# Device Guardian Access Management (DGAM) Security Architecture

This content was last updated in May 2025 and represents the status of DGAM and its vendors at that time. As Zebra continues to work to strengthen its security policies and practices, this information may change.

# Table of Contents

# 1. Zebra's Approach to Security

Device Guardian Access Management (DGAM) is an elegant, easy-to-use software solution to manage and control your mobile assets. DGAM is the intelligent way to keep your mobile computers safe.

Zebra Technologies has implemented reasonable administrative, technical, and physical safeguards to help protect against security incidents and privacy breaches involving a Zebra Technologies product, provided those products are used in accordance with Zebra's instructions for use. Working with key technology partners such as Google, Zebra Technologies leverages their capabilities while also adding the best practices and technology expertise of our enterprise data-driven professionals. We do this to ensure that the enterprise-grade of security and compliance protocols are met. We work to anticipate risks and partner with industry leaders to earn the trust of our customers. This dedication is backed by a security structure to ensure all aspects of security have oversight. However, as systems and threats evolve, no system can be protected against all vulnerabilities, and we consider our customers our most important partners in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention, and we will investigate. Where appropriate, we will address the issues with product changes, technical bulletins, and/or responsible disclosures to customers and regulators. Zebra continuously strives to improve security and privacy throughout the product lifecycle using practices such as:

- Privacy and Security by Design
- Product and Supplier Risk Assessments
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning and Third-Party Testing
- Access Controls appropriate to Customer Data
- Incident Response
- Clear paths for two-way communication between customers and Zebra

The purpose of this document is to highlight how Zebra's security and privacy practices have been applied to Device Guardian Access Management.

## 1.1 Software Assurance Maturity Model (SAMM)

Security it a multi-faceted issue. To ensure that we are addressing all aspects we have adopted the OWASP Software Assurance Maturity Model (SAMM). This model provides an effective and measurable way for Zebra to analyze and improve their software security posture.

The three main characteristics of SAMM are:

1. **Measurable:**
   Defined maturity levels across security practices
2. **Actionable:**
   Clear pathways for improving maturity levels
3. **Versatile:**
   Technology, process, and organization agnostic

## 1.2 Standards Compliance

In addition to internal processes, we verify that our partners comply with industry standard software security certifications.

- **ISO/IEC 27001—Information security management**

  ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS). ISO 27001 certification by a vendor assures Zebra that the vendor complies with proper management of assets such as financial information, intellectual property, employee details, or information entrusted by third parties.

- **SOC 2®—SOC for Service Organizations: Trust Services Criteria**

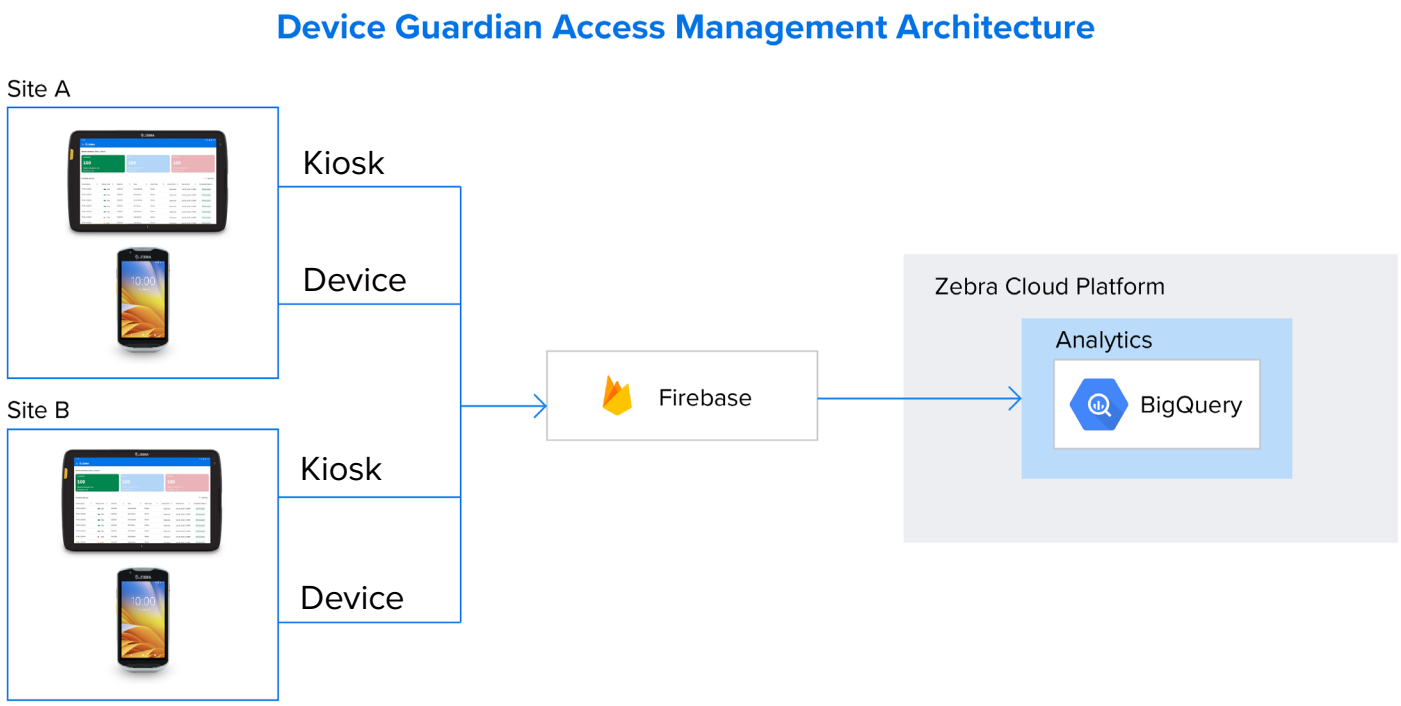
  A SOC 2 report is a description of a service organization's system and the suitability of the design and operating effectiveness of controls relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

  As of the writing of this document, Zebra has confirmed that Google complies with both ISO/IEC 27001 and SOC 2 standards. Compliance documentation is publicly available at:

- Google Cloud Compliance and Regulations

# 2. Architecture

## 2.1 DGAM High Availability Architecture




# 3. Physical and Logical Security

## 3.1 Cloud Providers

The cloud provider used by Zebra is Google. The Google Cloud Platform (GCP) allows Zebra to innovate faster and realize its vision of delivering enterprise asset intelligence to its customers.

## 3.2 Data Isolation

DGAM provides a separate instance for each customer. Only GCP has physical access to these servers, and GCP is responsible for the physical hardware and networking. Zebra has control of the application and data that resides within GCP Services, such as Google Cloud SQL.

## 3.3 Data Sovereignty

Data is governed by laws of the country in which it is physically stored, as well as the jurisdiction to which the data subject resides (i.e., GDPR). Zebra ensures that data is hosted in data center pairs where both members are either in the same jurisdiction or in mutually compatible jurisdictions guaranteeing the data sovereignty is retained should data be transferred from data center to another.

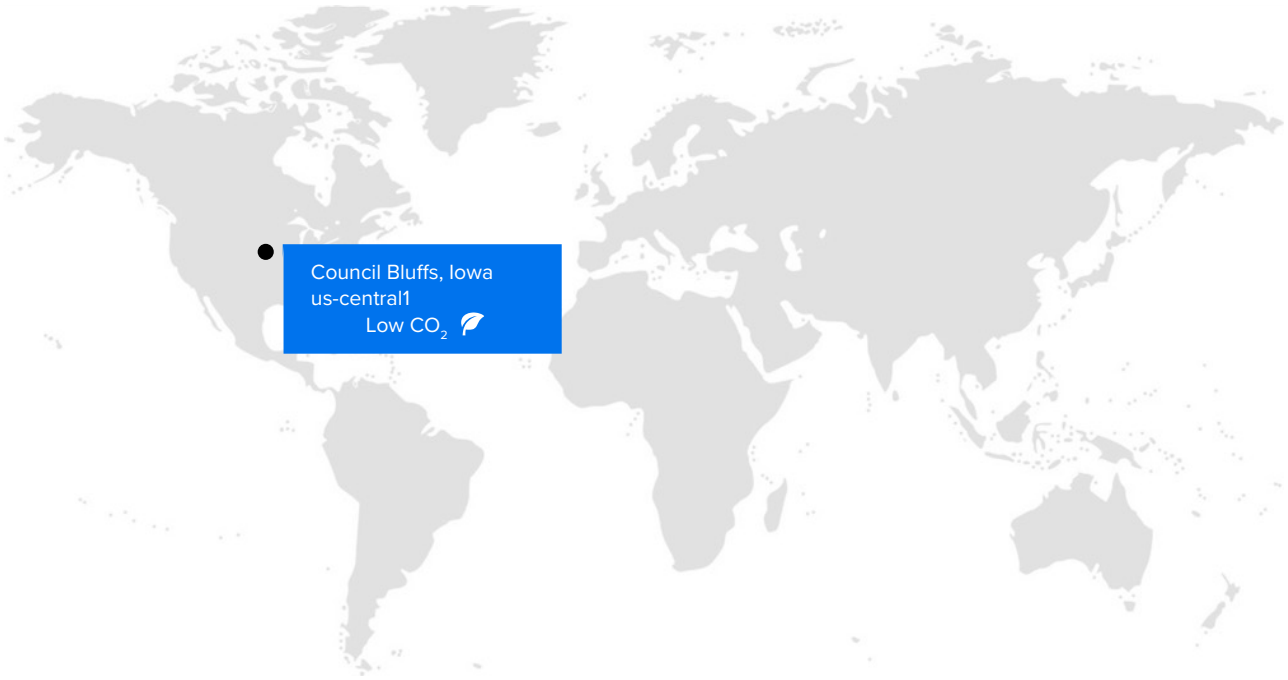
## 3.4 Customer Site Security

Zebra customers are responsible for physical security at the customer site.

Zebra customers often require the ability to configure Firewall settings to allow the customer network to securely connect to our Zebra Data Services API. It is strongly recommended that firewall rules target the Fully Qualified Domain Name (FQDN) and are reviewed annually ensuring that only necessary connections are configured.

## 3.5 Google Data Centers Used by DGAM

DGAM uses Google data centers to achieve enterprise level system uptime, resiliency, and security. All customers use data centers based in the US region. Google services are deployed to the us-central1 region, which is located in Council Bluffs, Iowa. In the event of a catastrophic event, Disaster Recovery activities are targeted from a multi-regional GCP storage bucket.



# 4. Availability

## 4.1 Data Backup and Recovery

Data within DGAM is stored in a Google Storage Bucket automatically. All administrative activities are automated by GCP, including backups, failover, replication, software patching, and capacity scaling. Firestore offers near-zero downtime of less than 10 seconds for planned maintenance, with flexible maintenance windows.

Because we utilize public cloud services for hosting, backup, and recovery, Zebra does not implement physical infrastructure or storage media within DGAM other than the kiosks located at the customer site.

For more information on the robust features of Firebase Firestore, please see: https://firebase.google.com/docs/firestore

## 4.2 Disaster Recovery

DGAM operates on a business continuity/disaster recovery plan that conforms to the National Institute of Standards and Technology (NIST) publication entitled “NIST Special Publication (SP) 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems.” The disaster recovery plan has been reviewed and scored by a third-party consultant. Disaster recovery testing occurs annually. Random years are observed by the third-party consultant.

For more information on NIST SP 800-34, please visit: https://www.nist.gov/privacy-framework/nist-sp-800-34

## 4.3 Business Continuity

Kiosks located at customer sites act as edge servers and are capable of keeping normal business operations functioning in the event of interruption at DGAM Cloud Servers. It keeps track of devices and their statuses, and it enables users to continue with their business by checking-out their devices.

# 5. Information Lifecycle

## 5.1 Data Retention

For data stored and processed by Zebra, the specific terms of the customer’s contract with Zebra Technologies defines the data retention policy that is configured in DGAM. Zebra recommends storing the minimum necessary data required to make use of the historical tracking features available in DGAM.

## 5.2 Data Destruction

DGAM is hosted on Google Cloud Platform. When data is deleted under the terms of the contract with the customer, the following steps occur in the deletion pipeline.

1. Respond to deletion request
2. Data removal
3. Logical deletion from active systems
4. Backup expiration
5. Secure media sanitization

In addition to the deletion pipeline, a disciplined media sanitization program enhances the security of the deletion process by preventing forensic or laboratory attacks on the physical storage media once it has reached the end of its life cycle.

# 6. Vulnerability Management

## 6.1 Vulnerability Scanning

Zebra conducts continuous scanning of Zebra platforms using third party tools such as CodeQL and SonarQube. Continuous monitoring of defect resolution occurs in Nucleus, and procedures are in place to automatically open and track known issues. Identified vulnerabilities are assessed for risk and mitigated or remediated according to their severity level. Zebra conducts penetration testing annually, or when significant changes warrant an early retest. Penetration testing typically includes server hardening, exposed services, backups, public code repositories, exposed internal services by misconfiguration, and exploitation of older software versions.

## 6.2 Patch Policy

Zebra enforces a Patch Management Policy to ensure that all Zebra cloud systems and applications are proactively managed and patched with appropriate security updates. A patch corrects an identified operational or security issue or delivers minor functional enhancements to infrastructure and application software. Patch Management is a continuous activity designed to prevent risk events that result in inadequate management of technology estate.

## 6.3 Distributed Denial of Service (DDoS) Attacks

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users of the service or resource they expected.

Google Cloud Armor safeguards content hosted on the system. It is configured with a combination of industry-standard and custom rules capable of automatically enabling and disabling the most effective controls to safeguard our customers. The Google Cloud Armor rules used to detect and block malicious traffic are in accordance with the best practice guidelines documented by OWASP, specifically the OWASP Top 10. Protection against DDoS attacks is included, ensuring Zebra products are always accessible.

For a link of how Google was able to detect and shut down a DDoS attack measuring 46 million requests per second, please see the following article: https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

# 7. Encryption

Encryption is a process that takes legible data as input (often called plaintext) and transforms it into an output (often called ciphertext) that reveals little or no information about the plaintext. The encryption algorithm used is public, such as the Advanced Encryption Standard (AES), but execution depends on a key, which is kept secret. To decrypt the ciphertext back to its original form, you need to employ the key.

## 7.1 Encryption in Transit

All DGAM connectivity to web pages is encrypted in transit using HTTPS/Transport Layer Security (TLS).

Only Zebra employees whose jobs require it may access the Google environment, which includes infrastructure tools, servers, and services. Those persons connect securely via AES-128 encryption and requires multi-factor authentication.

Google Pub/Sub messages from devices are not currently the primary transport mode for data. However, if such a message is sent, the message is secured via Customer Managed Encryption Keys (CMEK). In this case, Zebra manages the key.

For more information on Encryption in Transit, please see: https://cloud.google.com/docs/security/encryption-in-transit

## 7.2 Encryption at Rest

All DGAM data stored in Google Cloud is encrypted at the storage level using AES-256. Firestore automatically encrypts all data before it is written to disk. The data is automatically decrypted when read by an authorized user.

For more information on Encryption at Rest, please see: https://cloud.google.com/firestore/docs/server-side-encryption

# 8. Personnel

Zebra has created a vibrant security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training, and in company-wide events to raise awareness.

## 8.1 Security Awareness

All employees and non-employees are required to participate in mandatory education and training activities as part of Zebra's security awareness program. Continuing education campaigns, annual security training, and targeted security bulletins are among the actions designed to maintain the effectiveness of Zebra's security posture.

## 8.2 Employment Requirement Guidelines

Zebra regularly screens its offer-stage employment candidates with a background check. Prior to beginning employment, all candidates must submit to a drug screening.

## 8.3 Background Checks

The background method used by Zebra differs depending on the candidate's future role and applicable law. Background checks, to the extent permitted by law.

- Employment history
- Verification of education, as required based on role
- Criminal search
- Social Security Number verification
- Global sanctions and enforcement check

## 8.4 Subcontractors

Zebra requires subcontractors to assure the competency and eligibility of its employees who provide services to Zebra's clients. Subcontractor personnel are required to complete background checks applicable to the services performed and must be at least as stringent as those required of Zebra employees.

## 8.5 Third Party Risk Management

Zebra requires business associate agreements and nondisclosure agreements with the suppliers it uses to provide the solution, as appropriate based on that entity's access to data and other confidential information. Zebra requires that its suppliers complete a security questionnaire as part of the evaluation process for the supplier. In addition, Zebra conducts annual supplier security risk assessments based on that supplier's risk profile.

# 9. Incident Management

Zebra's Security and Monitoring team is the control center for security incident management and continuous threat monitoring 24 hours a day, 7 days a week, 365 days a year. To protect Zebra environments, the Security and Monitoring Team coordinates responses to international, federal, and technology sector threat intelligence information. Furthermore, the team leverages industry standard tools and techniques to monitor logs to detect possible unauthorized activity and focus on prospective threats.

Zebra maintains a security incident management process to investigate, mitigate, and communicate system security events occurring with a tenant. Customers who have been impacted are promptly notified of relevant security incidents and advised of necessary corrective actions to be taken.

Zebra does not publicly discuss "named" vulnerability events (i.e., WannaCry, SamSam, etc). If customers have questions about Zebra's approach to certain events, Zebra will engage in private discussions.

## 10. Change Management

Zebra uses the Scaled Agile Framework (SAFe) to track changes through the Software Development Lifecycle. Code changes are managed through controlled Program Increments that follow the change from initial approval through release.

Our security best practices are tailored to the type of change and level of risk involved. Security reviews are conducted at multiple checkpoints in the Software Development Lifecycle. Changes are validated, assessed, and approved commensurate with the risk they pose. Change Advisory Boards (CABs) are used by Zebra to review major changes with known downtime or heightened risk.

## 11. Disclaimer

The information contained in this Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and Zebra, or Zebra's subsidiaries or affiliates (collective, "Zebra"). Zebra does not make any promises or guarantees to customer that any of the methods or suggestions described in this Security White Paper will restore customer's systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Security White Paper.

ZEBRA

**NA and Corporate Headquarters**
+1 800 423 0442
inquiry4@zebra.com

**Asia-Pacific Headquarters**
+65 6858 0722
contact.apac@zebra.com

**EMEA Headquarters**
zebra.com/locations
contact.emea@zebra.com

**Latin America Headquarters**
zebra.com/locations
la.contactme@zebra.com