EDWARDS

Cybersecurity Protocols & Processes

Comprehensive Fire & Life Safety

UPGRADE YOUR DATA PROTECTION

For Fire & Life Safety, system and operational security is integral. That's why the credentialed experts at Edwards protect your data while it is in transit and at rest. Our certificate-based protection of data in transit uses Secure Socket Layer/ Transport Layer Security (SSL/TLS) alongside client-side encryption.

TWO POSSIBILITIES FOR ENCRYPTION

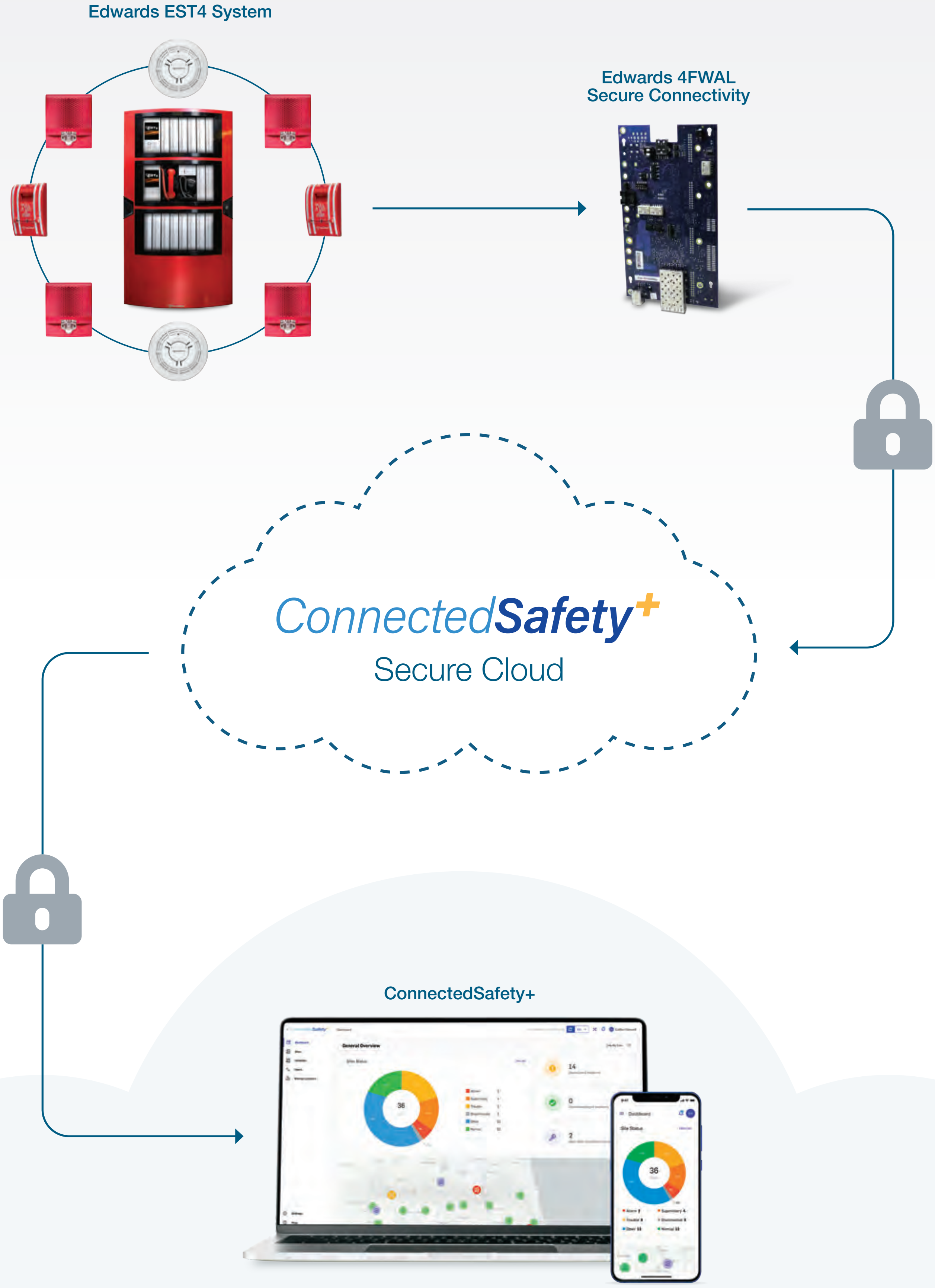
CLIENT-SIDE ENCRYPTION

You encrypt your data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, encryption keys, and any related tools.

SERVER-SIDE ENCRYPTION

Amazon S3 encrypts your objects before saving them on disks in AWS data and then decrypts the objects when you download them using AES-256 encryption.

CONNECTEDSAFETY+ NETWORK TOPOLOGY



Edwards EST4 System

Edwards 4FWAL Secure Connectivity

ConnectedSafety+ Secure Cloud

ConnectedSafety+

DATA COMMUNICATION WITHIN THE CLOUD

All internal communications between various cloud services use HTTPS for integrity and confidentiality within the cloud. Communications between mobile and cloud platforms are over HTTPS with a TLS 1.3 encrypted tunnel. In addition, the firewall in perimeter security is ensured through IPS/IDS and packet inspection.

COMPATIBLE AMAZON WEB SERVICES (AWS)

powered by
aws

AWS SOC 1 Report
available to AWS customers from AWS Artifact

AWS SOC 2 Privacy
Type II Report – available to AWS customers from AWS Artifact

AWS SOC 2 Security
Availability & Confidentiality Report, available to AWS customers from AWS Artifact

AWS SOC 3 Security, Availability and Confidentiality Report
publicly available as a whitepaper.

This is in accordance with the AWS shared responsibility model which can be found here https://aws.amazon.com/compliance/shared-responsibility-model/.

PARTNERS IN ENHANCED CYBERSECURITY

To further reduce risks and ensure optimal outcomes, Edwards utilizes Okta for login, credentials, and role-based authentication for web and mobile applications. Okta's data protection meets the highest industry standards, complying with FedRAMP and NIST SP 800-53, ISO 27001/27017/27018 and GDPR requirements.

COMPATIBLE CLASSES OF CYBERSECURITY TOOLS

SECURITY REQUIREMENTS

Captures security requirements during the secure SDLC process and meets industry compliance frameworks.

THREAT MODELING (TM)

Identifies threats early in the design using TM activity during security architecture review.

STATIC APPLICATION SECURITY TESTING

Analyzes source code during static application testing using industry standard tools.

SOFTWARE COMPOSITION ANALYSIS

Identifies open-source security and license risks in open-source solutions.

DYNAMIC APPLICATION SECURITY TESTING

Detects conditions indicative of a security vulnerability in an application in its running state to identify security weaknesses and vulnerabilities.

PENETRATION TESTING

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network.

CUSTOMIZABLE SOLUTIONS THROUGH A DEDICATED PARTNER NETWORK.

No one knows your facility better than you, which is why you need a partner you can count on to provide the best in fire and life safety solutions for your unique application. Edwards' network of partners—the people we entrust with our technology—provide unrivaled system design, service and know-how to deliver solutions that meet stringent life safety requirements. And they're ready to do the same for you.

See what's possible for your facility. Contact your Edwards Partner today.

For inquiries regarding Edwards Professional Services & Solutions, contact Edwards.PSS@carrier.com.

UL CERTIFIED
SAFETY
SIGNALING
US
E12345

Helps Reduce Cooking Nuisance Alarms

UL 268 7th Ed.

LISTING
STATE OF CALIFORNIA
STATE FIRE MARSHAL
SERVICE

FM
APPROVED

EDWARDS

LIFE SAFETY & INCIDENT MANAGEMENT

edwards.fire@carrier.com
edwardsfiresafety.com

8985 Town Center Parkway
Bradenton, FL 34202