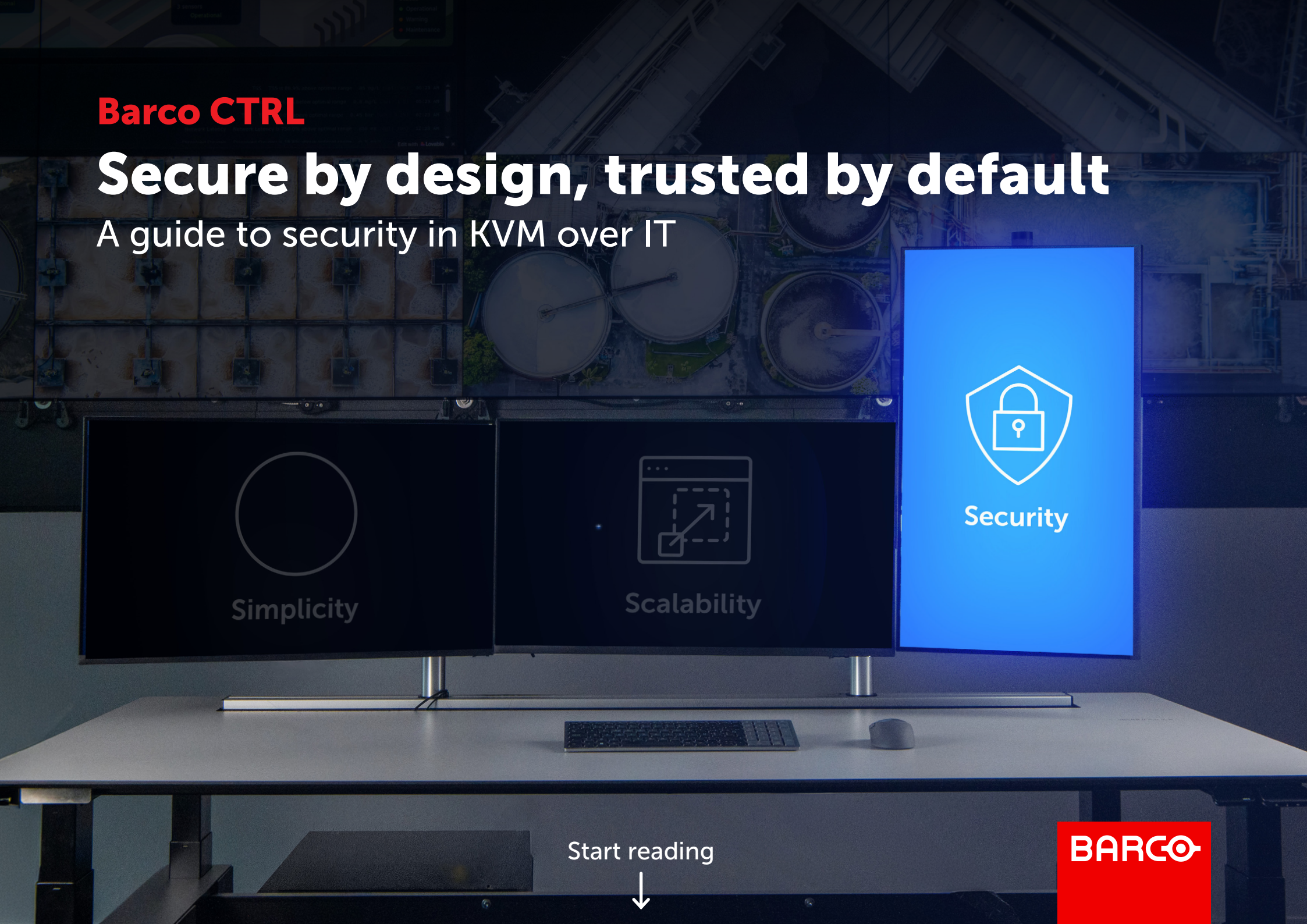
Barco CTRL

Secure by design, trusted by default

A guide to security in KVM over IT



Start reading

↓

Security is the foundation, not a feature

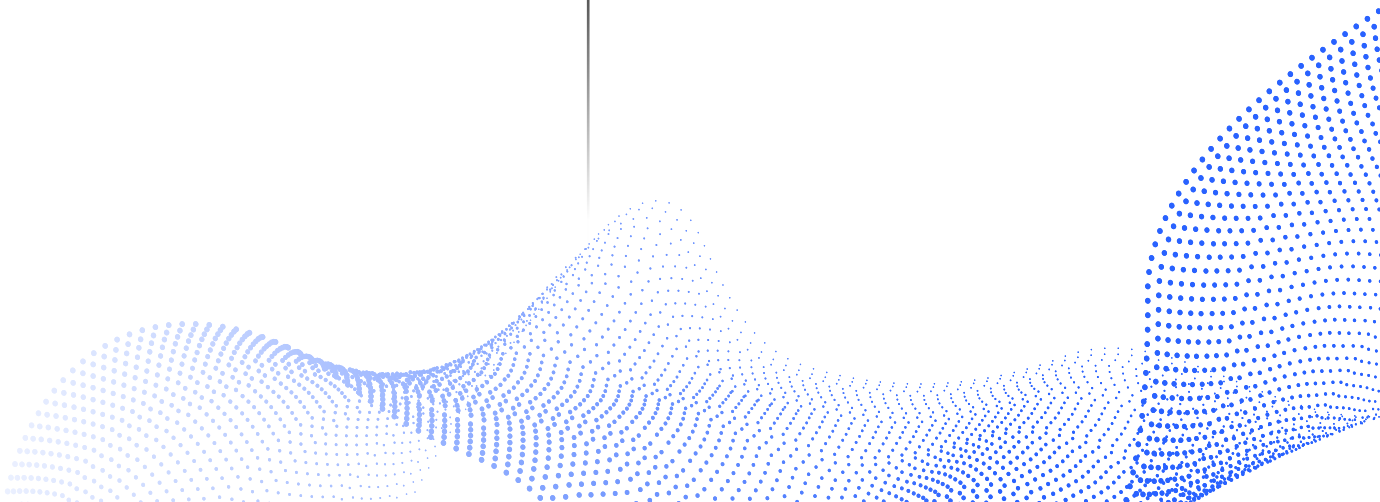
Control rooms sit at the center of critical operations. Power grids, transportation networks, emergency response systems, oil and gas infrastructure, ... the decisions made in these rooms have real consequences for real people. That makes them an attractive target for anyone who wants to cause disruption.

Cybersecurity in control rooms has never been more important and the stakes have never been higher. New regulations can hold executives personally accountable for security failures. Threat actors are growing more sophisticated. And the convergence of IT and operational technology means that hardware that has always operated on a digital island is suddenly connected to the outside world, which creates new attack surfaces its design never considered to address.

Barco CTRL was built for exactly this environment. **As a KVM over IT platform, security is not an add-on or an afterthought. It is the foundation on which every other capability rests.** Designed from scratch following Security by Design principles, and supported by a dedicated in-house security team, Barco CTRL gives organizations the confidence to connect their critical operations to the networks they need – without opening the door to threats they cannot afford.

This e-book explores 12 ways in which Barco CTRL approaches security, from the architecture of the platform itself to the regulatory landscape it helps organizations navigate.

Content



Part 1
Security by design

1. Security by design and Zero Trust

Most security approaches start with a product and add security to it afterward. Barco CTRL started the other way around. **From the very first design decision, security was the foundation – not a layer to be applied on top, but the principle that shaped every architectural choice.**

This Security by Design approach is complemented by a Zero Trust architecture. In a Zero Trust model, nothing is assumed to be safe by default: not a device, not a user, not a network connection. Every access request is authenticated and authorized, every communication channel is verified. This is especially important in control room environments, where the consequences of a successful intrusion can extend far beyond the IT system itself.

Additional best practices, including the Shift Left methodology – which embeds security testing early in the development process rather than at the end – ensure that vulnerabilities are identified and addressed before they can ever reach a deployed system.

The result is a platform that does not just claim to be secure, but is built to be.

2. The 5 pillars of Barco CTRL security

The security architecture of Barco CTRL is built around five clearly defined pillars, each addressing a distinct layer of the system. Together, these five pillars form a defense-in-depth strategy with no gaps.

1

Identity management ensures that only authorized users and devices can access the system, using robust authentication mechanisms including multi-factor authentication (MFA) and attribute-based access controls (ABAC).

2

Communication protection encrypts all data in transit using TLS 1.2 and 1.3 and mTLS, with certificate-based authentication ensuring that every connection is legitimate.

3

System protection covers the full lifecycle of the platform – from secure boot processes that prevent unauthorized software from loading to encrypted storage and rigorous update management.

4

Audit logging creates comprehensive, tamper-evident records of all system activity – logins, configuration changes, data access – providing the accountability trail that both internal governance and external regulations require.

5

Media protection ensures that content is encrypted and access-controlled at the device level, preventing data from being extracted even if a physical device is compromised.

3. No open doors

One of the most common attack vectors in any networked system is the endpoint – the individual device that connects users to the network. Open, general-purpose computers are particularly vulnerable: they can run unauthorized software, accept unknown USB devices, and be compromised by users who install applications outside the approved environment.

Barco CTRL addresses this by using a dedicated appliance model.
The decoders and encoders that make up the CTRL hardware are purpose-built, locked-down devices that run only Barco-signed software. Boot settings are inaccessible to users, unauthorized software cannot be installed, and the risk of a compromised endpoint introducing malware into the system is eliminated by design.

This approach is particularly effective against insider threats, one of the most underestimated risks in critical infrastructure environments. When the hardware itself prevents unauthorized access at the device level, the attack surface shrinks dramatically. The appliance model is therefore not just a hardware choice, but a security strategy.

4. Secure by default

A system that is secure by design but requires extensive configuration to activate that security is only as safe as the person who configures it. Human error in security setup is one of the most common causes of vulnerabilities in deployed systems – a missed setting, a default password left unchanged, an unnecessary port left open.

Barco CTRL is secure by default. This means that **when the system is deployed, it is already in its most secure state without requiring any additional security configuration from the installer.** Unnecessary services are disabled, default credentials are not used, and all communication channels are encrypted from the moment the system comes online.

This approach removes a significant source of risk from the deployment process and ensures that every Barco CTRL installation – regardless of the technical expertise of the installer – starts from the same strong security baseline. When needed, the user can choose to loosen the security a bit, for example to integrate legacy systems. The awareness however makes a big difference.

Security that depends on correct configuration is security that can fail. Security that is built into the default state is security that simply works.

Part 2

Security in operation

5. Patch management made effortless

Delayed patching is one of the most common and most preventable causes of security breaches in critical infrastructure. Organizations know they need to stay current, but the practical challenges of updating complex systems in 24/7 environments – downtime, manual processes, the fear of operational disruption – create friction that leads to dangerous delays. Some organizations update their systems only once a year, running year-old vulnerabilities in environments that demand the highest security standards.

Barco CTRL removes that friction entirely. **Security patches and system updates can be rolled out automatically across the entire installation from a central location**, reaching every device in the network in a single action. The process typically takes no longer than a coffee break, with minimal system downtime. No USB drives, no manual visits to individual hardware components, no extended maintenance windows.

This transforms patch management from a source of organizational anxiety into a routine operational task. By eliminating the practical barriers to timely updates, Barco CTRL removes the main reason organizations give for running outdated software – and in doing so, closes one of the most exploited gaps in control room security.

6. The dedicated Barco security team

Security is only as strong as the people behind it. Many technology vendors treat product security as a compliance function – a team that reviews things before release and signs off on certifications. Barco takes a fundamentally different approach.

The Barco Control Rooms division has product security engineers, product security architects, and security champions embedded directly in every development team. Security is not reviewed at the end of the development process, but is present at every step of it. Weekly security meetings ensure that vulnerabilities are identified and remediation approaches are defined before they can reach a deployed system.

This philosophy extends beyond internal development. Barco's security team engages regularly with partners and customers on complex security questions that go beyond standard sales conversations – providing the kind of expert guidance that organizations need when navigating genuinely difficult security challenges in critical infrastructure environments. Security expertise, in other words, is part of the product.

Staying current is built into the platform, not bolted on.

7. A dedicated security roadmap

Cybersecurity is not a destination. Threat actors evolve, regulations change, and vulnerabilities are discovered in systems that were considered secure yesterday. A platform without a forward-looking security commitment is a platform that will eventually fall behind.

Barco CTRL has a dedicated security roadmap that ensures the platform stays at the forefront of cybersecurity over its entire lifecycle. This includes regular penetration testing conducted by independent experts, ISO 27001 certification, and a proactive vulnerability management process that addresses issues before they can be exploited.

The roadmap also responds to the evolving regulatory landscape. As new requirements come into effect – from NIS2 and NERC-CIP to the EU Cyber Resilience Act – Barco works to ensure that CTRL deployments meet or exceed the emerging standards.

8. Operational continuity as a security feature

Security and availability are often treated as separate concerns. In reality, they are deeply connected. A system that goes down – whether due to a cyberattack, a hardware failure, or a botched update – creates exactly the kind of chaotic, high-pressure environment in which security mistakes are most likely to happen. Keeping the system running is itself a security measure.

Barco CTRL is built with server redundancy. If this hardware component fails, a spare takes over automatically without operator intervention. On the software side, all services run in isolated containers on the server – if one service malfunctions, it cannot take down the rest of the system. The same isolation applies at the decoder level, where a single source issue cannot affect the broader hardware device.

This architecture means that even in the unlikely event of a partial failure, the control room continues to operate. Operators remain in control, decisions continue to be made, and the security posture of the system is maintained throughout.

Resilience and security, in Barco CTRL, are two sides of the same design principle.

Part 3

Security in context

9. IT-OT convergence

Control rooms stand at a unique crossroads. On one side is the IT world – progressive, connected, comfortable with frequent updates and rapid change. On the other is the OT world – conservative by necessity, where stability is paramount and downtime can have catastrophic consequences. These two worlds have fundamentally different relationships with security, and bringing them together without compromising either is one of the defining challenges of modern critical infrastructure.

As a KVM over IT platform, Barco CTRL is designed to operate confidently in both environments. It integrates natively into the IT infrastructure, inheriting its security policies, identity management, and monitoring tools. At the same time, it respects the operational imperatives of OT environments – delivering security measures that work transparently in the background without creating friction for operators whose focus must remain on the operation itself.

This balance is not easy to achieve, and it is not achieved by accident. It requires deep understanding of both worlds – the kind of understanding that comes from more than three decades of presence in control room environments, combined with a security philosophy that treats operational excellence and cybersecurity as complementary goals rather than competing ones

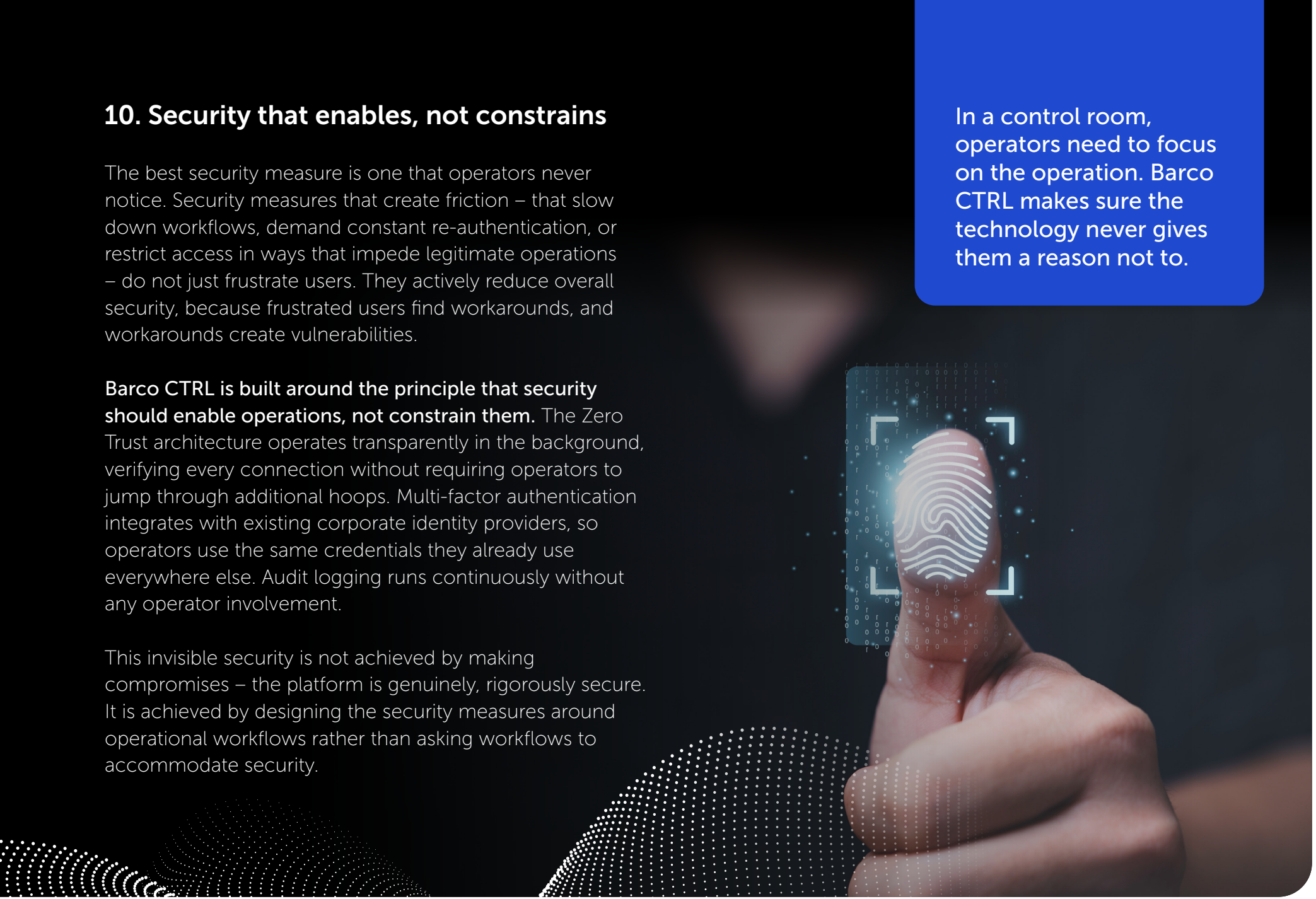
10. Security that enables, not constrains

The best security measure is one that operators never notice. Security measures that create friction – that slow down workflows, demand constant re-authentication, or restrict access in ways that impede legitimate operations – do not just frustrate users. They actively reduce overall security, because frustrated users find workarounds, and workarounds create vulnerabilities.

Barco CTRL is built around the principle that security should enable operations, not constrain them. The Zero Trust architecture operates transparently in the background, verifying every connection without requiring operators to jump through additional hoops. Multi-factor authentication integrates with existing corporate identity providers, so operators use the same credentials they already use everywhere else. Audit logging runs continuously without any operator involvement.

This invisible security is not achieved by making compromises – the platform is genuinely, rigorously secure. It is achieved by designing the security measures around operational workflows rather than asking workflows to accommodate security.

In a control room, operators need to focus on the operation. Barco CTRL makes sure the technology never gives them a reason not to.



11. Regulatory compliance

The regulatory landscape for critical infrastructure is changing rapidly, and the consequences of non-compliance are no longer just financial. The NIS2 directive requires organizations in critical and important sectors to implement comprehensive cybersecurity risk management measures, with executives personally accountable for their organization's compliance. Administrative fines can reach 10 million euros or 2% of global annual turnover for essential entities.

The EU Cyber Resilience Act, coming into effect in December 2027, will require manufacturers to handle vulnerabilities and provide security updates throughout a product's lifecycle. This places new obligations on technology providers – obligations that Barco is already building into the CTRL platform ahead of the deadline. Industry-specific regulations, such as NERC-CIP for the bulk power system in North America are implemented as well, to secure the availability of critical infrastructure. And ISO 27001 certification further demonstrates that Barco's security management processes meet internationally recognized standards.

For organizations deploying Barco CTRL, this means choosing a platform that is already aligned with the direction of travel in regulatory requirements – not one that will require significant rework when new rules come into force.

12. Liability and shared responsibility

When a security breach occurs in a control room environment, the question of who is responsible is rarely simple. **Liability is distributed across a chain of stakeholders: the manufacturer who built the platform, the integrator who deployed it, and the end customer who operates it.** Each carries distinct obligations, and each can be held accountable when those obligations are not met.

Manufacturers are expected to address vulnerabilities promptly and distribute security updates. Integrators are responsible for communicating the availability of those updates and supporting customers through deployment. End customers bear responsibility for installing patches in a timely manner – a responsibility that becomes a liability exposure when it is neglected. Under emerging regulations like NIS2 and the EU Product Liability Directive, these obligations are becoming legally enforceable rather than merely contractual.

Barco approaches this shared responsibility model actively. The combination of automated patch management, clear security guidance for integrators and customers, and a proactive vulnerability management process is designed to make it as easy as possible for every stakeholder in the chain to meet their obligations. Security liability, at its best, is a shared incentive – and Barco CTRL is built to align those incentives across the entire value chain.

Conclusion: security as a foundation, not a feature

In critical infrastructure environments, security is not optional and it is not negotiable. The consequences of a breach – operational disruption, reputational damage, regulatory penalties, and in the most serious cases, real-world harm – are too significant to treat cybersecurity as anything other than a foundational requirement.

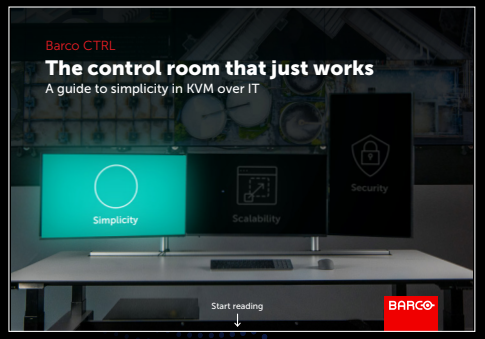
Barco CTRL was designed with that reality in mind. **From the Security by Design principles that shaped its architecture, to the five security pillars that protect every layer of the system, to the dedicated team that maintains and advances its security posture over time: security is what Barco CTRL is built on!**

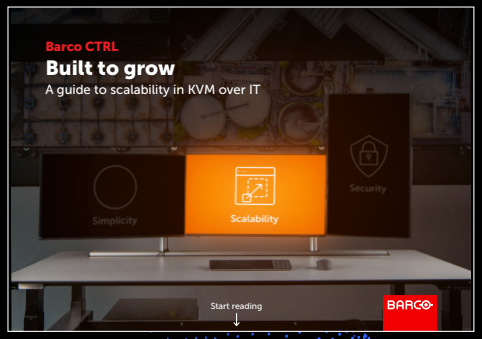
At the same time, Barco CTRL recognizes that security which impedes operations is security that will be circumvented. The platform is designed to be as invisible as it is robust – protecting operators, IT managers, and organizations without ever getting in the way of the work that needs to be done.

Ready to see Barco CTRL in action?

Request your personal demo

and discover how Barco CTRL simplifies your control room from day one.





Today, the combination of uncompromising security and effortless operation is the only acceptable standard for a control room platform trusted with critical infrastructure.

www.barco.com/ctrl

BARCO