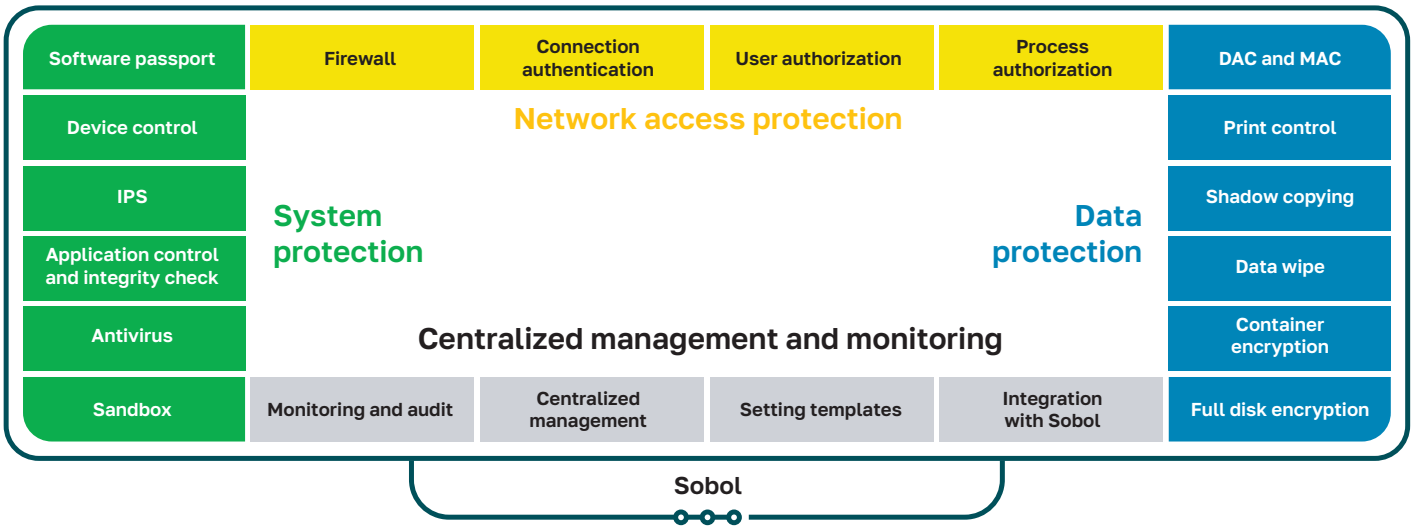
SECURITY code

Secret Net Studio

Information-centric endpoint protection,
Zero trust network access

- Sensitive data protection
- Integrity control
- Support for distributed infrastructures
- Software-defined segmentation
- Compliance with security regulations
- Centralized management

Functions



Key features

Device control

- Control of connection and disconnection of external devices.
- A wide range of devices, including webcams, mobile phones, 3G modems, network cards, flash drives, and printers is supported.
- Protection against substitution of VID and PID of the connected device.
- Control by groups, classes, models and individual devices.
- Hierarchical inheritance of settings.

Centralized deployment and management

- Centralized deployment, update, and maintenance.
- Single point of administration and management.
- Delegated hierarchical policies.
- Convenient grouping of protected objects.
- Federated reporting and responding.

Security event management

- Centralized management of all security-related events.
- Group-based hierarchical alerting and reporting.
- Policy-based event acknowledgement and response actions.

Application whitelisting and integrity control

- Creating a list of those allowed to run applications.
- Monitoring the integrity of files, directories and registry.
- Setting the integrity monitoring time.
- Selecting a response to information security events.

Secure login

- User authentication can be further enhanced with two-factor authentication using hardware tokens. For domain users, you can use certificates as well.
- Session lock when user inactivity or withdrawal of electronic identifier.
- Strengthened password authentication and password policies.

Host based firewall

- Traffic filtration based on:
  - IP-address;
  - Port number;
  - Process name;
  - User.
- Mutual host authentication before network connection.
- Time and weekday related policy.
- Network traffic encryption.
- Firewall export/import rules.

Encrypted containers and disks

- Container mounting as disk.
- Secure encryption key storage.
- Encryption key backup.
- Granular data access control.
- Full disk encryption.
- Key storage on electronic keys or removable disks.

Context-aware access control

- Context-based access control for:
  - Files;
  - Printers;
  - USB-devices;
  - Network interfaces.
- Context is set by:
  - User rights;
  - User session type;
  - File/device classification tag.
- Windows Terminal session support.
- Every Windows file system support.

www.securitycode.net

115230, Moscow, 1st Nagatinsky proezd 10/1

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