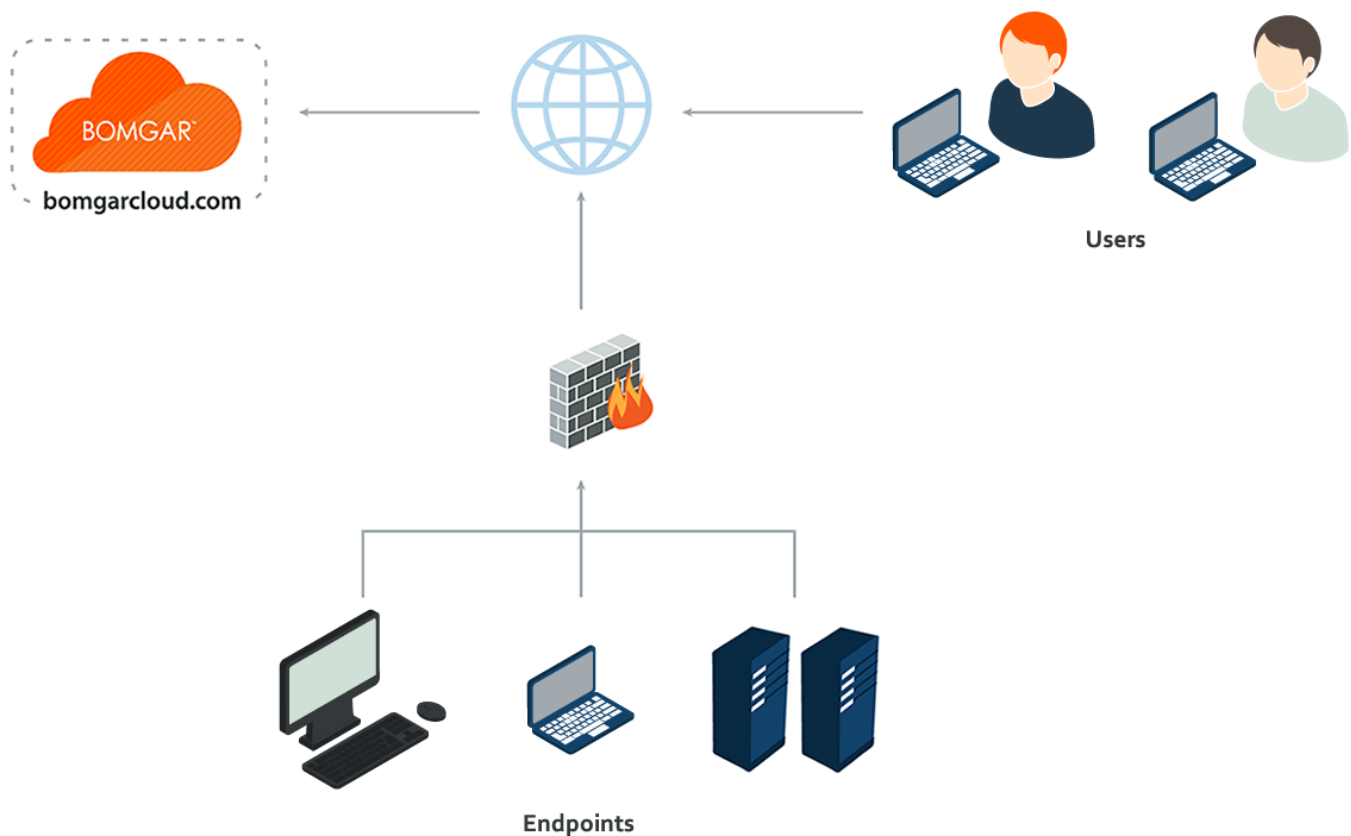


BeyondTrust Privileged Remote Access Cloud Network Infrastructure

The architecture of the BeyondTrust application relies on the BeyondTrust Cloud instance as a centralized routing point for all communications between application components. All BeyondTrust sessions between users and remote systems occur through the server components that run on the appliance. To protect the security of the data in transit, BeyondTrust uses TLSv1.2 to encrypt all application communications.

Customers may configure the security features such that the BeyondTrust deployment complies with applicable corporate policies or regulations. Security features include role-based access control, secure password requirements, and a full audit trail.

BeyondTrust enables remote control by creating a remote outbound connection from the endpoint system to the BeyondTrust Cloud instance. The BeyondTrust Cloud site is designed and tested to ensure it works properly and securely in the BeyondTrust Cloud infrastructure. Since all BeyondTrust sessions are initiated via outbound connections from the client to the appliance, it is possible to remotely control computers using BeyondTrust through firewalls.



BeyondTrust Appliance Network Infrastructure

Each BeyondTrust Cloud site comes with a subdomain of the bomgarcloud.com DNS address, such as yoursite.bomgarcloud.com. Optionally, if you would prefer to use your company web address with your own SSL certificate, you can use a Canonical Name

(CNAME) record to point your default site address to your preferred address.

Since users use this site to access the /login interface, a simple yet descriptive name is the best approach. For instance, a company named 'Example' might use access.example.com for their CNAME record.

Example Firewall Rules for Cloud Deployments

Below are example firewall rules for use with BeyondTrust Cloud, including port numbers, descriptions, and required rules.

Firewall Rules	
Internal Network to the BeyondTrust Cloud Instance	
TCP Port 443 (required)*	Used for all session traffic.
BeyondTrust Cloud Instance to the Internal Network	
TCP Port 25, 465, or 587 (optional)	Allows the appliance to send admin mail alerts. The port is set in SMTP configuration.
TCP Port 443 (optional)	Appliance to web services for outbound events.