HOW BRIVO IS CYBER SECURE

Cybersecurity is central to what we do. To honor our customer's trust, we follow three best practices to deliver a platform that integrates physical security and cybersecurity.

How We Build Products

Designed with Encrypted Device Communication:
256-bit encryption[1]

Reducing Your Potential for Cyber Attacks:
No open inbound ports that make malicious attacks more likely [2]

Bot & DDoS Attack Monitoring:
Real-time alerts to take corrective action [3]

How We Deploy Applications

Regular and Automatic Software Updates:
Safeguarding you against the latest cyber threats

Triple Redundancy:
Ensures high availability [4]

How We Manage Our Business

Detailed Internal Training:
Technical and security training for our developers, testers and other personnel

Annual Audits by Third Parties:
Validated by more than a decade of information security audits [5]

CERTIFICATIONS

CSA STAR · Privacy Shield Certified · PCI DSS COMPLIANT · VERACODE · AICPA SOC

GLOSSARY

1. To protect data and account access, the ACS6000 and ACS300 support the latest standard and longer key lengths: TLS1.2+ with AES 256 encryption (the same level trusted for banks) and a SHA256 certificate with a 4096-bit key.

2. Brivo control panels communicate outbound only on port 443. Eliminating "attack vectors" created by open ports on your network.

3. Components that detect malicious "bots" as well as DDoS attacks are embedded in our Brivo Onair Cloud service.

4. Every production component of Brivo Onair has a redundant counterpart; including firewalls, load balancers, web servers, application servers and database servers.

5. Brivo utilizes proper administrative controls to protect sensitive information. We implement the controls in verifiable and measurable ways. Independent auditors periodically check controls and systems to verify compliance. Brivo's annual SOC 2 audits are conducted by an independent service auditor.

brivo®
simply better security
sales@brivo.com
1.833.462.7486
brivo.com

Contact your local Brivo dealer to request additional information.