GALLAGHER Security

The Controller 7000

The platform with cybersecurity at its heart



The Controller 7000

The platform with cybersecurity at its heart

The need to merge cyber and physical security **2**

Introducing the Controller 7000 Platform **3**

A brief history of the Controller 7000 Platform **4**

Hardware embedded with security **5**

- NXP i.MX 8X System-on-Chip 5
- NXP Edgelock Secure Element 5
- Arm TrustZone 6
- Secure Boot 6
- Anti-Rollback 7
- Immutable Identity 7

Software designed for the future **8**

- Trusted Execution Environment 8
- Firmware Protection 9
- Data Protection 10
- Strong Cryptographic Protection 10

Production with security from the start **11**

- Controller Hardware Production 11
- Controller Firmware Production 12

Cybersecurity is a continuous journey **13**



The need to merge cyber and physical security

As cyber-physical attacks grow in number and complexity, organizations everywhere are forced to reassess the cybersecurity preparedness of their physical security systems. Protections that were cutting-edge ten years ago have been surpassed by new technologies, even in cases where hardware continues to function smoothly.

As such, physical security systems must begin transitioning to a similar maintenance approach as IT systems, with cybersecurity at the heart. Examples include:

Communication protection

Prevents data transfers from being visible to, or intercepted by, unauthorized parties and uses techniques such as cryptography.

Data protection

Prevents secret data stored inside devices from being accessed by unauthorized parties.

Firmware protection

Prevents on-chip firmware from being reverse engineered.

Operation protection

Prevents critical operations from malicious intentional failure.

Tamper protection

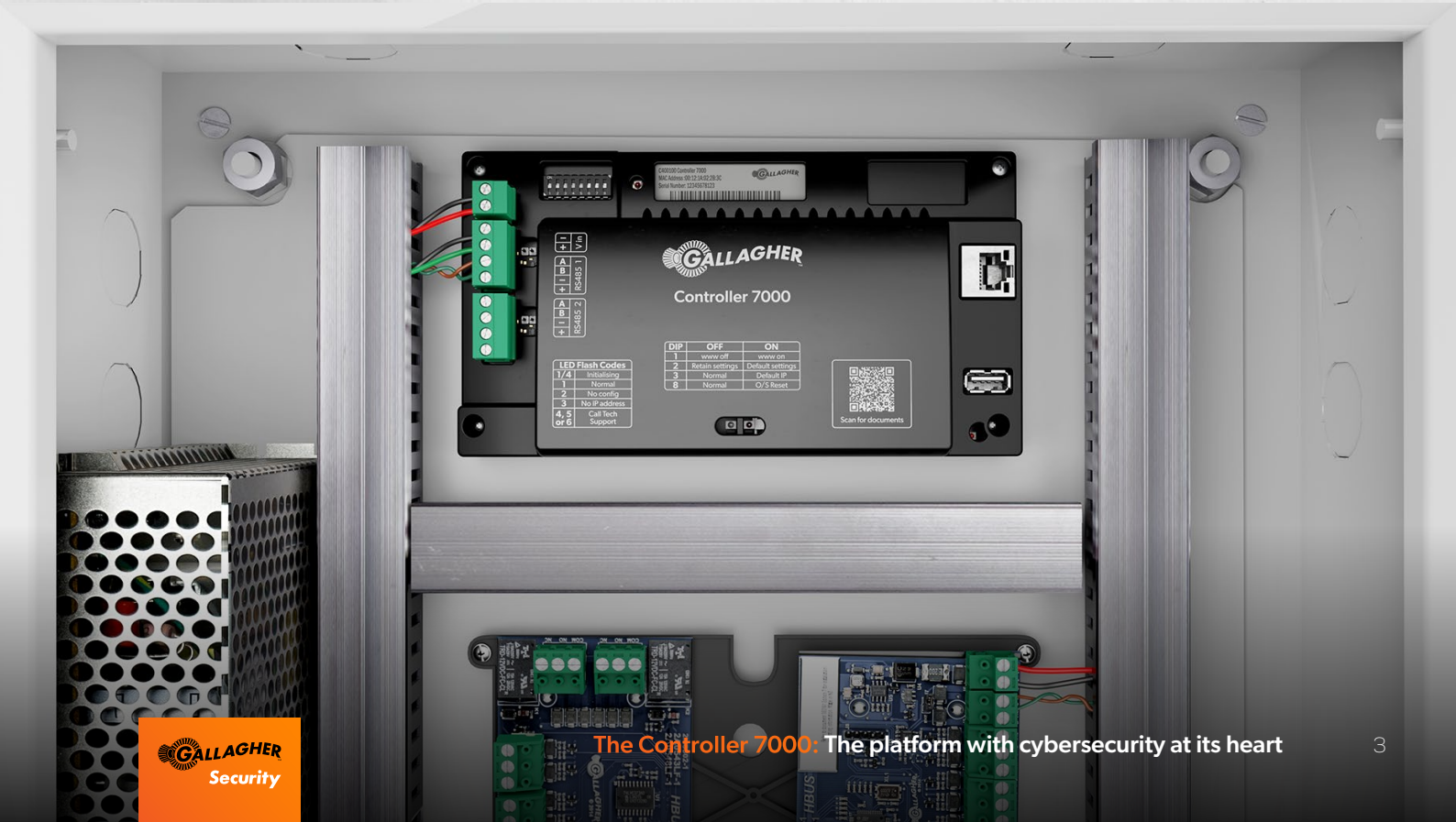
In many security-sensitive products, anti-tampering features are needed to prevent the device's operation or protection mechanisms from being overridden.

Authenticity Protection

Prevents substitution of malicious firmware or hardware by using cryptographically strong device authentication.

Introducing the Controller 7000 Platform

Gallagher Security's answer to the need for convergence of physical and cyber protections comes in the form of the Controller 7000 Platform, a new generation of controllers built with cybersecurity from the inside out. The following white paper details the cyber protections of the Controller 7000, demonstrating its cybersecurity capabilities and differentiating it among other controllers on the market.





A brief history of the Controller 7000 Platform

In early 2023, Gallagher Security launched the first products of the new Controller 7000 generation, the Controller 7000 Single Door (C7000 SD). A networked security controller that offers full support for Gallagher's distributed control architecture, the C7000 SD featured a new security architecture designed to provide the highest level of protection against cyber threats and introduced Power over Ethernet (PoE) capabilities.

Expanding on that foundation, the Controller 7000 Platform introduces a Standard variant, Enhanced variant and High Security variant, designed from the ground up with cybersecurity at its core, featuring:

- Cutting-edge, cybersecure hardware components
- Software features that are designed to keep controller firmware safe from attack
- A secure, end-to-end production model designed to be resilient to supply chain attacks

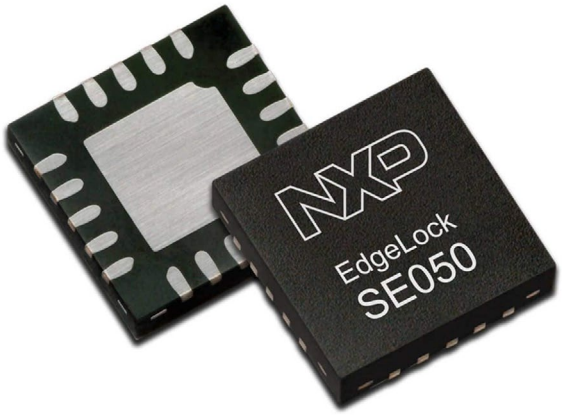
The result is a new line of controllers built with layered cybersecurity protections designed to safeguard against threats into the future.

Hardware embedded with security

Secure products are built on secure platforms, and secure platforms are built on top of hardware technology that integrates security features at the silicon level.

The Controller 7000 Platform is built around two such devices:





NXP i.MX 8X System-on-Chip

i.MX 8X is an advanced and modern system-on-chip that integrates Arm Cortex-A application cores, a Cortex-M microcontroller for real-time processing, and a system security controller all within one package.

i.MX 8X provides the Controller 7000 Platform with critical security features baked into the hardware, including Arm TrustZone, secure boot with anti-rollback capability, immutable device identity, hardware root-of-trust, and lifecycle state.

NXP Edgelock Secure Element

NXP Edgelock is a hardware cryptographic engine and key store. It provides the Controller 7000 Platform with storage for the line's most critical keys and implements the crypto algorithms that operate on those keys. The platform's critical keys never leave the device. Edgelock contains hardware protections that detect and prevent tampering; the Controller 7000 Platform also encrypts all communication to the chip, which prevents eavesdropping.

Arm TrustZone

Arm TrustZone is a technology that provides hardware-enforced isolation between two "worlds" built into the CPU: a secure world and a normal world.

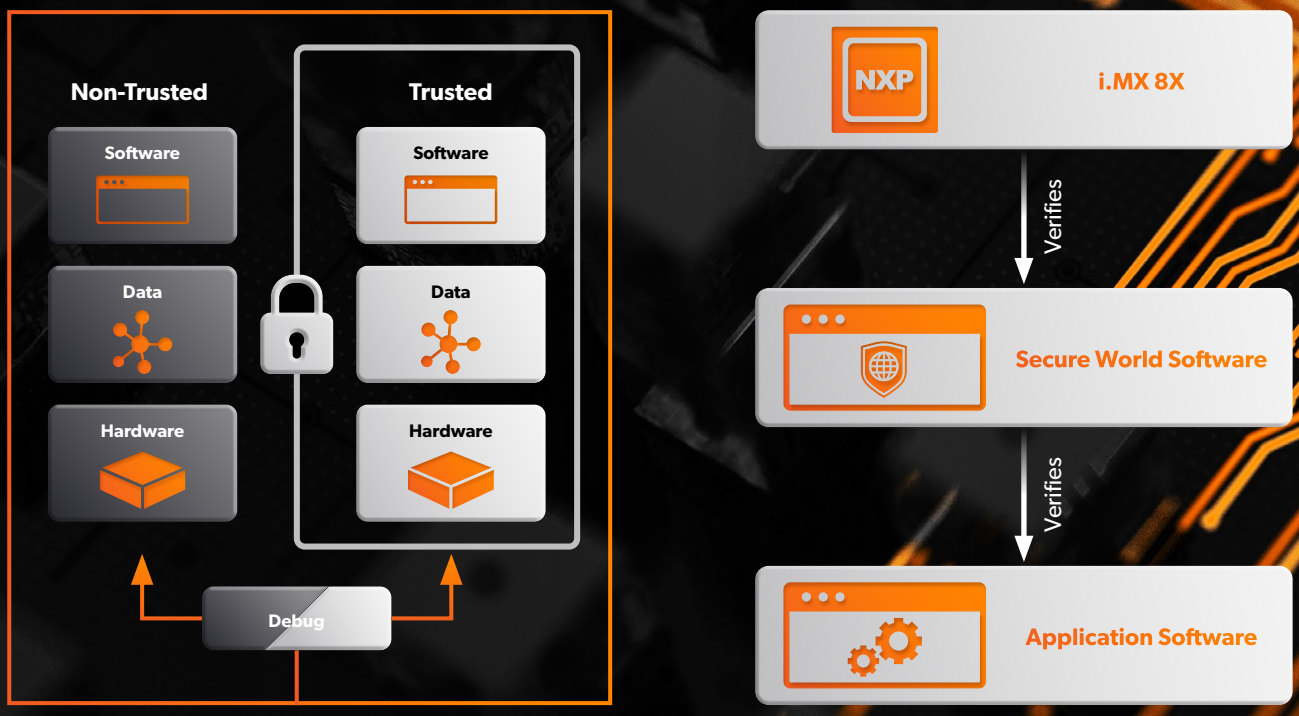
The secure world contains the most security-critical code, cryptographic keys, and hardware resources. These are isolated in hardware in such a way that any exploits found in normal application software (running within the normal world) cannot access or expose those critical secrets.

The Controller 7000 Platform is built on TrustZone as a foundational technology. It is used to isolate code, keys, and resources related to the Controller's identity, trust, boot security, and data, communications, and firmware protections. Previous generations of processor chips were not capable of similar hardware enforced protection.

Secure Boot

Trust of a hardware platform is built on trust for the firmware that runs on that platform. The best place to enforce this trust is at the very beginning of platform startup – at system boot.

The Controller 7000 Platform uses the boot security features of the i.MX 8X to enforce its firmware policies and is configured to boot only authentic and quality-controlled Gallagher code. The i.MX processor is configured with these boot policies during factory production, at the hardware level. The Controller 7000 Platform can therefore provide high assurance that its running firmware is Gallagher-authentic and free from malware. This is critical for preventing attacks on the firmware, both while the controller is in the supply chain and after it has been installed on a site.



Anti-Rollback

Anti-rollback is closely related to secure boot: it's the ability to permanently prevent software with discovered vulnerabilities from ever again running on the device.

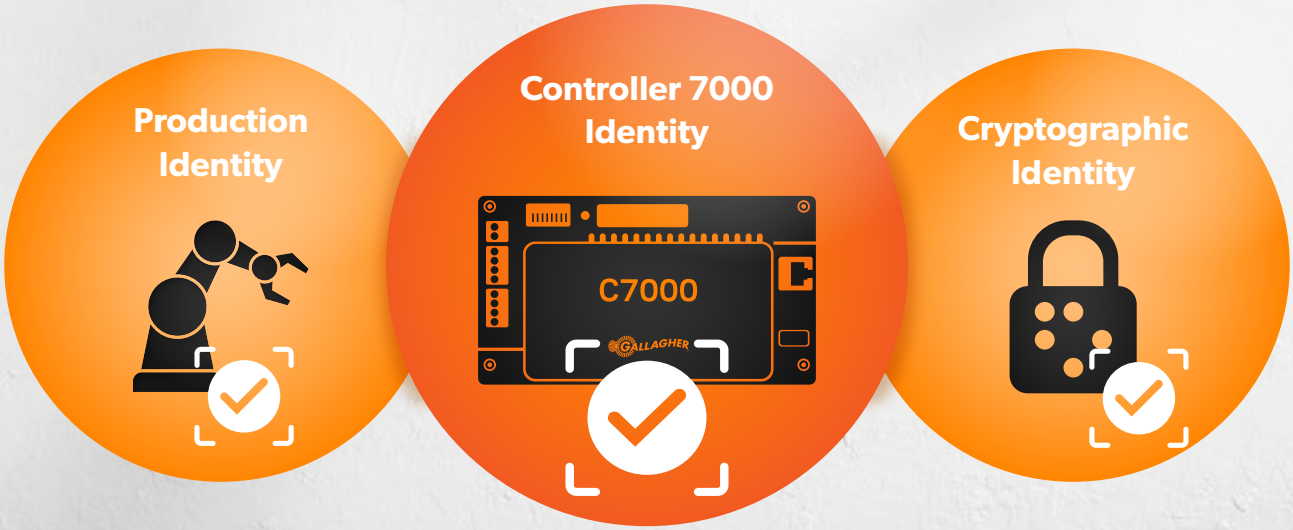
One attack vector for secure hardware is to trick administrators into installing old versions of software – with known vulnerabilities that were discovered after release – back onto their hardware, making that hardware susceptible to attack. The Controller 7000 Platform uses hardware features within the i.MX 8Xi. MX 8X to permanently disable the ability to boot old versions of code with discovered vulnerabilities.

Immutable Identity

Secure controllers rely on having strong and unchangeable unique identities built into their hardware.

A secure identity consists of both the manufactured identifiers – including the serial number – as well as the cryptographic keys that are used to attest to that identity. A secure identity is essential for preventing counterfeiting or cloning of authentic Gallagher hardware, which can lead to security attacks on installed sites, or business damage via inauthentic but compatible copycat hardware.

The Controller 7000 Platform uses hardware features of both the i.MX 8X and the Edgelock secure element to permanently assign production and cryptographic identities into the controller in such a way that the identity cannot be leaked or altered after production.



Software designed for the future

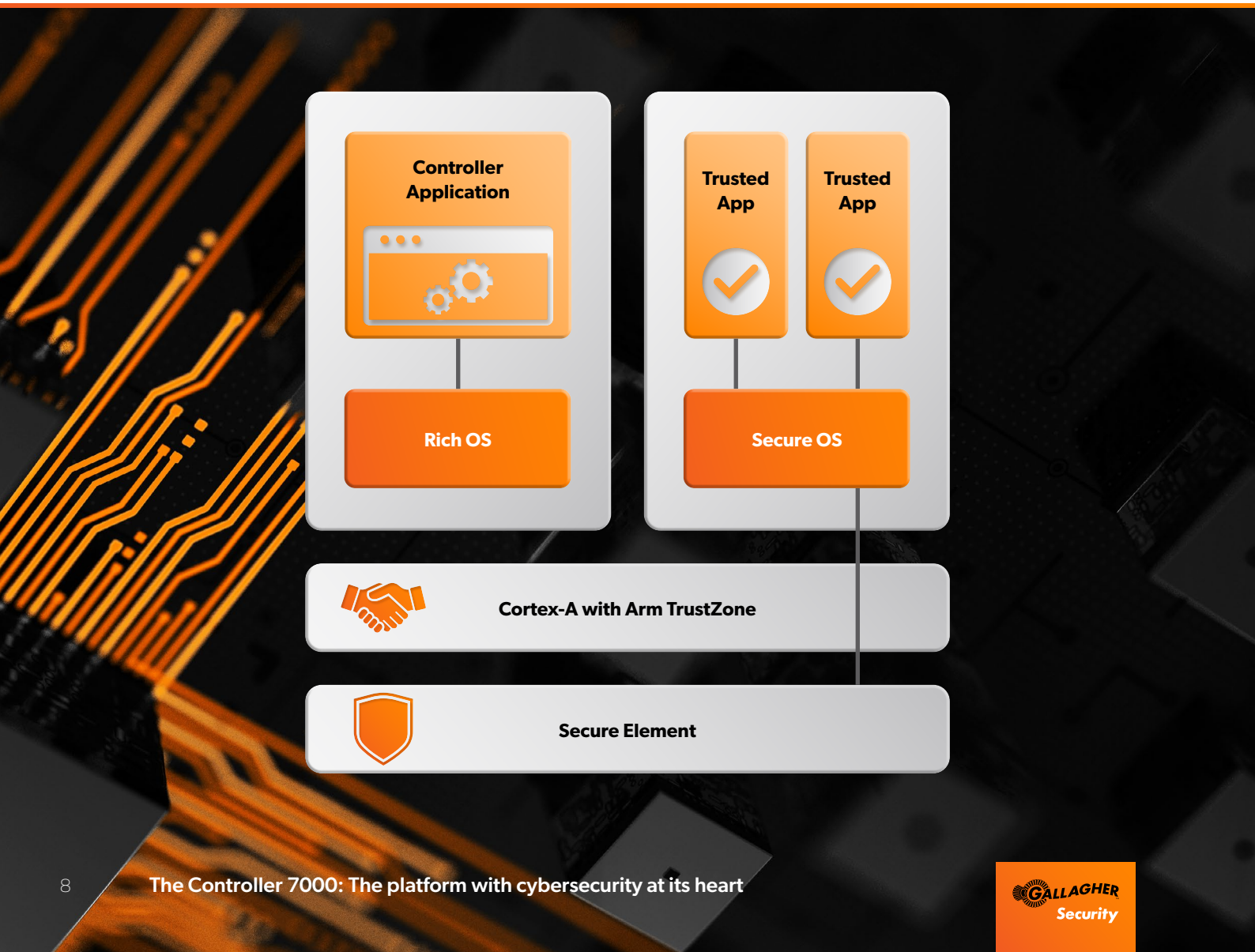
Secure platforms run trusted and authentic software that is architected for security. That means protecting data travelling through communication channels and data at rest on the controller itself. And that software uses only industry-standard, strong cryptography for providing these protections.

The Controller 7000 Platform firmware is architected for security from the ground up.

Trusted Execution Environment

The Controller 7000 Platform uses a small, separate, and secure operating system within a Trusted Execution Environment (TEE) to protect, store, and process security-sensitive data. The TEE runs on top of the hardware features provided by Arm TrustZone; only the TEE has access to critical device secrets.

This software architecture helps isolate critical cryptographic keys, keeping them safe. This reduces the impact of any security vulnerabilities that may be discovered and attacked in the main application or operating system. Attacks are more likely to be contained, not exposing secrets that could compromise a whole site.



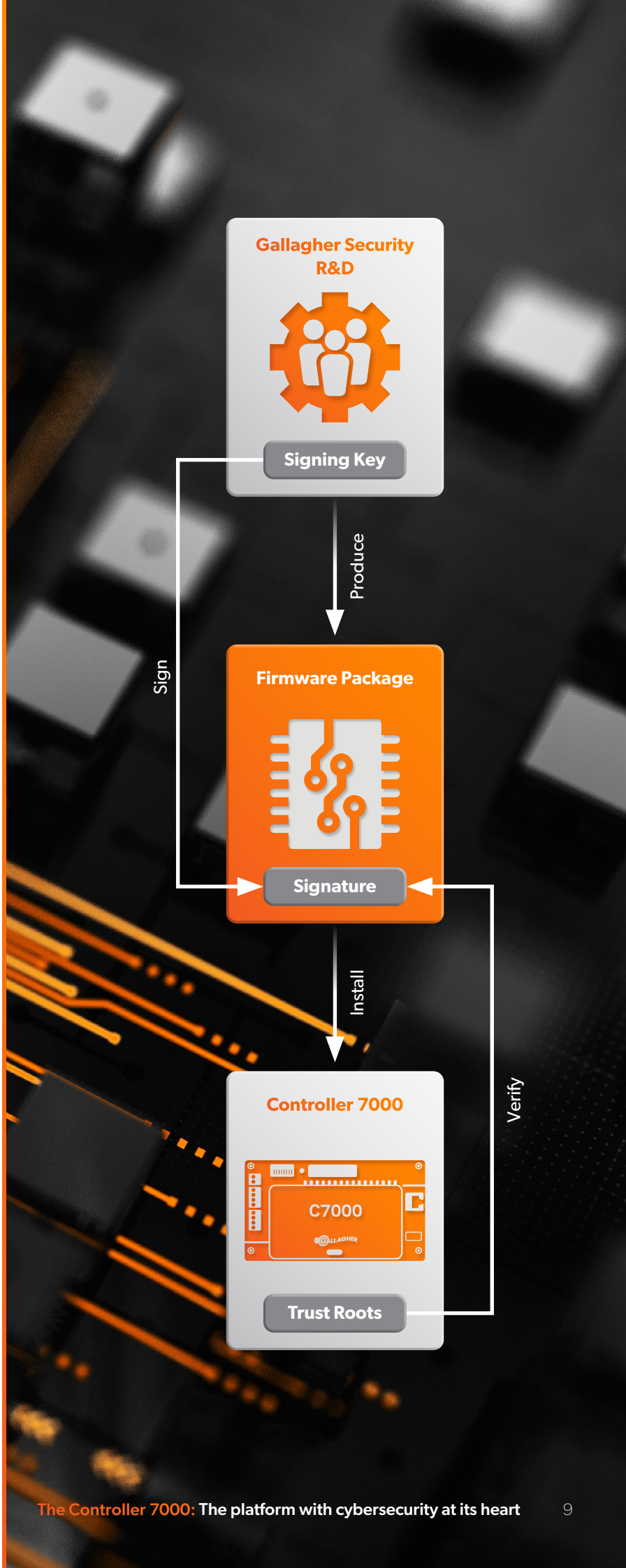
Firmware Protection

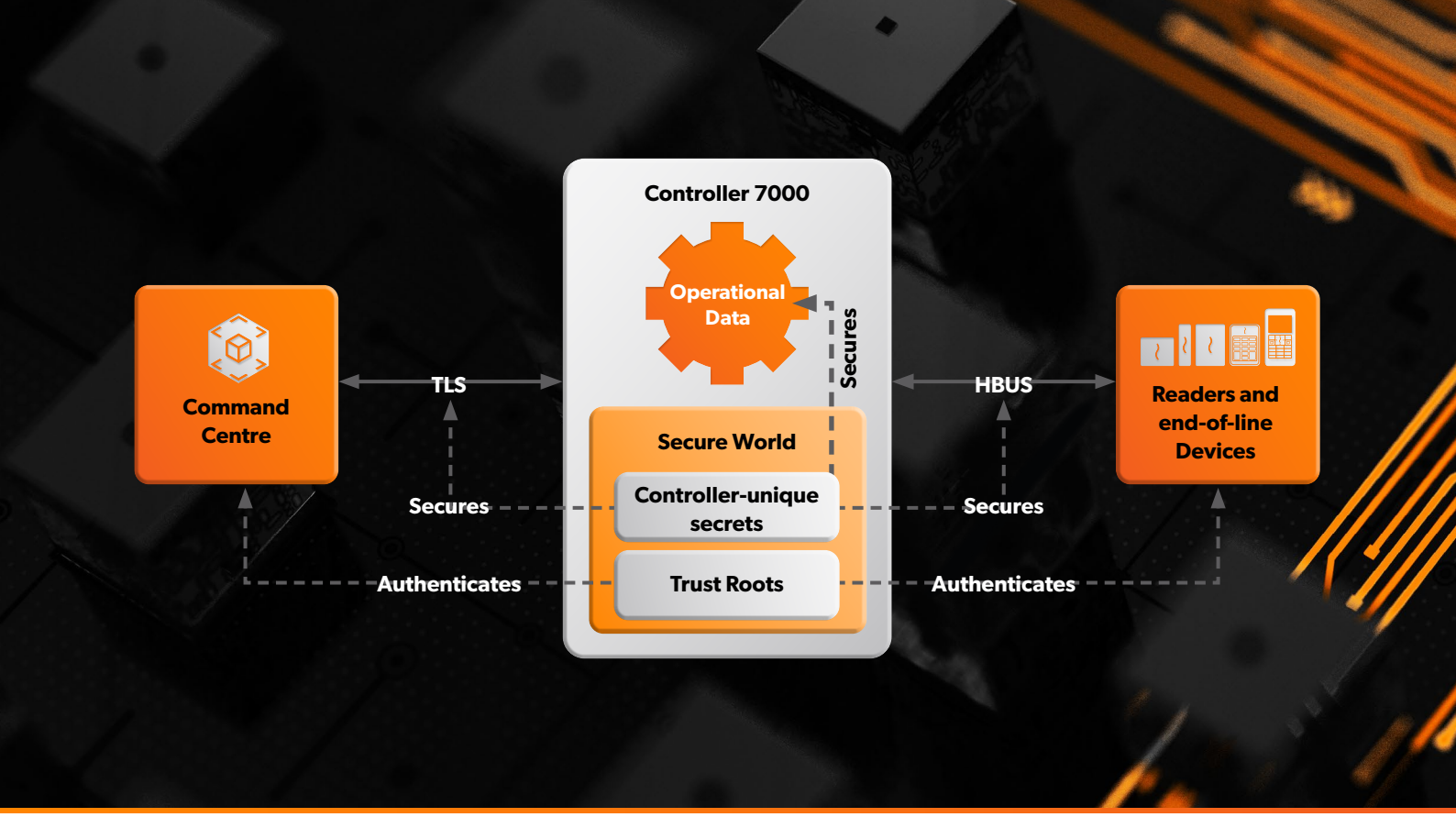
A controller is only as secure as the firmware allowed to run on the device. Gallagher uses cryptographically strong signature algorithms and tightly controlled signing keys to ensure that only authentic software can ever run on the device.

The Controller 7000 Platform then uses embedded trust roots protected within the secure element to validate what is allowed to be installed onto the device. The same sort of validation happens at an even finer-grained level when the device is booted.

Every piece of software that runs on the Controller 7000 Platform is protected in this way.

This firmware production, update, and installation system ensures that software is authentically Gallagher in origin, untampered during transit, and resists attacks even after it has been installed on the device.





Data Protection

The Controller 7000 Platform uses trust roots embedded within its secure world hardware to authenticate the server, peer controllers, and bus devices that it communicates with. After the device is authenticated, the platform generates and stores unique keys that are then used to protect all communications to that device.

Communication keys are therefore isolated and strongly protected. Data in transit is encrypted and authenticated and resists eavesdropping or man-in-the-middle attacks.

Data at rest stored on the controller itself is likewise protected by unique keys isolated within the secure world. Sensitive data residing on the controller, such as Personal Identifiable Information (PII) and User Codes, are encrypted to prevent sensitive data leakage.

Strong Cryptographic Protection

Controller 7000 Platform has sought to standardize on the NSA's Commercial National Security Algorithm (CNSA) suite for all core and new protections wherever possible. The CNSA suite is listed as appropriate for protecting data up to Top Secret classification.

The CNSA suite specifies the following:

Purpose	Algorithm	Strength
Key establishment	ECDH	p-384
Symmetric block cipher	AES	256
Digital signatures	ECDSA	p-384
Digests	SHA	384

Production with security from the start

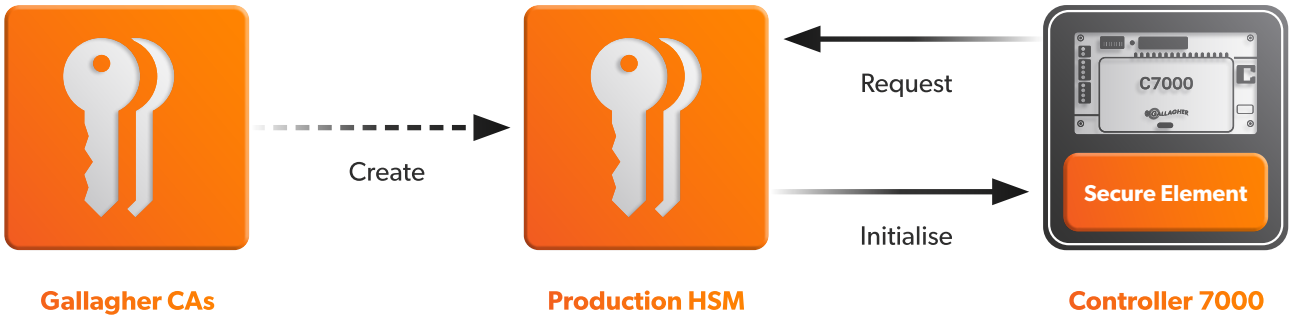
Along with the Controller 7000 Platform, Gallagher is introducing cutting edge security processes for controller and firmware production.

Controller Hardware Production

Gallagher reviewed best practice security infrastructure when designing the generation, processing, and storage of cryptographic key and certificates for the Controller 7000 Platform. The result is a production system that delivers strong assurance of platform quality and authenticity.

The production system directly uses security features of the i.MX 8X and Edgelock hardware – such as lifecycle state, security state, cryptographic root of trust, boot mode, and secure boot fuses – to completely configure and then lock down the security state of the platform during production initialization. This critical phase of production brings together the platform's hardware security with the high-end production infrastructure and access and auditing controls.

The resulting controller hardware that leaves production is secured and resistant to tamper attacks in the supply chain or once installed. This is an intentional approach to platform security that covers the whole lifecycle of the product.





Controller Firmware Production

The same new cutting-edge infrastructure and strong process controls are now applied to the job of firmware production and update releases for the Controller 7000 Platform.

Gallagher Security has introduced new release controls on controller firmware which are designed to assure the quality and authenticity of the code distributed to customers. The only firmware that can run on customer hardware is firmware that has first passed all quality assurance, documentation, and release controls.

This production infrastructure also introduces redundancy and disaster recovery procedures that better fortify Gallagher against security challenges.



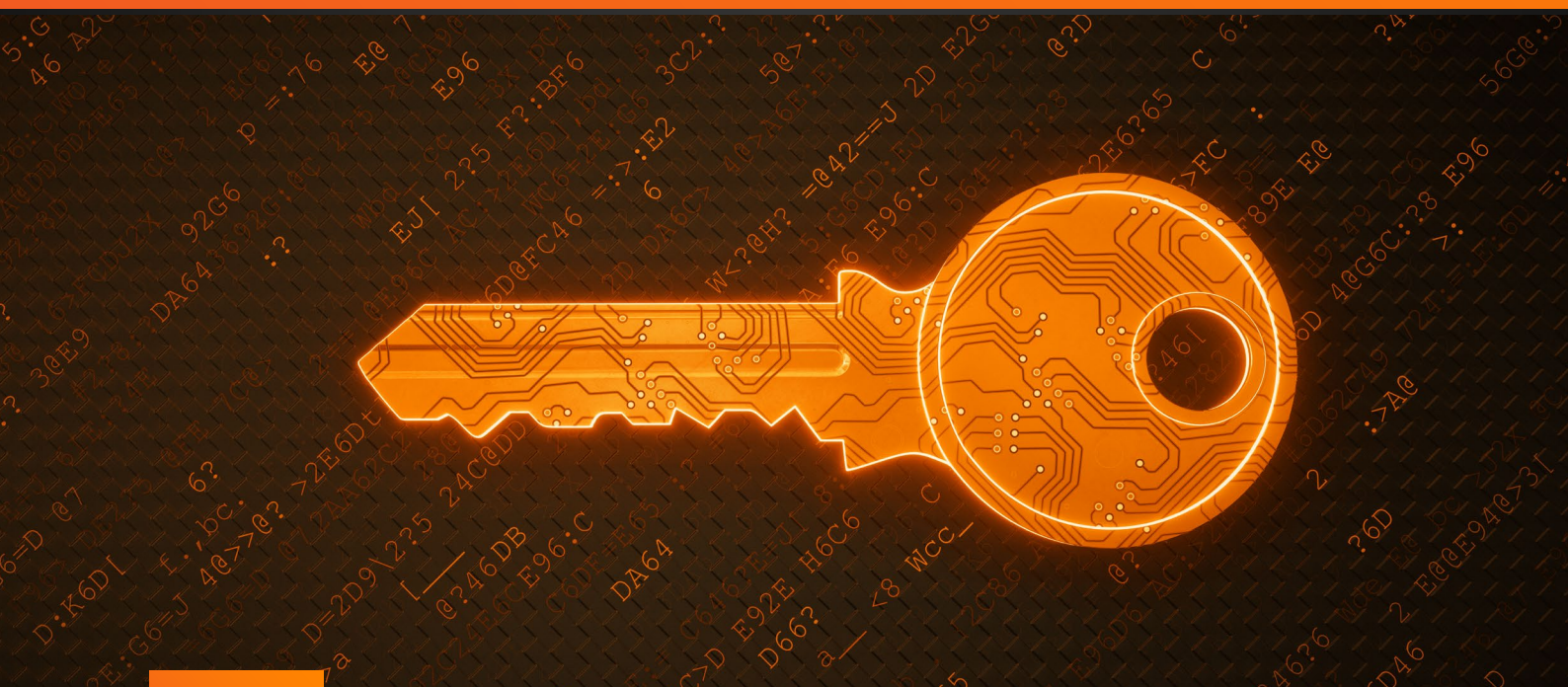
Cybersecurity is a continuous journey

As businesses become increasingly dependent on technology and data, the need to maintain a robust cybersecurity posture has never been more critical.

However, the reality of this challenge is clear: keeping up with cybersecurity is a relentless battle that must be confronted head on. By acknowledging that cybersecurity is not a destination, but rather a continuous journey, businesses can proactively address the threats that evolve alongside the digital landscape to secure the future of their people, data, and assets.

Gallagher Security upgrades our controller security over time to keep ahead of cybersecurity threats; these security improvements are available to customers with Software Maintenance agreements.

Upgrading hardware and software to reinforce cybersecurity measures empowers businesses around the world to protect their investments well into the future, which is ultimately the goal of the Controller 7000 Platform.





security.gallagher.com

Gallagher World Headquarters

181 Kahikatea Drive, Melville, Hamilton 3204
New Zealand

Phone +64 7 838 9800
Email security@gallagher.com