Janus Technology

Current technologies fail to adequately meet the task

Site-Site Virtual Private Network (VPN), VLAN, Firewall, Antivirus Software are most commonly used today for infrastructure protection. All of these technologies expose your network to data breaches

- Site-Site VPN’s lacks individual resource to resource security
- VLAN’s are not security solutions lacking authentication and encryption
- Firewall requires continuous updates for new and evolving threats
- Antivirus Software are only as good as the known threat

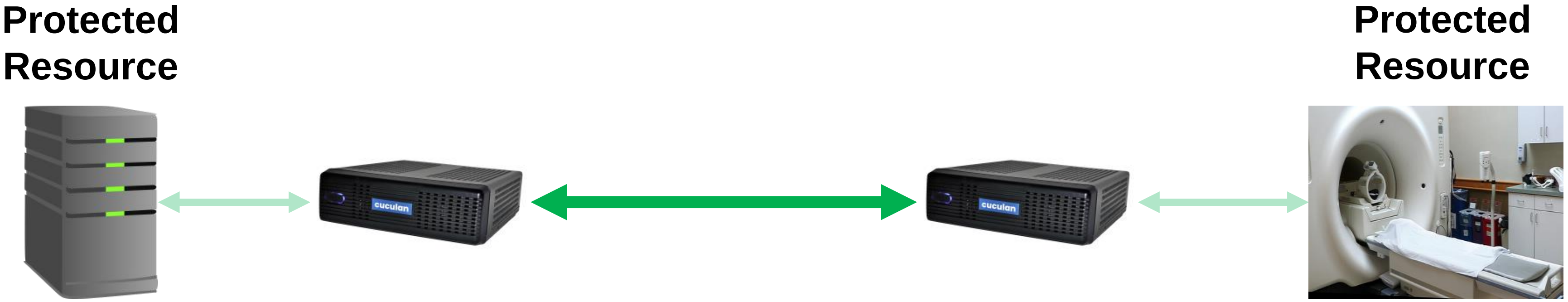
These technologies address pieces of the overall security posture. Janus technology uses a **new paradigm** that groups critical resources within a protective barrier excluding all unauthorized users.

The solution is **self-contained** with all required components delivered in a zero-trust solution including encryption, segmentation, availability, management as well as protection for legacy equipment.

The fundamental premise of the solution is that the **network is not trustworthy** and, as such, places no dependency on internal or external company resources.

Janus Security Goals

Bi-directionally authorize source/destination communication

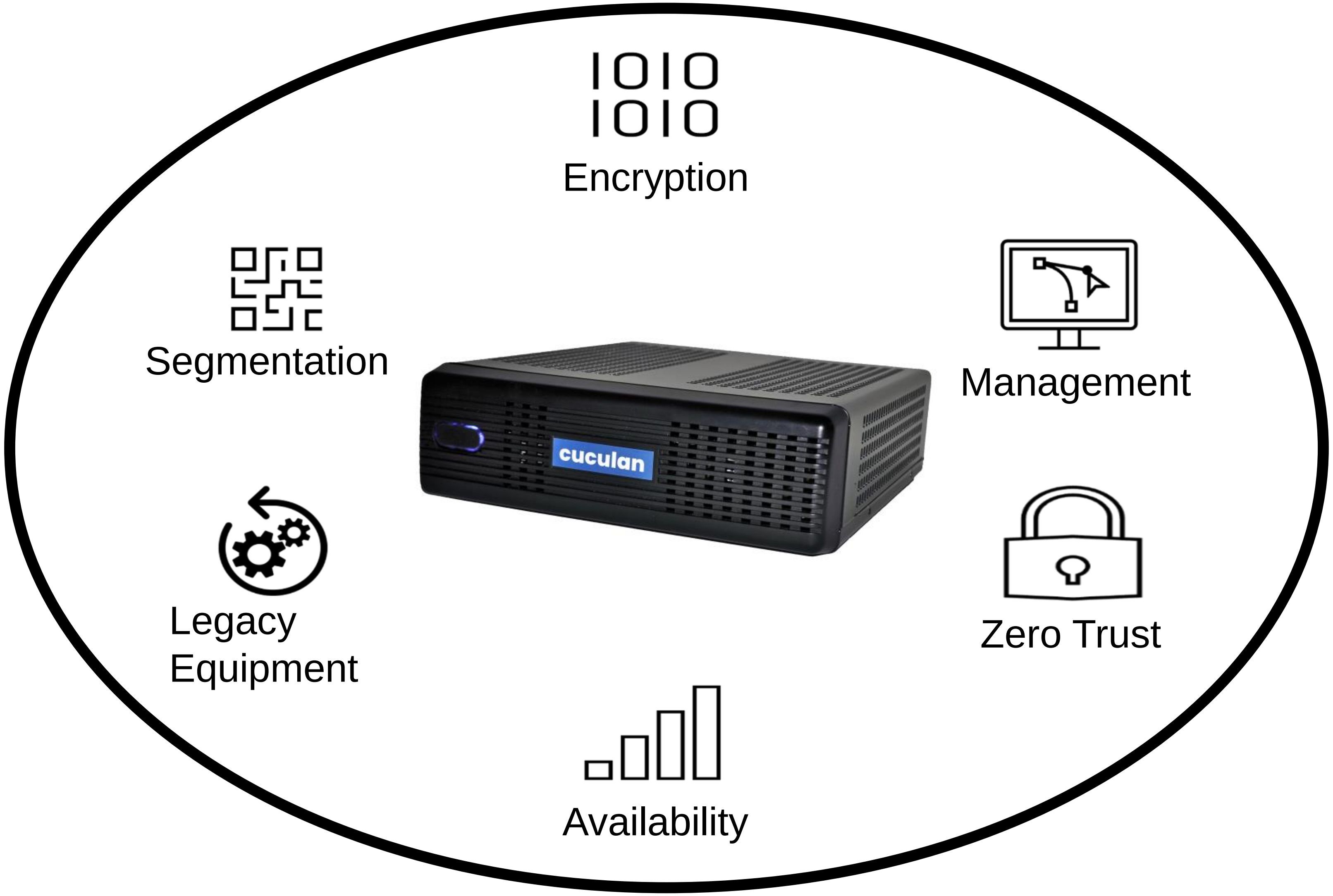


Protected Resource

Protected Resource

Conceal protected resources on the network with secure end to end communications

Solution Components



Encryption

Segmentation

Management

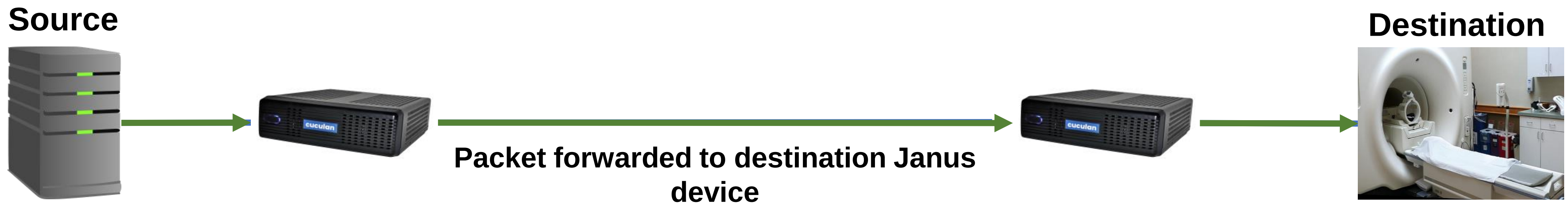
Legacy
Equipment

Zero Trust

Availability

Elements	Description
Encryption	Network traffic is encrypted using industry validated TLS 1.3 cryptographic protocol with replay protection. Each packet is encapsulated to conceal resources and ensure data integrity and confidentiality. Cryptographic keys are automatically managed internally with periodic updates
Segmentation	Attack surface is reduced using micro-segmentation. Unwanted lateral movement is prevented
Availability	Network availability is enhanced via automatic failover by using two devices
Zero Trust	Two-way network communication between source and destination is proactively authorized using certificate-based mutual authentication
Legacy Equipment	Legacy equipment is protected with plug-in self-contained security. There is no need to reconfigure the network, employ third party services or intrusive agents
Management	Network operations can add, configure, maintain and monitor the Janus security infrastructure using the management application, and use our published API to integrate with your local applications

How it works



Source

Destination

Packet forwarded to destination Janus device

Packets sent, in-line, to a Janus device, which then

- Verifies the source protected resource
- Verifies the packet is formatted correctly
- Verifies the destination protected resource

If verified as a valid communication, the Janus device

- Encrypts and encapsulates each packet to be sent
- Sends packets to the destination Janus device

The in-line Janus device receives transmitted packets and

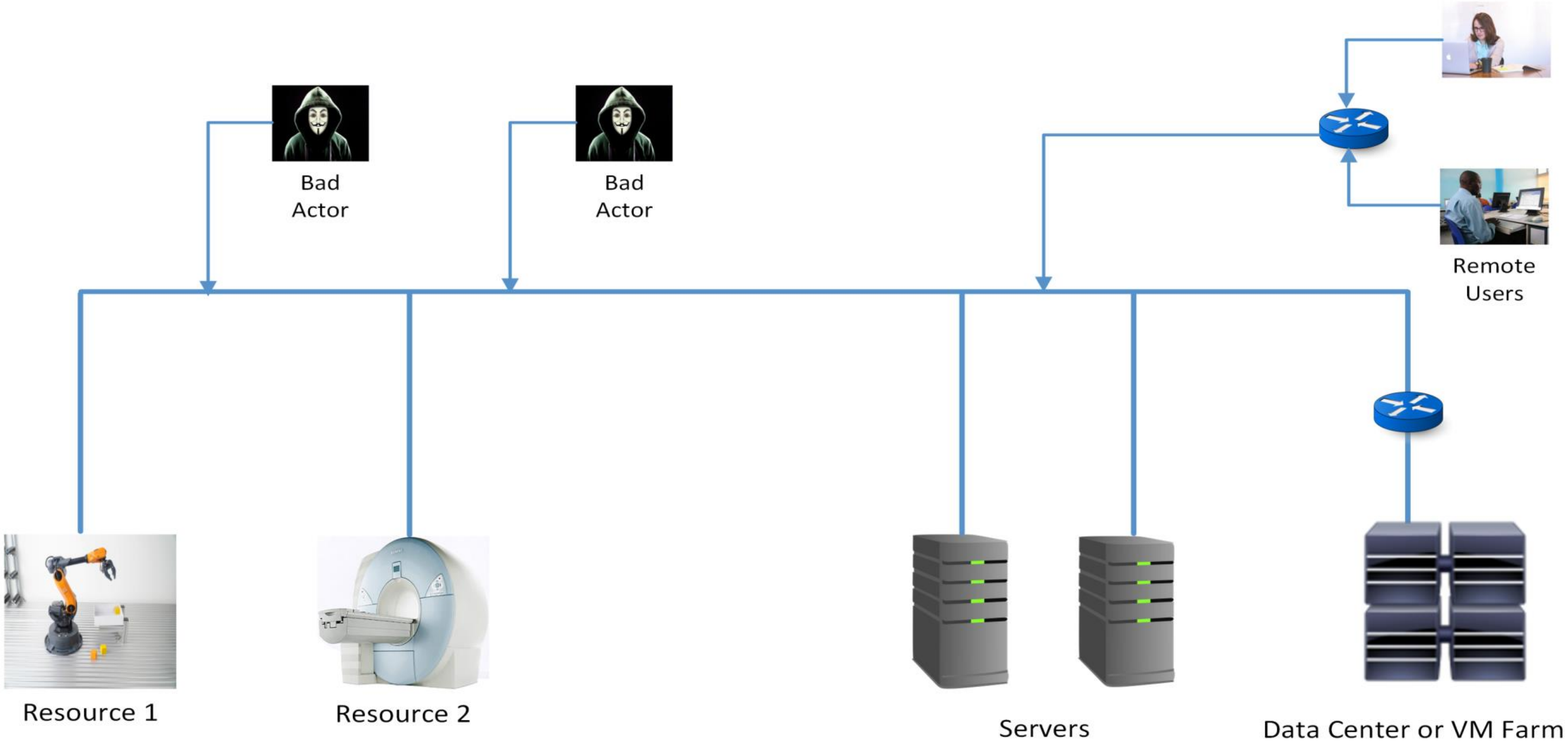
- Verifies the source Janus device
- Verifies each packet is formatted correctly
- Verifies the transmitted packet is not a replay
- Un-encapsulates and decrypts the packet
- Verifies decryption integrity
- Verifies the destination protected resource is an authorized resource

If the communication is verified

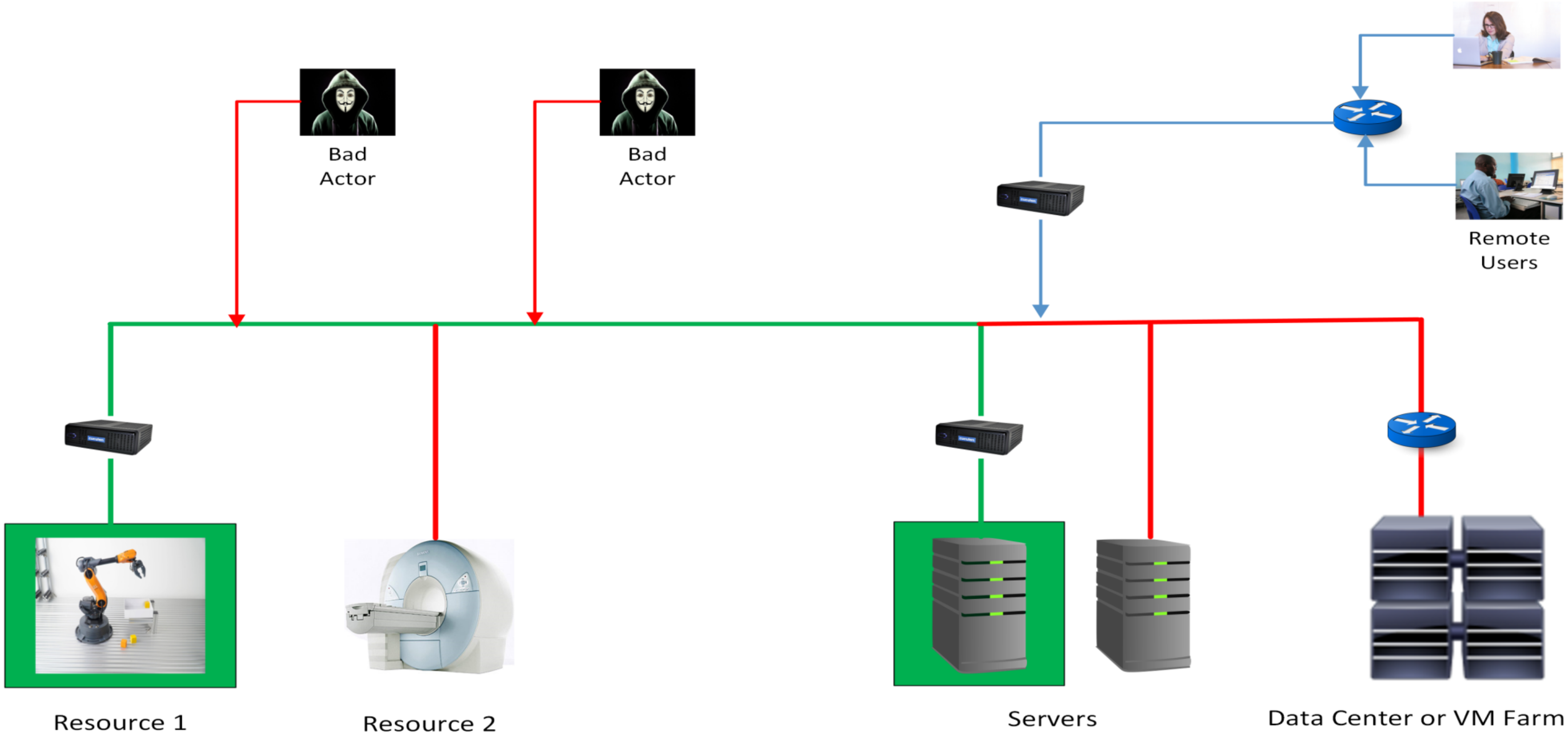
- The packet is sent to the destination protected resource

Use Cases

Example network implementation without Janus-10

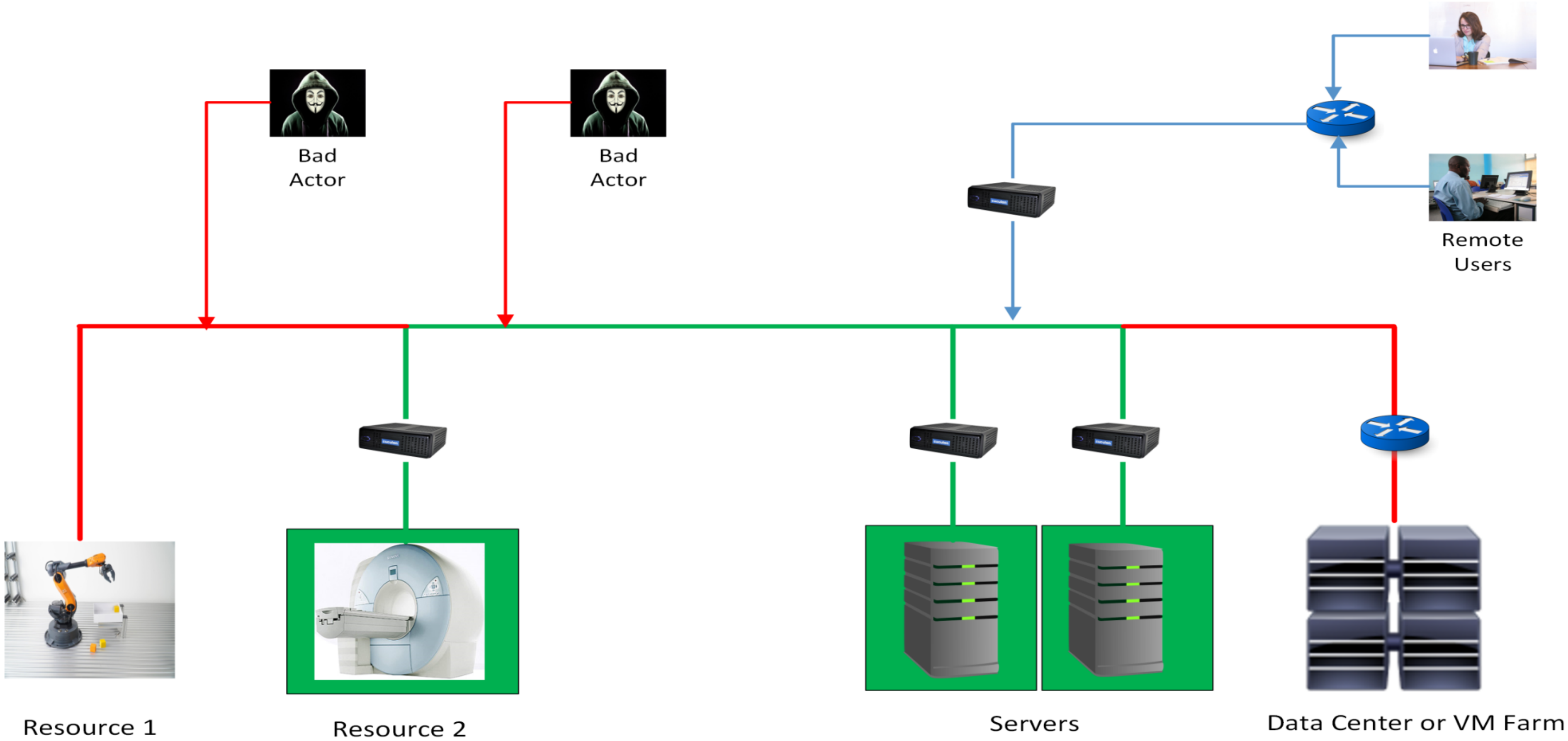


Point to Point with Janus-10



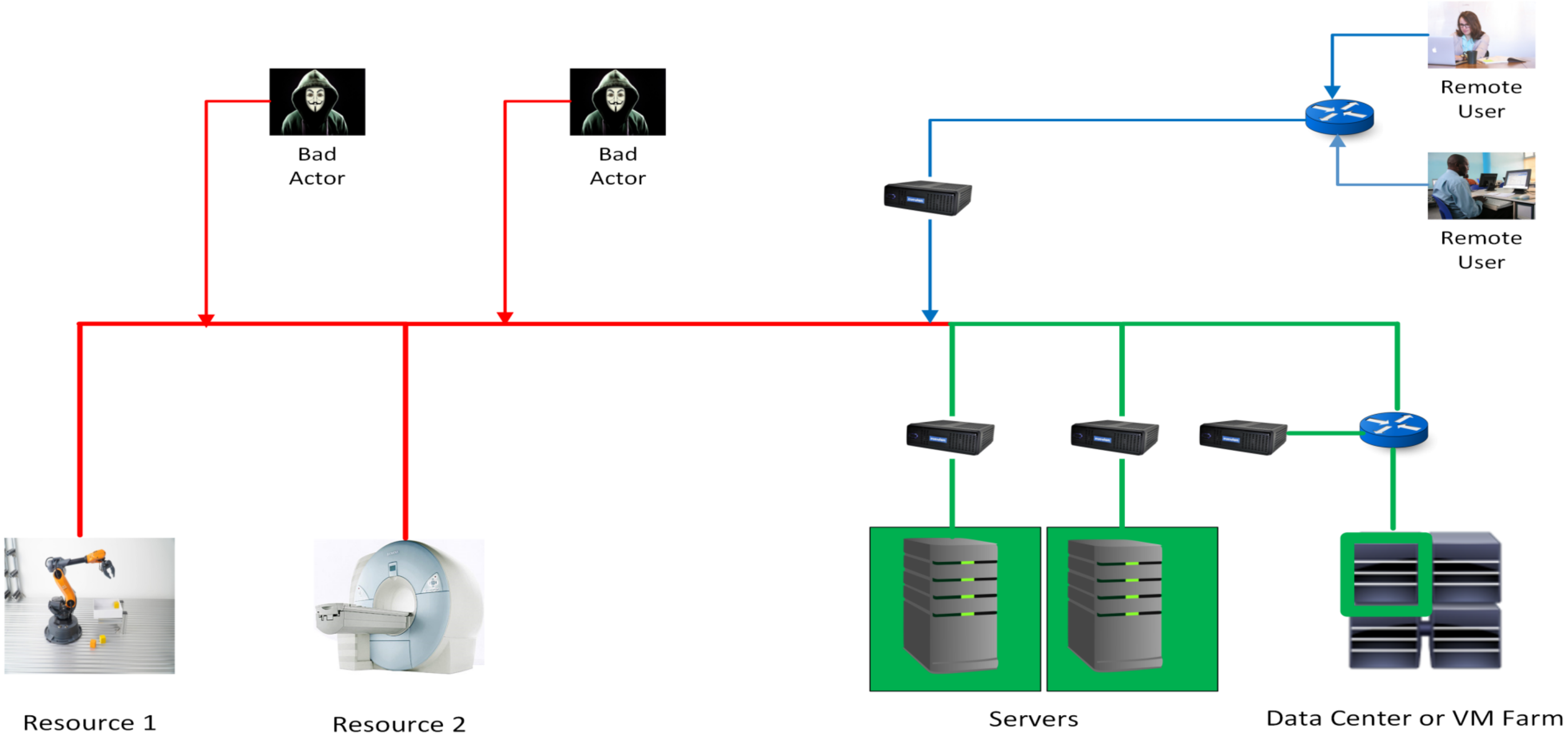
Protected Resource 1 and Server have authorized access to each other
All other resources are prohibited from accessing either Protected Resource 1 or Server

Point to Multipoint with Janus-10



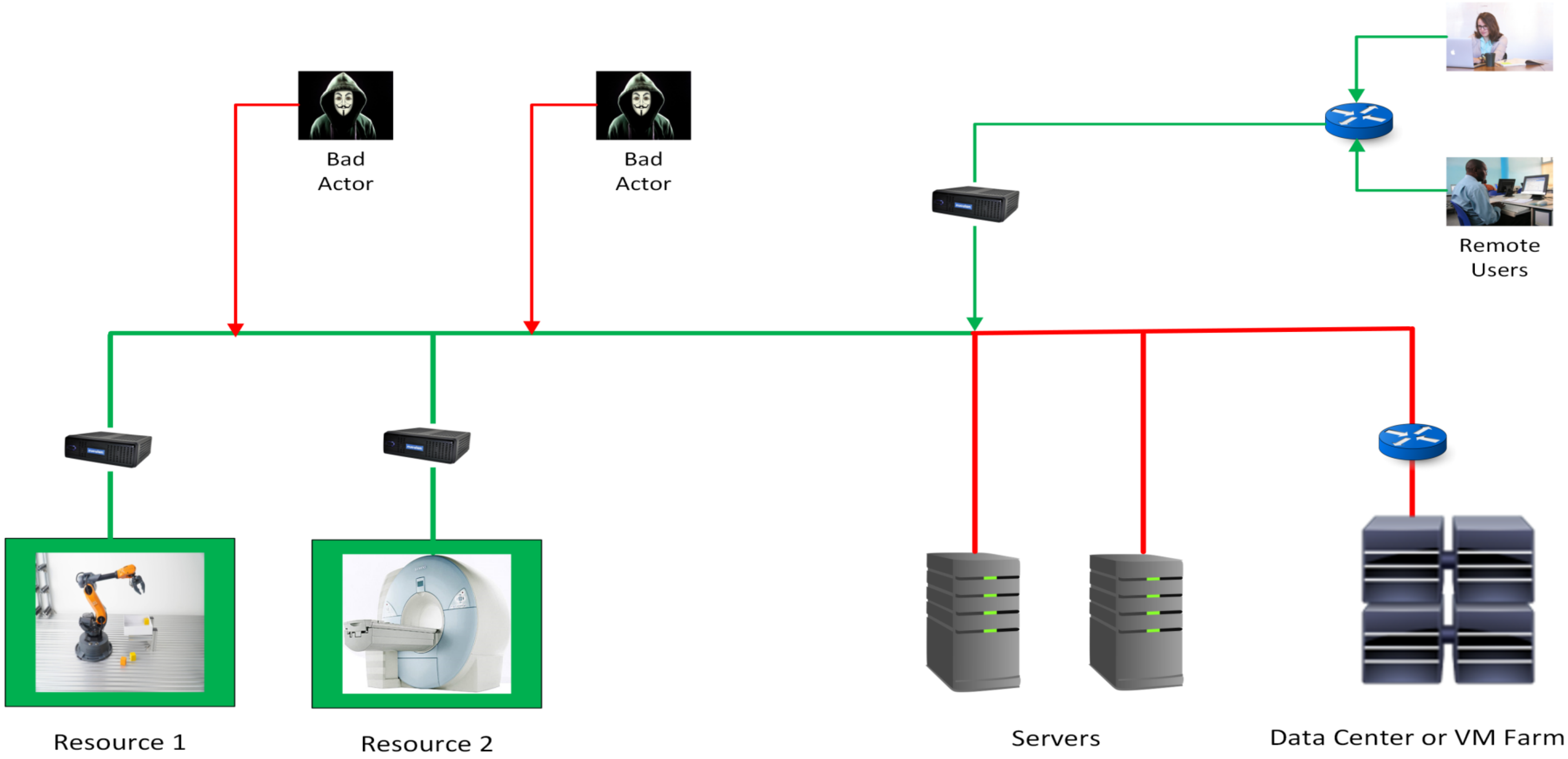
Protected Resource 2 has authorized access to both servers
All other resources are prohibited from accessing either Protected Resource 2 or either Server

Multipoint with Group of Resources



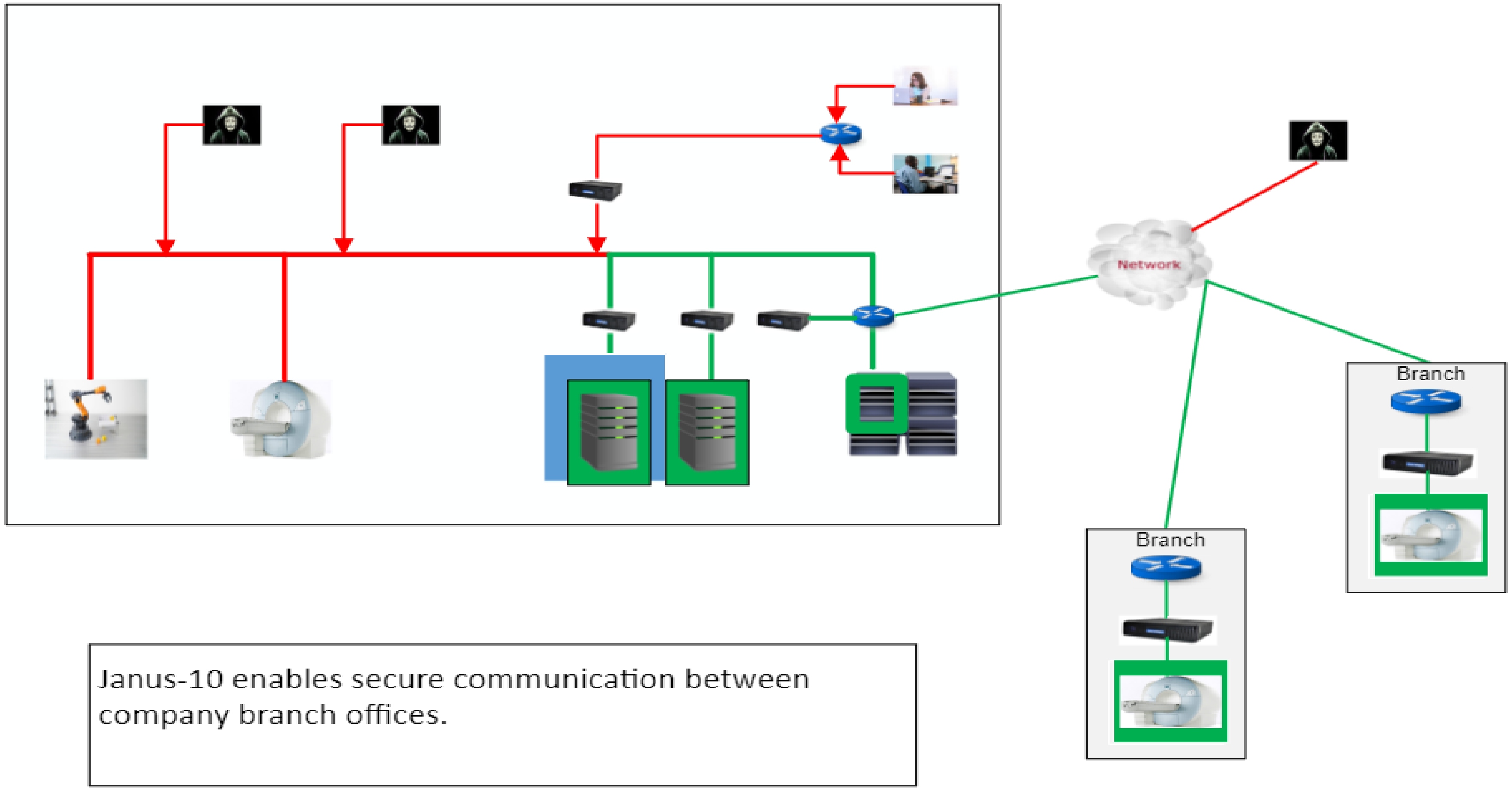
Servers are authorized to access one server in the data center or VM farm
Servers are prohibited from accessing all other resources

Remote access with Janus-10



Remote user has authorized access to Protected Resource 1 and Protected Resource 2
Remote user is prohibited from accessing all other resources

Remote Access with Branch Offices

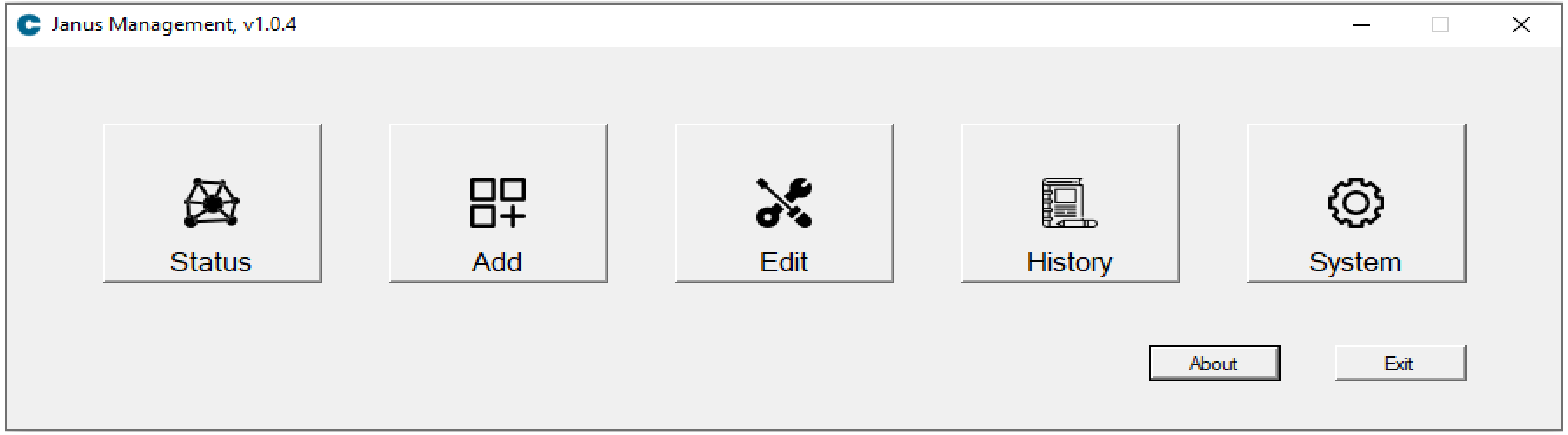


Janus-10 enables secure communication between company branch offices.

Note: The Janus-10 icon represents redundant units, for automatic failover where required

Janus Operations

- Secure centralized management via the Wide Area Network (WAN)
- Add, configure, maintain and monitor security infrastructure
- Remotely update Janus software (encrypted/authenticated)
- Provide biometric user access to Janus Management software



A single dashboard that manages the total Janus security environment

Janus-10 inline device

- Uses encrypted storage, a hardware TPM module, secure boot, and limits external access exclusively to the management API
- Physically isolates the protected resource from the WAN
- Supports TCP, UDP, DNS, and NTP packets
    - Unencrypted DNS and NTP packets are masqueraded
- Support network operation where DNS/NTP/Internet access is not available
- Third party/cloud subscription/agents are not required for operation with all capabilities contained in the Janus device
- Each Janus Device
    - Can manage up to 1000 Janus connections
    - Has a small form factor, 7.6” W x 8.6” D x 2.5” H
    - Network interfaces support both 1G and 10G
    - Provides industry standard syslog for status and events
    - Requires less than 50 watts power

Summary

Challenge	
Provide source/destination authentication through proactive bi-directional control	✓
Encrypt data between resources	✓
Enable micro-segmentation	✓
Physically isolate resources from the Wide Area Network	✓
Provide secure centralized management	✓

Contact

contact@cuculan.com

www.cuculan.com