ZEBRA

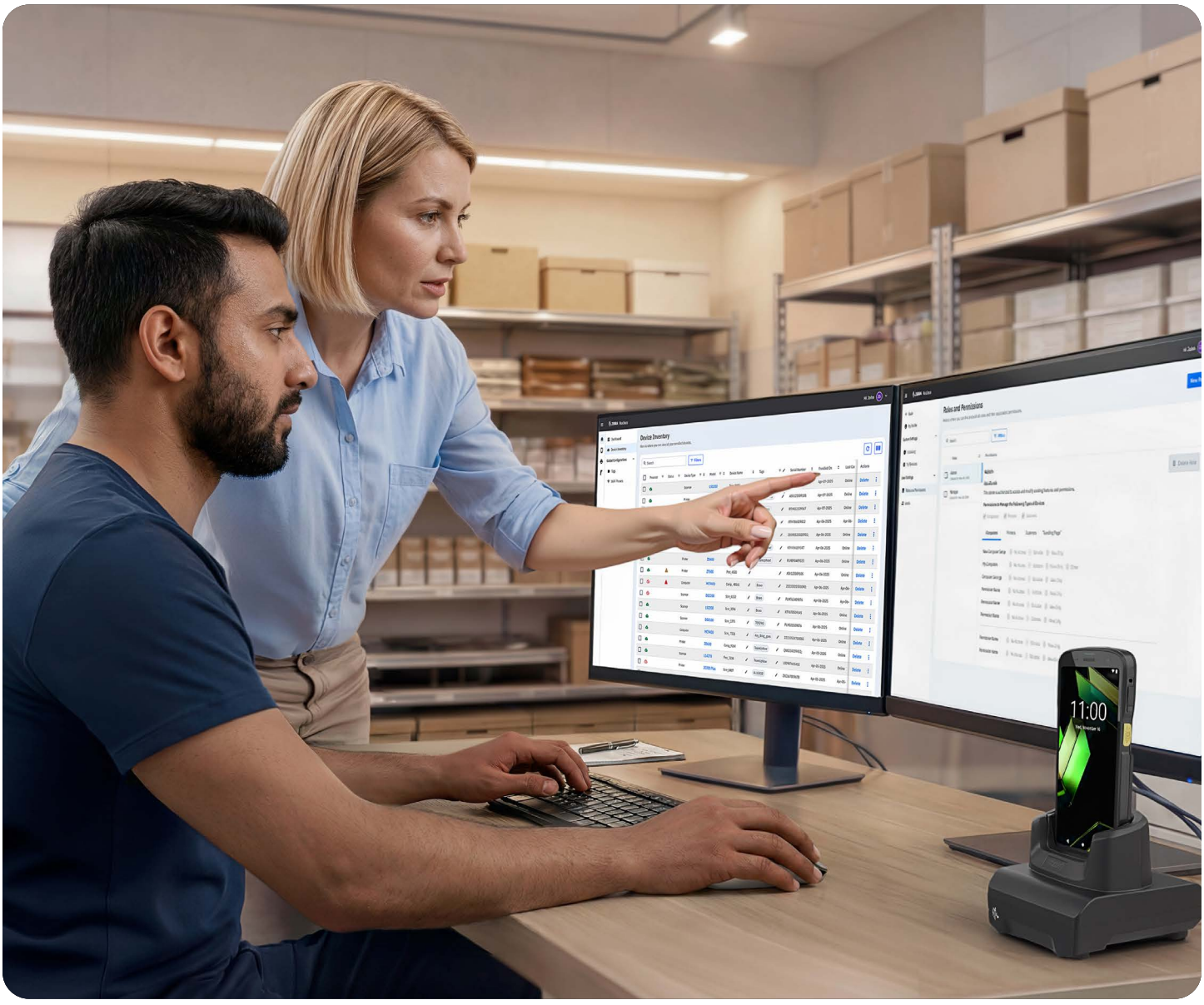
# Zebra Nucleus

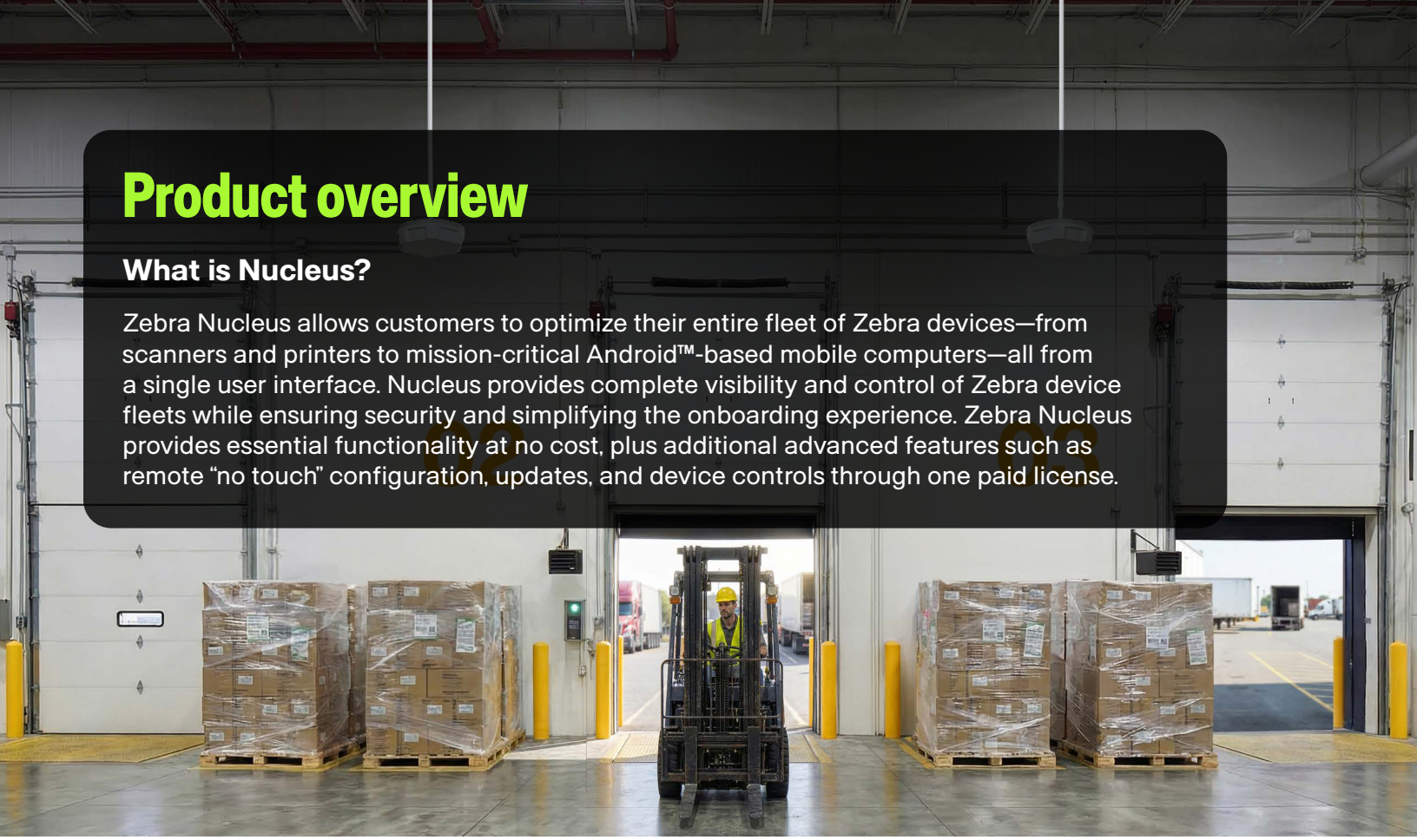
Secure-by-default device management and compliance guide

# Table of contents

# Introduction

In today's highly connected enterprise landscapes, network security is only as strong as its least-protected endpoint—and edge devices like mobile computers, barcode scanners, and thermal printers are often the overlooked gateways to sensitive corporate networks. The Zebra Enterprise Device Security Playbook serves as the authoritative, blueprint-style resource designed specifically for IT administrators, cybersecurity professionals, and Independent Software Vendors (ISVs) tasked with safeguarding enterprise operational environments. Recognizing that these edge devices handle critical real-time data and sit directly on corporate subnets, this guide bridges the gap between high-level security theory and tactical deployment. By combining threat-modeling insights with hands-on, step-by-step device-hardening procedures, this document provides the actionable configurations and best practices necessary to eliminate vulnerabilities, protect data in transit, and ensure your entire fleet of Zebra printers, scanners, and mobile computers stands resilient against modern cyber threats.





# Product overview

## What is Nucleus?

Zebra Nucleus allows customers to optimize their entire fleet of Zebra devices—from scanners and printers to mission-critical Android™-based mobile computers—all from a single user interface. Nucleus provides complete visibility and control of Zebra device fleets while ensuring security and simplifying the onboarding experience. Zebra Nucleus provides essential functionality at no cost, plus additional advanced features such as remote “no touch” configuration, updates, and device controls through one paid license.

## Key features and benefits

### Fleet management and optimization

Manage printers, mobile computers, and scanners from anywhere in the world through a single user interface. Administrators gain complete visibility into device status, online/offline presence, alerts, and errors across their entire fleet.

### Device updates and configuration

Configure all device settings and update device OS or firmware remotely, ensuring consistent and up-to-date deployments across the fleet.

### Visibility and control

Get real-time status monitoring and comprehensive control over device configuration, ensuring settings are enforced consistently across the workforce.

### Simplified onboarding

Nucleus provides multiple options for customers to onboard their devices, streamlining the initial setup process and reducing deployment time.

### Remote “no touch” configuration

Administrators can configure devices without manual intervention, significantly reducing onboarding time and minimizing human error.

### Secure operations

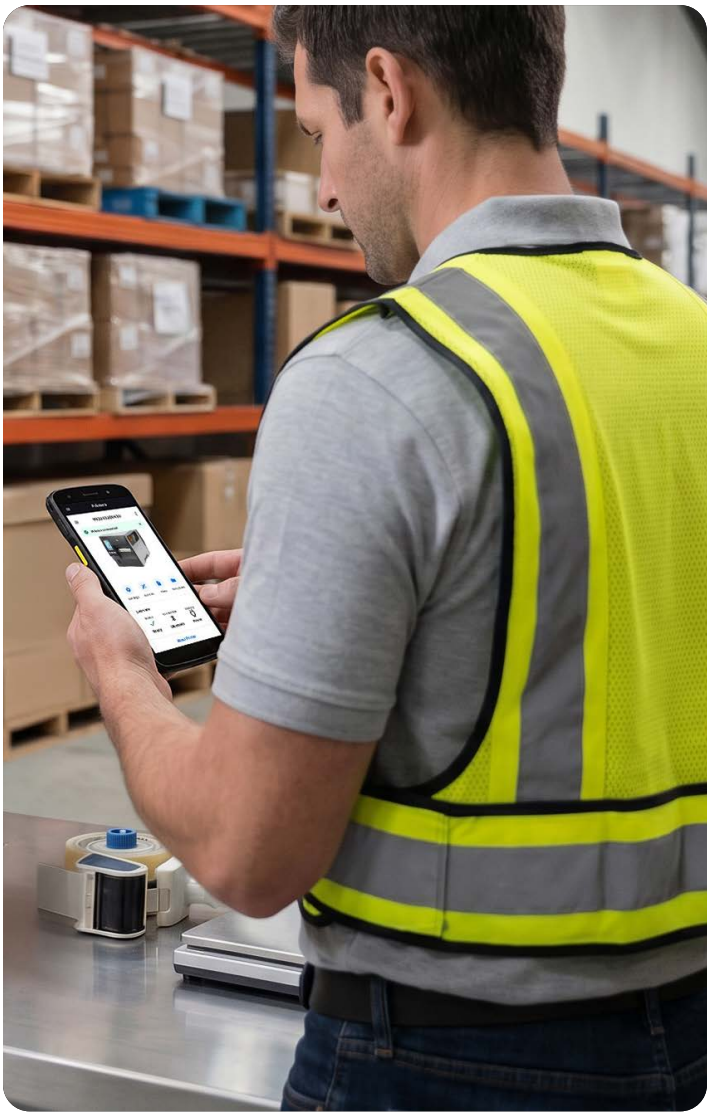
Multiple layers of security protect device data and corporate information throughout the device lifecycle.

## Target users and deployment scenarios

Nucleus serves customers across all verticals and organization sizes, ranging from small business owners with a single device to large enterprise customers with 10,000+ devices.

### Deployment models

Nucleus is a SaaS-only product. However, it includes complementary components: Nucleus Client (Windows®): Acts as a proxy between scanners that lack network connectivity (e.g., Bluetooth or USB only) and the Nucleus SaaS product, enabling management of disconnected devices. Nucleus Connector (Mobile): Assists with printer onboarding and device configuration.



## Use cases

### Small business

A small retail shop with 5 scanners uses Nucleus to see real-time status of their devices and ensure their configuration is kept consistent.

### Enterprise

A multi-national logistics company with 10,000+ devices across multiple regions uses Nucleus to see their large number of devices at a glance and ensure that device configuration is enforced consistently across their entire workforce.

# System overview

## Architecture overview

Nucleus operates as a cloud-based fleet management platform where customers must onboard their devices to enroll them with the product. The onboarding process is tailored to each device type:

### Mobile computers

Customers use the Nucleus web UI to create a “New Computer Setup” that allows them to configure the device’s WiFi or Ethernet settings. The setup wizard then presents a barcode that the mobile computer can scan to enroll itself into Nucleus.

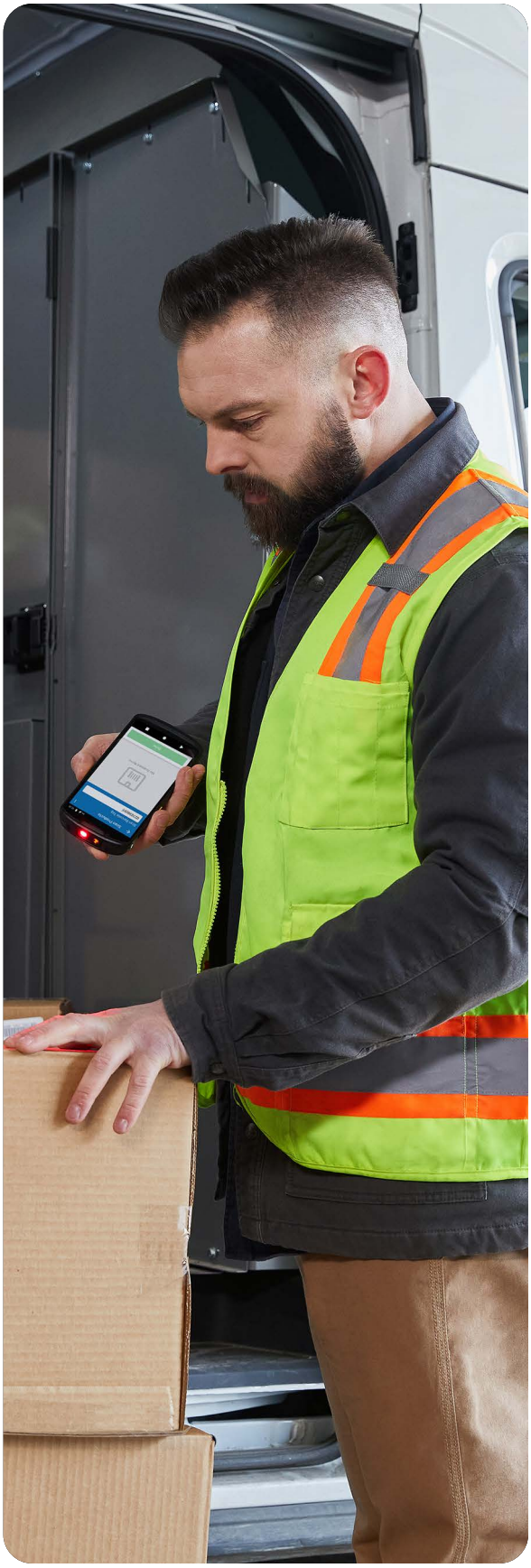
### Scanners

Customers create a setup in the Nucleus web UI and download the Windows Nucleus Client along with a unique configuration file. The Windows Nucleus Client is installed with the custom configuration file, which provides secure connection details to  the customer’s Nucleus tenant.

### Printers

Customers have four configuration options: 1. Use USB or Bluetooth via a Chrome browser to discover locally connected printers and configure them 2. Format a USB drive to utilize the printer’s USB mirror feature for configuration 3. Use the Nucleus Connector to complete the final configuration step 4. Manually configure WiFi/Ethernet settings in the Nucleus web UI (common to all Zebra hardware device types).

**Once devices are enrolled, they establish long-lived, streaming connections to Nucleus for real-time communication and status reporting.**



## Core components

**Nucleus web UI**

The primary interface where administrators create onboarding setups, configure devices, monitor fleet status, and manage device settings.

**gRPC Backend APIs**

The main communication protocol between the Nucleus web UI and backend services, as well as between scanners (via the Windows Nucleus Client) and the backend. All gRPC connections use TLS 1.2 or higher. There are various REST APIs for some aspects of the product that will eventually migrate to gRPC methods over time.

**WebSocket Connections**

Printers establish secure WebSocket connections over TLS with mutual authentication. Each printer has a unique client certificate scoped to its tenant.

**Nucleus Client (Windows)**

Runs on Windows systems and acts as a proxy between scanners without network connectivity (Bluetooth or USB connections) and the Nucleus SaaS backend. Stores device certificates in the Windows Certificate Manager.

**Nucleus Connector**

Assists with printer onboarding and device configuration on mobile devices.

**Google Kubernetes Engine (GKE)**

The primary infrastructure platform hosting the majority of the Nucleus product and backend services.

**PostgreSQL Database**

Hosted on Google Cloud, serves as the primary relational database for tenant data, device configurations, user accounts, and system state.

**Redis Memorystore**

Hosted on Google Cloud, used for ephemeral operations and caching when durability is not required.

**Google Firebase**

Provides cloud messaging and connection infrastructure for mobile device connections to Nucleus.

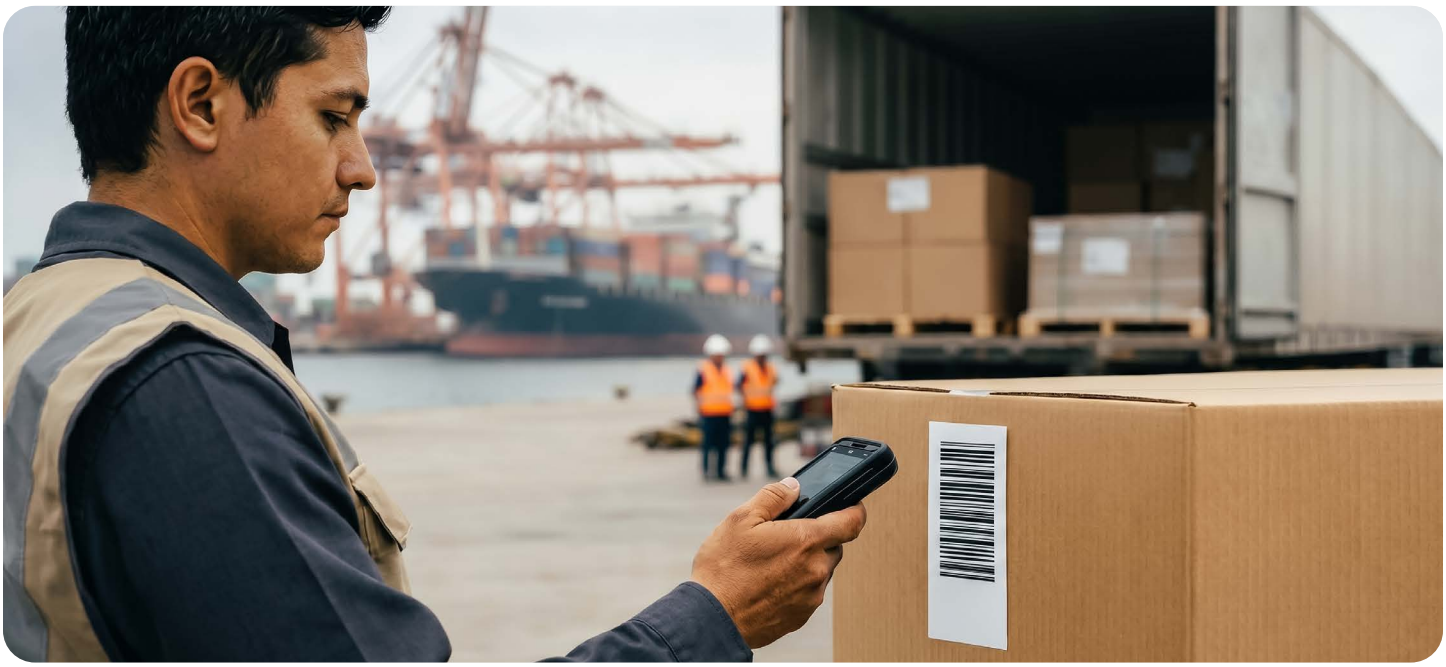
**Internal Message Queuing System**

Handles asynchronous device operations and keeps the digital device representation (digital twin) synchronized with the actual device state.

## Data flow and architecture

### Scanner device enrollment flow

1. Customer creates an onboarding setup in the Nucleus web UI, specifying device type and network settings
2. Windows Nucleus client is installed with configuration file scanner
3. Device locally connects to the Nucleus Client
4. The Windows Nucleus Client connects to Nucleus via gRPC.
5. On first connection, the Windows Nucleus Client provides a nonce (generated per tenant) along with its tenant ID.
6. Backend verifies the nonce against the stored value for that tenant
7. Upon successful verification, a unique client certificate is generated and exchanged
8. Future connections use TLS mutual authentication with the client certificate
9. Device is linked to its digital twin in the Nucleus backend by tenant ID and unique serial number



## Data flow and architecture

### Printer device enrollment flow

1. Customer creates an onboarding setup in the Nucleus web UI, specifying device type and network settings
2. A configuration file is sent to the device via BT or USB (printer)
3. Device applies network settings and connects to the internet
4. Device establishes connection to Nucleus via WebSocket over TLS
5. Connections use TLS mutual authentication with the client certificate
6. Device is linked to its digital twin in the Nucleus backend by tenant ID and unique serial number

## Data flow and architecture

### Mobile device enrollment flow

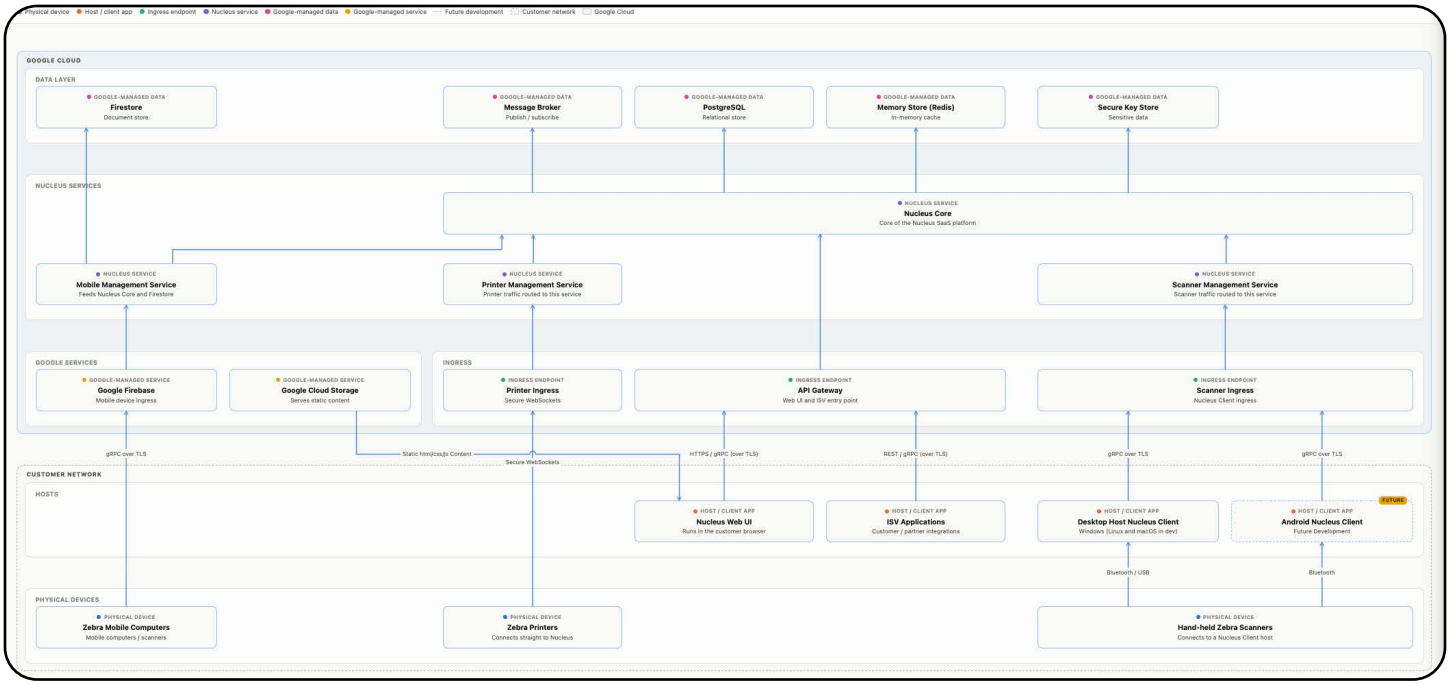
Configuration push flow

1. Administrator makes a change in the Nucleus web UI (e.g., push a firmware update, change device settings)
2. Web UI sends request to backend via gRPC method
3. Backend gRPC method verifies the user is authorized to perform the action
4. If the action affects system preferences or non-device settings: data is written directly to PostgreSQL
5. If the action involves a device:
   - Message is queued in the internal message queuing system
   - Message is routed to the target device(s) based on tenant ID and serial number
   - Device receives and applies the configuration
   - Device confirms completion, and the digital twin is updated to keep backend state synchronized

Status reporting flow

1. All device connections to Nucleus are long-lived, streaming connections
2. Devices continuously report status, alerts, errors, and health metrics over their established connection
3. Status data is processed and stored:
   - Device presence (online/offline) is tracked in real-time based on connection state
   - If the long-lived connection drops, device is marked offline
   - When connection resumes, device is marked online
4. Historical data is retained indefinitely pending future retention policy definitions
5. Dashboard displays aggregated device status and metrics in real-time

# SYSTEM OVERVIEW



# Integrations and deployments

## Deployment model

Nucleus is a SaaS-only product hosted on Google Cloud and accessible worldwide. All infrastructure, databases, and services are managed by Zebra and hosted on Google Cloud Platform.

## Complementary components

- **Nucleus Client (Windows):** Deployed on customer Windows systems to enable scanner management
- **Nucleus Connector:** Deployed on customer mobile devices to assist with printer onboarding

## Third-party integrations

Nucleus integrates with the zDNA system for much of the mobile device management functionality. Nucleus serves as the authentication provider for users and acts as a facade to much of the zDNA functionality, providing a unified management interface for customers.

# Multi-tenancy and data isolation

Nucleus is a multi-tenant SaaS platform with strict data isolation between customers. The system ensures that users can never access data from tenants they are not authorized to view.

## Tenant identification

When a device connects to Nucleus for the first time, it provides:

- For scanner and printers—a unique certificate for scanners and printers (generated per tenant)
- For mobile devices—a secure token from the server, (generated per tenant)

This token is presented to the server during its communication. The backend verifies that the provided tenant ID matches the nonce, ensuring each device is correctly assigned to its tenant.

## Data isolation architecture

Nucleus uses PostgreSQL's schema concept to logically separate data for each tenant within the same database infrastructure. This approach provides:

- Logical tenant separation at the database level
- Efficient resource utilization while maintaining complete data isolation
- Simplified backup and recovery operations per tenant

## User access control

- Users can only see and interact with data from tenants they are explicitly authorized to access
- Users cannot view or modify data from other tenants
- Users interact with a single tenant at a time, though the product allows them to switch between authorized tenants in the web UI
- The most common use case for multi-tenant access is Zebra partners who manage multiple customer fleets as a service

## Query scoping

All gRPC API calls and database queries are automatically scoped to the authorized tenant. The backend enforces tenant boundaries at the query level, ensuring data from one tenant is never returned to users of another tenant.

# Security

Nucleus implements multiple layers of protection to safeguard customer and user data throughout the product lifecycle. All data is encrypted at rest using industry-standard encryption, secure communication protocols are enforced, and continuous security monitoring and testing are performed.

# Data storage

Nucleus stores two primary categories of data:

**User account data**

Limited personal information provided by users during account creation, including first name, last name, and email address. This data is stored in PostgreSQL within the Google Cloud us-central region (Iowa, US). zDNA does not store any user data when used with Nucleus.

**Device data**

The majority of Nucleus storage consists of device-related data, including:

- Device configuration settings
- Device status and health metrics
- Enrollment information
- Historical telemetry and logs
- Digital twin representations of managed devices

---

Device data does not contain personal identifiable information (PII). All data is stored in Google Cloud's us-central region (Iowa, US) and encrypted at rest on Google's infrastructure.

# Security of data at rest

## Data at rest—in Cloud

All data stored in Nucleus is encrypted at rest using AES-256 encryption. The encryption architecture leverages multiple layers of protection:

### Encryption key management

- All sensitive encryption keys are stored and managed in Google's Key Management Service (KMS)
- Keys are never stored in plaintext within the application or database
- Google KMS manages key rotation, access control, and audit logging for all encryption keys
- Only authorized Nucleus services have access to encryption keys through Google KMS

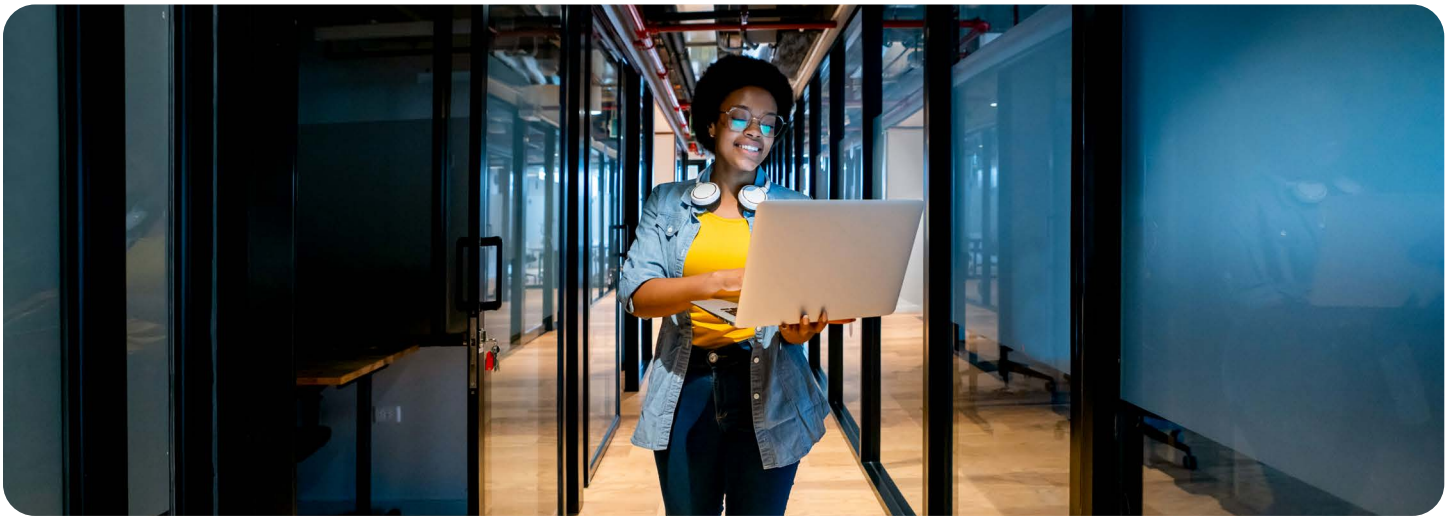
### Database encryption

- PostgreSQL databases storing customer and device data are encrypted at rest using AES-256
- Encryption is enforced at both the application level and the Google Cloud infrastructure level
- Redis Memorystore used for ephemeral data also encrypts data at rest

### Data retrieval process

When data is retrieved from storage:

1. Application requests data from PostgreSQL or Redis
2. Data is decrypted using keys retrieved from Google KMS
3. Only authorized queries scoped to the requesting user's tenant are returned
4. Decrypted data is held in memory only for the duration of the request



# Security of data in transit

**Network protocol and encryption**

All data transmitted to and from Nucleus is encrypted using industry-standard TLS:

**Nucleus web UI**

Enforces TLS 1.3 or higher for all browser-based communication

**No unencrypted channels**

Nucleus does not support any unencrypted communication paths

**gRPC communications**

All gRPC connections between the web UI and backend, and between devices and backend, use TLS 1.3 or higher

**WebSocket connections**

Printers establish secure WebSocket connections over TLS with mutual authentication using X.509 certificates

**Device authentication and mutual TLS**

Devices authenticate to Nucleus using TLS mutual authentication:

1

On first connection, device presents a unique nonce and tenant ID

2

Backend verifies the nonce and tenant pairing

3

Backend generates a unique X.509 client certificate for the device (RSA-2048 key strength)

4

Device stores the certificate:

- Scanners/Windows Client: Stored securely in Windows Certificate Manager
- Printers: Stored securely in internal printer filesystem alongside other device certificates
- Mobile Devices: Stored securely within the device OS

5

On subsequent connections, device authenticates using the client certificate via TLS mutual authentication handshake

6

Certificates are valid for 3 years and are rotated on a 3-year cycle


**Certificate compromise and recovery**

If a device certificate is compromised, the device must be re-enrolled into Nucleus. The re-enrollment process generates a new unique certificate for the device.

# API security and access control

**User authentication**

Nucleus users authenticate using Zebra's Ping Identity SSO system

Authentication is enforced for all access to the Nucleus web UI

Session-based authentication via the web UI controls access to backend services

**Authorization and access control**

Nucleus implements role-based access control (RBAC) with two primary roles:

| Role | Permissions | Notes |
|---|---|---|
| User | View and manage devices, view fleet status, configure devices, push updates | Cannot manage user accounts |
| Admin | All User permissions plus: add/delete/update user accounts, send user invitations | Full administrative access |

- Access control is enforced at the backend for every gRPC and REST method
- Each API method validates the user's role before executing
- Queries are automatically scoped to return only data from the user's authorized tenant(s)

**API architecture**

- Currently, Nucleus APIs are not public and are accessed only through the web UI
- All API calls are session-authenticated via the web UI
- Future public API access will require additional authentication mechanisms (planned for future releases)

# Security measures and audits

Nucleus maintains a comprehensive security program with continuous monitoring, regular audits, and formal bug bounty testing.

**Internal Security Audits**

While not currently ISO 27001 certified, these audits ensure alignment with international security standards.

**Penetration Testing**

- Internal penetration tests are conducted several times per year
- Nucleus participates in a formal HackerOne bug bounty program
- HackerOne conducts independent security testing and vulnerability research
- Disclosed vulnerabilities follow a documented remediation timeline:
  - Critical Severity: 30 days to remediate
  - High Severity: 60 days to remediate
  - Lower Severity: 90 days to remediate
- To date, HackerOne has not identified any significant vulnerabilities in Nucleus

**Continuous security monitoring**

Nucleus leverages enterprise security tools for continuous threat detection and vulnerability management:

- **CrowdStrike:** Endpoint detection and response (EDR) for infrastructure security
- **Chainguard:** Docker image hardening and container security
- **Endor:** Software Composition Analysis (SCA) with vulnerability scanning
- **Cycode:** Static code analysis and software composition analysis to identify vulnerabilities in application code

These tools provide real-time visibility into security posture and enable rapid identification and remediation of vulnerabilities.

**Disaster recovery and business continuity**

Nucleus maintains a documented Disaster Recovery (DR) plan that is reviewed quarterly and practiced quarterly through disaster recovery drills:

- **Backup Frequency:** Automated backups are performed every 15 minutes
- **Recovery Time Objective (RTO):** Nucleus can be restored to full operation within 6 hours or less
- **Data Retention:** Backups are retained in accordance with the DR plan to enable point-in-time recovery
- **Testing:** DR drills are conducted quarterly to validate recovery procedures and ensure operational readiness

# FAQ

## Hosting and deployment

**Q: In which region is Nucleus hosted and where is the data stored?**

A: Nucleus (including zDNA) is hosted from the US Central region hosted by Google located in Iowa, US.

## Access control and authentication

**Q: Do all users have unique IDs?**

A: Yes. Upon creation of a zebra.com account to utilize in Nucleus, they are given a unique id for their account.

**Q: Are password complexity requirements enforced?**

A: Yes. Here are the Zebra Password Policies The password must have at least 1 of the following characters: ~!@#$%^&*()-_=+[]{}|;:,.<>/? The password must have at least 1 of the following characters: 0123456789 The password must have at least 1 of the following characters: ABCDEFGHIJKLMNOPQRSTUVWXYZ The password must have at least 1 of the following characters: abcdefghijklmnopqrstuvwxyz 6 prior passwords will be maintained in the password history count for a maximum of 365 days The user's account will be locked out after 5 distinct failed password attempts; repeated attempts of the same password are not counted Automatically unlock accounts that were locked by failed password attempts after 1 minute.

**Q: What is the minimum password length?**

A: The password must be between 12 and 255 characters.

**Q: What is the maximum number of days between required password changes?**

A: TBD - put Zebra's Ping SSO policy here?

**Q: What is the password history requirement (how many previous passwords before reuse)?**

A: The password will be checked to make sure it is not the same as the user's current password.

## Certifications and compliance

**Q: Where can I find Zebra's Privacy Policies?**

A: www.zebra.com/about-zebra

**Q: Where can I find Zebra's Regulatory Compliance Information?**

A: www.zebra.com/about-zebra

**Q: Is Nucleus ISO 27001 certified?**

A: Nucleus is not currently ISO 27001 certified. However, Nucleus has been through internal ISO 27001 audits to validate information security controls and practices align with ISO 27001 standards.

**Q: What Windows versions are officially supported?**

A: Zebra officially supports Windows 11 and newer versions for both the Nucleus Client and Nucleus Connector.

**Q: Is Nucleus SOC 2 Type 2 certified?**

A: No, Nucleus does not currently hold SOC 2 Type 2 certification.

**Q: Does Nucleus comply with GDPR?**

A: Nucleus complies with GDPR principles for personal data protection. The personal information Nucleus stores is limited to user-provided account data (first name, last name, email address). The vast majority of data stored in Nucleus is machine-generated device data and telemetry, which is not classified as personal data under GDPR. Nucleus maintains appropriate technical and organizational measures to protect the limited personal data it processes in accordance with GDPR requirements.

**Q: Does Nucleus have other security certifications?**

A: Nucleus does not currently hold FedRAMP, PCI-DSS, or HIPAA certifications. The product is not designed for HIPAA compliance requirements. Security validation is primarily conducted through the internal audit program, HackerOne bug bounty testing, and continuous monitoring with enterprise security tools.

**Q: What is Nucleus's data residency policy?**

A: All Nucleus customer data is stored in Google Cloud's us-central region (Iowa, United States). Currently, Nucleus does not support alternative regional data residency.

# Conclusion

In today's rapidly evolving threat landscape, managing large-scale device fleets presents significant security and operational challenges. Nucleus addresses these challenges with a comprehensive, cloud-native solution that combines powerful fleet management capabilities with enterprise-grade security controls. Nucleus protects your most valuable assets—your device infrastructure and business data—through multiple layers of defense:

- **Data Security:** All data is encrypted at rest using AES-256 and in transit using TLS 1.3, ensuring confidentiality across the entire system
- **Secure Device Authentication:** Devices authenticate using cryptographic certificates with mutual TLS authentication, preventing unauthorized access and device spoofing
- **Strict Multi-Tenancy:** Complete data isolation ensures organizations never see each other's devices or configurations
- **Continuous Security Monitoring:** Automated security tools and regular penetration testing identify and remediate vulnerabilities before they can be exploited
- **Formal Bug Bounty Program:** HackerOne white hat testing provides independent security validation and rapid response to discovered issues
- **Business Continuity:** Automated 15-minute backups and a proven disaster recovery plan ensure your fleet management can be restored within 6 hours

Whether you manage 5 devices or 10,000+ devices across multiple regions, Nucleus provides the visibility, control, and security your organization requires to optimize your Zebra device fleet while protecting critical business data. By adopting Nucleus, you gain a trusted partner in device fleet management—one that understands the importance of security, reliability, and operational excellence.

For more information about Nucleus security, deployments, or to discuss your specific security requirements:

**Zebra Technologies | inquiry4@zebra.com | +1 800 423 0442**

**Visit zebra.com to learn more.**

ZEBRA