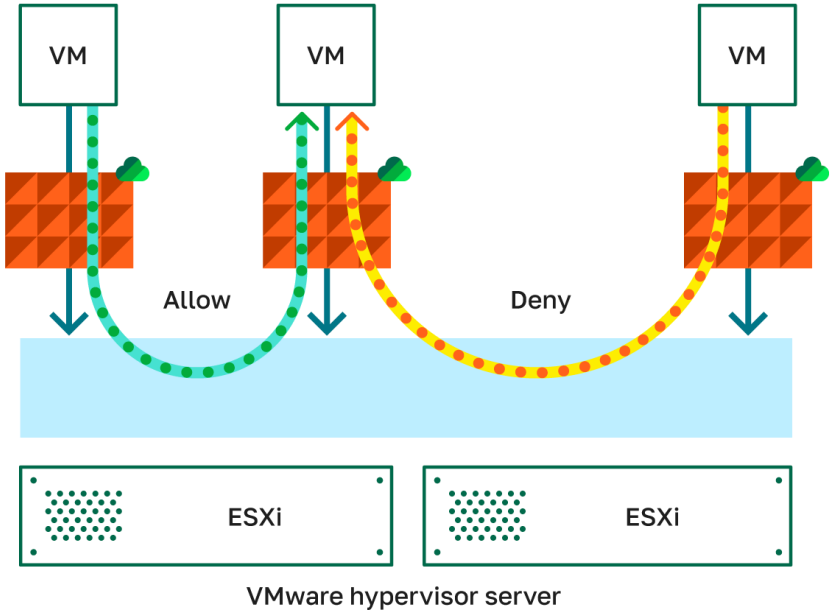
Key value

- Reduced risk of private cloud-related security incidents
- Reduced resources to ensure private cloud security compliance for auditors

Key features

- Private cloud security hardening
- Compliance requirements enforcement

Use cases: Virtual network segmentation



Key value

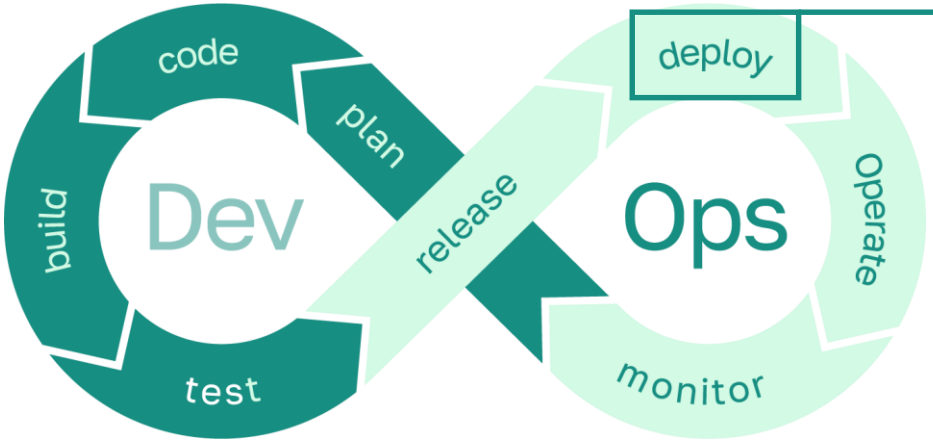
- Reduced risks of horizontal hacker propagation
- Fast VM quarantine
- DevSecOps implementation

Key features

- Flexible network segmentation for virtual networks
- Network security policy enforcement along with VM creation
- Little performance impact
- Segmentation doesn't affect network topology

SECURITY code

Use cases: DevOps integration



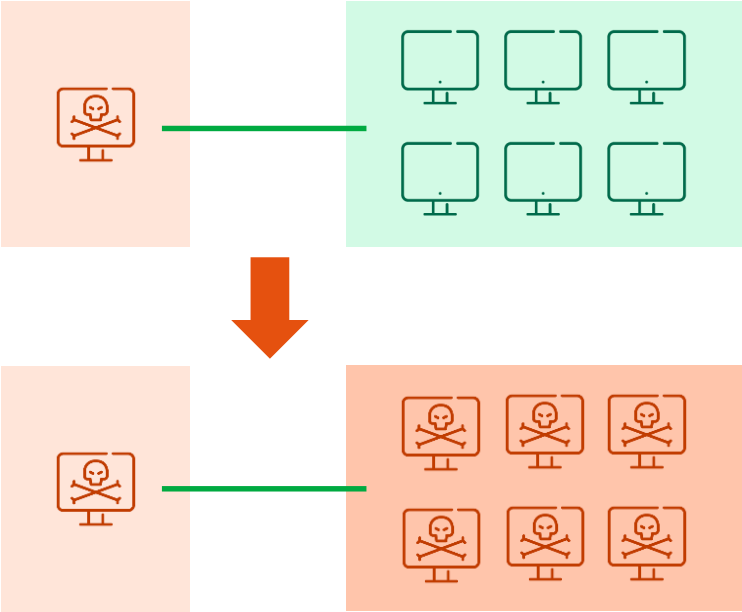
Challenges for security:

- Environment changes too fast
- Too complicated for security to keep it protected
- Hard to ensure compliance

What do we offer:

- Enforce Security and Access Control policy along with VM creation
- Apply Network filter
- Apply compliance template

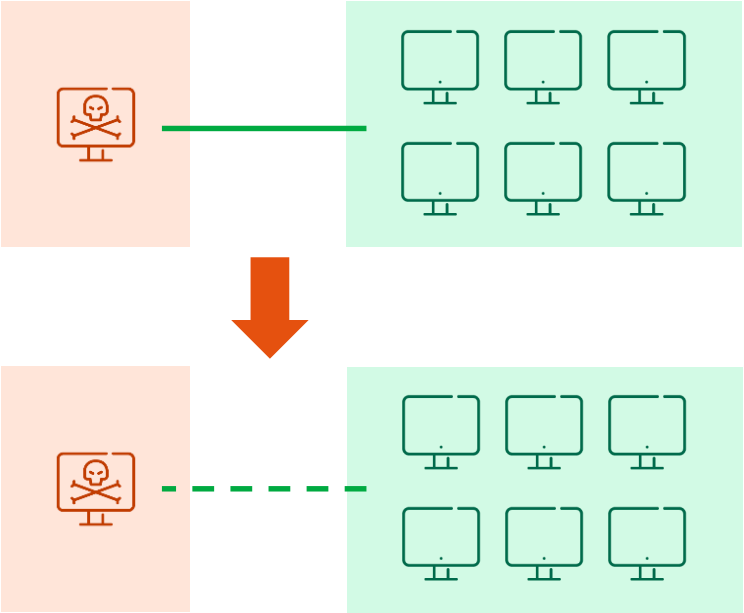
Use cases: Quarantine



Challenges for security:

- Often there is no east-west firewall at all
- Policy could become too complex and error prone
- Security operations may not react in time

Use cases: Quarantine



Challenges for security:

- Often there is no east-west firewall at all
- Policy could become too complex and error prone
- Security operations may not react in time

What do we offer:

- Through simple REST API integration – **quickly** change filter policy to lock down compromised endpoint

SECURITY code

Thank you!

Headquarters: Moscow, 1st Nagatinskij proezd, 10, bldg. 1

Service center: Moscow, Elektrolitnyj proezd, 9, bldg. 1

Phone: +7 (495) 982-30-20

E-mail: info@securitycode.ru

www.securitycode.ru