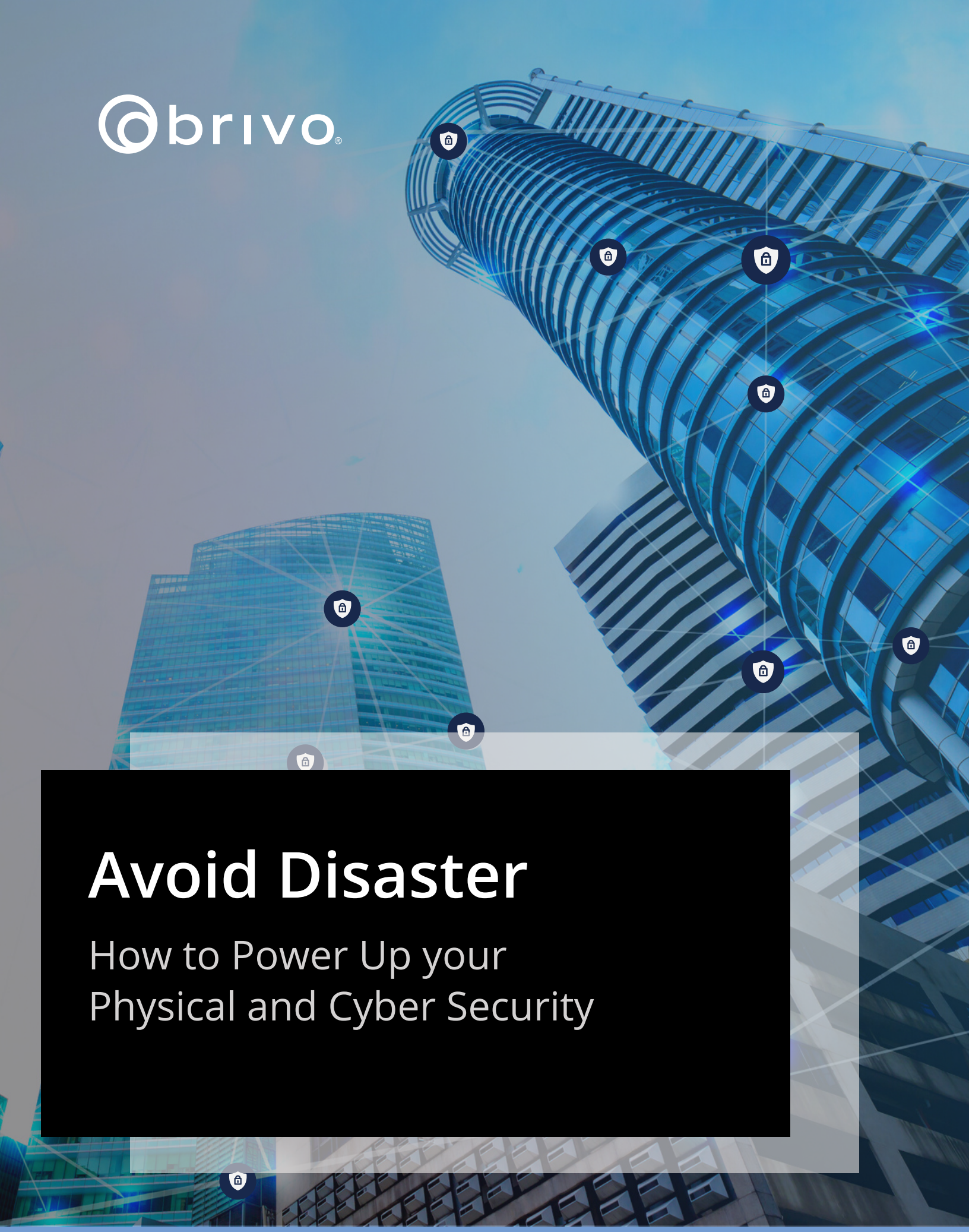


Avoid Disaster

How to Power Up your Physical and Cyber Security

Content

1 Why Should You Read This Guide?

Are you a security expert? If not, this guide is for you. Its aim is to provide a solid grounding in the basics of how to protect a facility. It covers physical and cyber security. At Brivo, security is our business. There's nothing more important to us than keeping your facilities and your information safe.

Brivo looks at security holistically in our technology, people, and processes. We use guidance from industry best practices, applicable publications and international regulatory requirements – all to help you power up your physical and cyber security.

2 An Easy-to-Follow Security Framework

Here's a simple view of three tiers of an access control platform. Don't get us wrong. It's more complicated than this. Physical and cyber security have high stakes. They are complex and ever-changing topics. That's why you hire experts to help you. But this is a useful place to start.

Customer	The Customer layer is how system administrators, security professionals and end-users will interact securely with Brivo Access
Policy	The Policy layer is where security principles become reality
Cloud	The Cloud layer is the foundation of Brivo Access, our secure access control platform

Security is our Business

Protecting your infrastructure and data is our top priority

3 What You Need to Know About Cloud Security

The Cloud layer is the foundation of Brivo Access, our secure access control platform. This includes Cloud Computing Security and Network Security. Let's break these important concepts down.

Cloud Computing Security

This section on Cloud Computing covers three important security decisions Brivo has made for Brivo Access.

Public Cloud Platform

We've optimized Brivo Access to run on an industry-leading public cloud. This cloud provider has a comprehensive security program, and they publicly provide details on that program. Organizations around the globe study and rely on this security. The cloud provider regularly updates its security, and Brivo tracks, evaluates, and adapts to these changes. Cloud security is a shared responsibility.

Resilient Design

To provide high availability of our services, Brivo uses a modern, resilient design. Brivo Access utilizes serverless functionality. This doesn't mean there are no servers. This means that we rely on our cloud provider for our servers. The cloud provider administers, maintains, and patches the infrastructure Brivo Access runs on. How does this ensure the platform is resilient? There are several important things to consider.

Scalability	• Scalability is fundamental for resiliency • This means we can adapt Brivo Access to meet changes in traffic in real-time • Serverless architecture enables Brivo Access to scale as needed
Fault tolerance	• Fault tolerance, or the ability of a system to operate when components fail, is crucial • Brivo Access runs on "highly available," fault-tolerant infrastructure spread across several availability zones • Brivo replicates services across three availability zones • This enables Brivo to provide services and release updates in the (unlikely) event of a public cloud outage
Back-up	• Back-ups are also essential to resilient design • We create back-ups of the Brivo Access database daily at our disaster recovery site • Brivo annually updates and tests our back-up procedures in a test environment to ensure efficient response time • In the event we can't communicate with our servers, Brivo Access Panels at our customer sites capture and store up to 60,000 events

Data Encryption

A key security consideration is how customer data is stored when it is not in use, i.e., data at rest. All data from Brivo Access is stored in the U.S. and encrypted to the industry standard AES-256. This is the same level of encryption used by U.S. financial institutions.

Network Security

Even though the public cloud is secure, Brivo takes extra reinforcing cybersecurity steps. These steps include “logical” settings. Logical security is the use of software and systems to control and limit access to information. We optimize the built-in security features of the public cloud. We also separate information into different accounts and security groups. This provides security by only keeping the least number of ports open.

Web Application Firewall

Brivo uses a firewall, a web security system, to monitor and restrict traffic flowing to the public cloud. This firewall denies traffic from known bad reputation IP addresses.

Intrusion Detection

Brivo uses intrusion detection to keep its systems and customer data safe. A team of security experts relies on the alerts from this system 24 x 7 x 365 to monitor for threats. If suspicious network traffic is detected, the Brivo team rule out false positive alerts. True positives – or actual threats are blocked permanently.

Office Network & Remote Access

Brivo’s office networks use logical separation, firewalls and two different Internet providers. Equipment has battery backup, surge protection and measures to prevent non-authorized access. Brivo has backup air conditioning in the event of HVAC failure. In the event of a disaster, employees can work remotely to provide customer support. In this case, they must use a Brivo-managed VPN to access network resources. Our VPN allows another layer of protection.

4 What You Need to Know About Brivo's Policies

The Policy layer is where security principles become reality. At this layer, we safeguard Brivo Access through policies and procedures. Our policies cover how we make and test changes to software in a secure manner.

Security Policies

We base our security policies on best practices and review them with experts on a regular basis. We engage a third party for annual audits. This ensures compliance with the American Institute of CPAs' criteria. It's known as System and Organization Controls or SOC 2. SOC 2 relies on five principles: security, availability, processing integrity, confidentiality and privacy.

Security Policy Area	Brivo Approach
Risk Management	We scan for risks and publish formal risk assessments every three months. Annually, senior leadership reviews risk assessments and creates an action plan to mitigate risk.
Supply Chain	Security in Brivo's relationships with its suppliers and vendors is vital. If a vendor has access to sensitive data, we evaluate them each year. We seek evidence of security best practices in audit reports, white papers and other security material. If we have concerns, we clarify and remediate them with our vendors.
System Access	Before granting access, Brivo thoroughly screens its employees in a five-part process. The process includes: 1. Completing interviews 2. Passing background checks 3. Signing confidentiality clauses 4. Acknowledging the employee handbook 5. Passing security training Brivo has a policy that governs access to sensitive systems based on the user's role with "least privilege" principles. This principle says that only the minimum necessary rights should be assigned. And further, that those rights should be in effect for the shortest duration necessary.

Brivo looks at security holistically in our technology, people and processes. We use guidance from industry best practices, applicable publications and international regulatory requirements.

Security Policy Area	Brivo Approach
Security Training	Brivo trains 100% of our employees on our robust security policies. Our employees receive training when they begin onboarding, and we refresh their training every year. We customize the training based on the employee's role. The curriculum covers: • physical security • safety • account management • social engineering attacks • data classification • information handling • security policies • how to report security events and more
Office Access	• Brivo offices are secured at the building and office level using our products. • We issue access control cards with the minimum access needed to perform their duties. • Brivo uses difficult to reproduce smart cards to access secured areas. • We have cameras throughout our offices. They monitor all access points and secure areas. • Security guards patrol the building and surrounding premises. • Visitors must sign in and receive an escort from an authorized Brivo employee. • Visitors wear unique badges while on the premises and return the badges when they leave.

Software Development Policies

Brivo uses security best practices throughout the Software Development Life Cycle (SDLC). This means that security is included throughout phases of development and deployment.

Secure Development

Brivo engineers receive training on how to develop software securely. We customize the curriculum to the programming language(s) the engineer uses. Completion is mandatory. Engineers receive messages in their development environments. These messages highlight security best practices or vulnerabilities. Engineers can also create a sandbox on their machine to check for flaws.

Change Control

Brivo takes extreme care that all system updates are secure. Updates follow strict criteria including formal documentation, automated testing and engineering review. Once changes are deployed, we will test to make sure that everything still works as designed (regression testing). We resolve issues by either rolling back or rolling forward as determined by the engineering team.

Vulnerability Scanning

Brivo uses three types of analysis to scan Brivo Access for vulnerabilities:

1. Static analysis scans of Brivo Access's software code are done automatically every time there's an update.
2. Source component analysis is built into our static analysis. It scans the third-party libraries that Brivo Access relies on. We check that the versions of libraries are free from known vulnerabilities.
3. Dynamic analysis scans are done weekly. Dynamic analysis is automated testing that crawls the website to potentially identify or exploit any vulnerabilities.

Third-party Testing

Brivo contracts with a well-respected third-party provider to test its systems every year. These tests aim to 1) discover vulnerabilities and 2) to exploit them. If our testing provider finds vulnerabilities, Brivo prioritizes fixes with our engineering teams. The testing provider re-tests our fixes. Our goal is to have no vulnerabilities after remediation.

5 What You Need to Know About Security at the Customer Site

The customer layer is how system administrators, security professionals and end-users will interact securely with Brivo Access.

Administering Brivo Access

An administrator is a Brivo Access user with privileges to sign in to the Brivo Access application. An administrator can observe or make changes to an account that controls one or more sites.

Sign-on

Brivo authenticates administrators by an email address and password. Brivo recommends administrators enable two-factor authentication on their account. Brivo Access supports "cookies" for a better user experience - allowing return to previous information in a browser. These cookies have the secure flag enabled. Administrators must log back in every 14 days.

Logging & Reporting

Administrator activity is logged in a report in Brivo Access. Examples includes log-ins, customer support requests, video motion events, and other events. Administrators can download an event log by running reports. Brivo retains the data according to https://www.brivo.com/terms-of-use-brivo-services.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol for email, messaging and the internet. Currently, Brivo Access supports TLS 1.3, and we have an A+ grade from Qualys SSL Labs. We watch for new best practices and create action plans to put them in place as they become available.

Access Control Panels

Brivo's access control panels are smart hardware that safeguards your buildings. These panels centralize your security system's intelligence. They control access through readers, door controls, and sensor hardware like latches and switches. Because of this significant role they play, it's essential that they meet Brivo's security standards. How do we do this?

Logging into an Access Control Panel

We start by making sure only authorized users can make changes. We do this by password-protecting the access control panels. We also make sure that panels are only accessible by a direct Ethernet connection. We encourage our customers to install panels in secure locations. From a cybersecurity perspective, we monitor the panels' connections. Any time a panel attempts communication with an unknown server, we will block it and sound an alarm. This prevents cyber-attacks.

Networking

For security, the Brivo control panel initiates communication sessions with the Brivo server. Panels will not accept inbound connections. They will only listen to network traffic within a secure session that was initiated by the control panel itself. This prevents cyber-attacks and unintended harm to the panels.

Encryption

We encrypt the data on the control panel using the AES256 encryption algorithm. The banking and financial services sector also rely on this level of encryption. When the control panels communicate with the Brivo data center, we protect the contents of that communication with a technology known as public key infrastructure (PKI). PKI, through digital certificates, lets Brivo offer our customers a high degree of confidence in our encryption.

Mobile Application Security

This section covers Brivo's security for two mobile applications. The first is the Brivo Access app. This application is for administrators. They can view activity, update permissions, and unlock doors, all from their mobile device. The second is Brivo Mobile Pass. This application provides users with virtual credentials to access doors.

Brivo Access App

The Brivo Access app authenticates the user through the same means as the Access web application. Activity in the mobile application is logged in the same way as the Access account. Administrators also have the same level of permissions in the application as they would in their Access account.

Brivo Mobile Pass

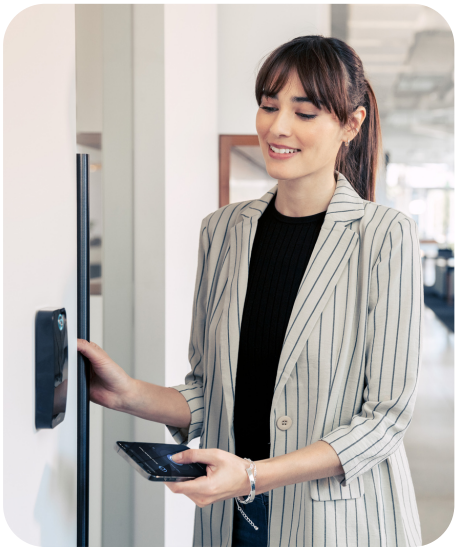
For a mobile credential to work, an administrator must assign it using a valid email address. The credential holder must confirm the credential using the same email address. The user will receive an email to activate the application on their phone. Brivo Mobile Pass will operate doors over Bluetooth, WiFi and NFC using encryption and timestamping.

6 Key Take-aways

Avoid disaster – power up your knowledge of physical and cyber security with a **trusted partner** like Brivo

Through our **20+ years** of experience, we've built technical know-how. We can keep your buildings, assets and end-users **safe and secure**

Our ultra-secure cloud deployment and careful policy choices lead to **simply better security**



WHY BRIVO

Brivo, Inc., created the cloud-based access control and smart spaces technology category over 20 years ago and remains the global leader serving commercial real estate, multifamily residential and large distributed enterprises. The company's comprehensive product ecosystem and open API provide businesses with powerful digital tools to increase security automation, elevate employee and tenant experience, and improve the safety of all people and assets in the built environment. Brivo's building access platform is now the digital foundation for the largest collection of customer facilities in the world, occupying over 300 million square feet across 42 countries.

visit brivo.com

To learn more about Brivo Access and security, contact:

brivo.com

brivo

contact us to get started:
sales@brivo.com