

Cyviz Defense Secure Command & Control for Multi-Classification Environments



Prepared for
Defense-related Organizations

Updated
20 October 2026



EXECUTIVE SUMMARY

For nearly three decades, Cyviz has helped defense customers build control rooms, from mobile units and briefing spaces to large command centers. Today, Cyviz delivers this expertise through the Cyviz Platform, a standardized, configurable, and upgradeable alternative to bespoke, room-by-room engineering.

This white paper outlines Cyviz' role in secure video routing, visualization, and command-and-control environments. The Cyviz Platform enables defense users to securely access, visualize, and collaborate with authorized information in physical, hybrid, and multi-classification environments, while supporting the required separation between security domains.

Cyziv supports demanding defense workflows, including mission planning, crisis response, operational command, and multi-source visualization.

Drawing on an established track record with defense organizations, government agencies, and global enterprises, Cyviz delivers secure, reliable, accreditation-aware solutions for environments where operational continuity, information assurance, and decision quality are critical.

Designed for lifecycle durability, the platform supports controlled technology integration and long-term evolution without compromising security, governance, usability, or the separation required between classified domains.



THE CHALLENGE

Defense environments are inherently complex, involving varied, secure, and classified systems. Traditionally, defense integrators addressed this with bespoke solutions that took months to engineer and deliver, which required extensive on-site support. Cyviz has recognized the need to deploy and administer these security-intensive environments faster and more simply.

Moving beyond custom-engineered meeting and collaboration systems, Cyviz addresses these challenges through repeatable platform architecture, secure integration, and long-term operational support. This positions Cyviz not only as a technology provider, but as a strategic partner for organizations operating business-critical and mission-critical environments.

OUR VALUE TO CUSTOMERS

Empowering defense users

Commanders, operators, and mission teams can securely connect, visualize, and collaborate across the information they need.

Solutions that simplify secure operations

Rapid deployment, intuitive operation, and a consistent user experience reduce support burden without compromising control.

A platform for mission assurance

A standardized, configurable, upgradable, scalable platform supports repeatable deployments and dependable long-term operation.

OUR COMMITMENT TO CUSTOMERS

Operator-centric design

We design around the people who must interpret information and act under pressure.

Security and accountability

Secure, classified environments require clear separation, traceability, and ownership of technology.

Standardized turnkey delivery

The platform approach reduces the long engineering and support cycles associated with bespoke systems.

OUR PLACE IN THE MARKET

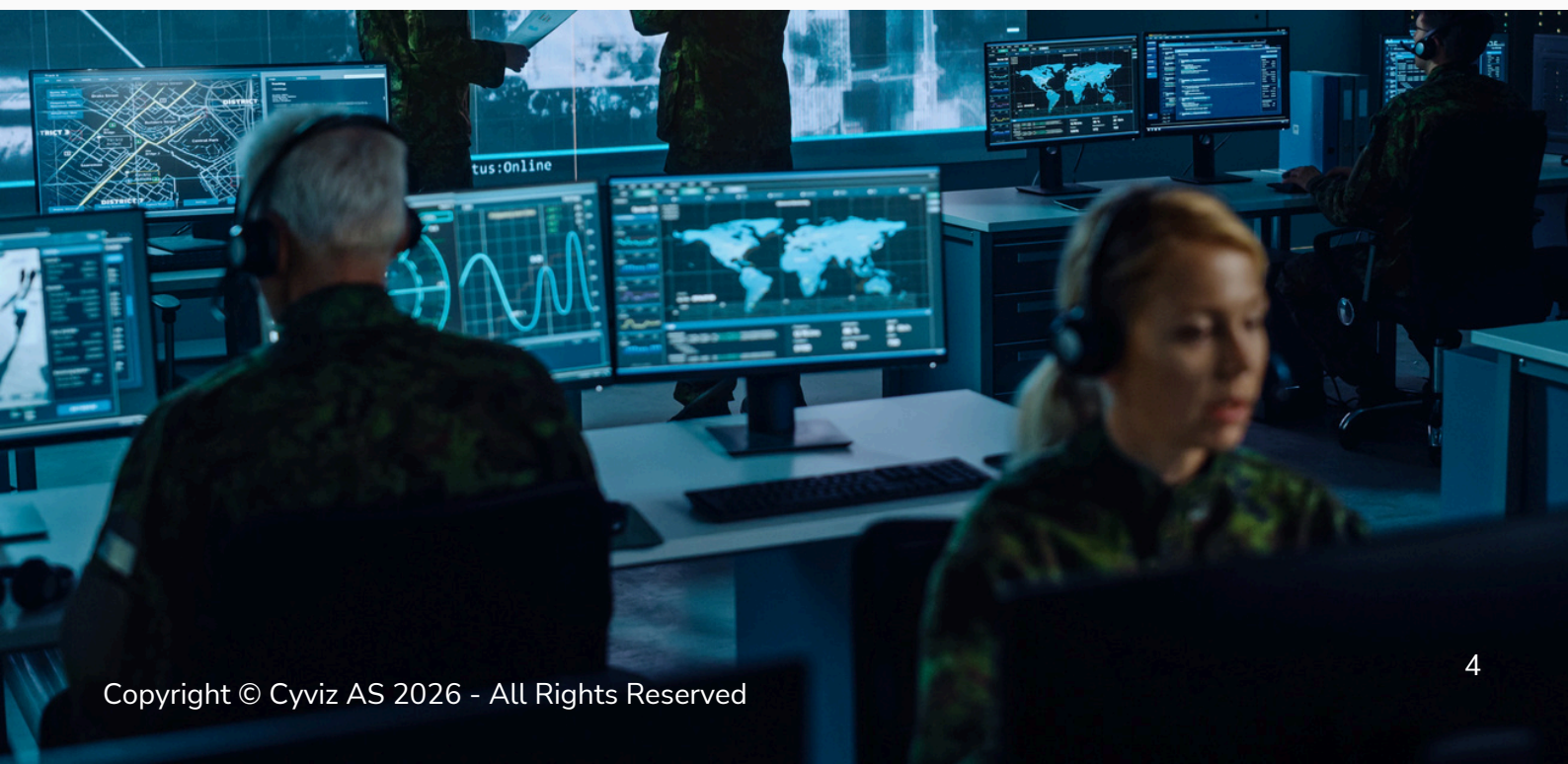
Cyviz delivers complete secure-room and operational-environment solutions for defense organizations that require more than traditional KVM routing or conventional AV integration. Rather than focusing solely on keyboard, video, and mouse control, Cyviz offers a broader, platform-led approach that combines secure visual computing, advanced visualization, collaboration, and operational control into a cohesive mission-support architecture.

Cyviz solutions support command decision-making, situational awareness, and operational efficiency across complex defense environments. The portfolio includes secure briefing rooms, mission-planning spaces, command-and-control environments, operations centers, and mission-critical collaboration rooms, enabling defense customers to access, visualize, and control authorized information within secure and multi-classification environments.

A key differentiator is Cyviz' ability to combine user-centric design with secure integration and scalable platform architecture. The result is a technically robust, operationally consistent solution model that adapts to evolving mission requirements. Cyviz also provides the consulting, design, implementation, lifecycle management, and support services needed to deliver predictable outcomes across the full defense solution lifecycle.

Cyviz' customer base includes defense organizations across markets such as the United Kingdom, the U.S. and the Netherlands, government bodies, global enterprises including Microsoft, Accenture, Thales and KPMG, and critical-operations companies such as Aker BP and Equinor.

In total, Cyviz has installed and supports more than 1,500 installations worldwide, providing a strong reference base for secure collaboration, advanced visualization, and mission-critical operational environments.





HOW WE COMPARE

Defense buyers evaluating this space typically weigh Cyviz against two other models. The first is point solutions from dedicated KVM/extender vendors, which route signals reliably but leave visualization, room control, and lifecycle management as separate procurements to integrate and support independently.

The second is bespoke AV integration, where a systems integrator custom-programs each room individually, flexible at the outset, but costly to maintain, inconsistent across an estate, and slow to modify as requirements evolve, since changes typically require on-site re-programming of the control system.

Cyziv's platform model treats KVM, visualization, collaboration, and room control as one standardized, configuration-led system rather than separately integrated components. The trade-off customers should weigh is that a platform approach concentrates more of the architecture with a single vendor; Cyviz addresses this through on-premises deployment options, selective and verified onboarding of third-party equipment onto the Cyviz Platform, and accreditation history with MODs in the UK,

Norway, and the Netherlands, as well as the U.S. Department of Defense. Organizations should evaluate this against their own vendor-diversification and exit-strategy requirements as part of due diligence.

COMPANY OVERVIEW

Cyziv is a global technology provider specializing in remote operations centers, conference rooms, executive boardrooms, visualization rooms, control rooms and experience centers. Since 1998, Cyviz has enabled digital workforces to connect, visualize and collaborate around critical data through IT-driven turnkey solutions designed to be simple to deploy, manage and support.

Cyziv currently employs approximately 160 people globally. The company is headquartered in Norway, with facilities in Oslo and Stavanger, and maintains a global office footprint including:

- UK, London & Edinburgh
- Netherlands
- U.S., Washington, Atlanta, Houston
- Saudi Arabia, Riyadh
- UAE, Dubai
- Singapore
- India

- Microsoft Technology Centers incorporating Cyviz
- 11 Cyviz Experience Centers (CEC)

- Selected Cyviz Customer Locations
- 7 Partner Showrooms



82 countries represented in
Cyviz' global customer base

18 locations with Cyviz Experience
Centers or Partner Showrooms

Cyviz has developed its standardized offering over many years across projects including Innovation Centers for Microsoft (Microsoft Technology Centers), North Sea oil-rig control rooms, and military customers in NATO countries. Organizations such as Accenture, BMW, and KPMG use Cyviz solutions, and defense companies including Boeing, Airbus, Lockheed Martin, Thales, Babcock, and QinetiQ.

Cyviz has delivered solutions used in accredited defense environments in the UK, Norway, the Netherlands, and the United States. Applicable deployments can incorporate products and technologies evaluated or certified against relevant security requirements, including TEMPEST and Common Criteria.

Cyviz is a project-based organization and the military / non-military project ratio varies by period; overall, 25–30% of Cyviz' projects are

Defense or Defense-related. Cyviz' turnkey solutions are built on proven design principles, use verified components, and are managed through the Cyviz Monitoring & Management Platform. Cyviz delivers solutions ranging from advanced collaboration rooms to operator desks and large command-and-control centers with associated break-out rooms for crisis handling.

In many cases, Cyviz solutions offer advanced routing of video and USB signals between computers, desks, large screens, and video walls; throughout this paper, we refer to this routing capability as "KVM" (Keyboard, Video and Mouse). KVM lets operators securely route the relevant computer resources to their desks and/or shared assets, such as a video wall or a virtual meeting, even when the underlying computers reside on different networks.

HIGH-LEVEL TOPOLOGY OVERVIEW

The topology below shows a typical system arrangement across five categories:

- IT Infrastructure; where the computer resources reside.
- KVM; the routing layer.
- Operator Desks; where operators work with desktop screens, mouse, and keyboard.
- Cyviz Solution; the audio-visual resources for team collaboration.
- Other Destinations; places where video signals may be shared with other groups.

IT INFRASTRUCTURE

IT infrastructure refers to the workstations operators and other room users need to fulfill their roles. Typically, this includes physical computing devices (PCs, thin clients, or laptops) that one or more operators must view and, in many cases, control via keyboard and mouse, along with other video-output devices such as video-conferencing codecs or special-purpose appliances.

In a multi-classification environment, these PCs are expected to reside on individual networks tied to a particular classification (for example, Network A for OFFICIAL, Network B for SECRET, Network C for TOP SECRET); networks associated with defined security domains, whose required separation and security boundaries must be maintained.

Alongside the workstations sit the KVM encoder units, connected via video and USB cabling. This topology keeps the KVM layer separate from the computer network layer, a separation that must hold even where the KVM layer is itself IP-based. IT networks must remain isolated from AV networks, and the two must not be conflated (see the KVM section).

KVM

The KVM layer represents the core routing fabric for signals throughout the system. In some cases, the requirement is simply to display video from a computer; in others, the operator station needs full KVM connectivity to a set of computers.



Computers must be connected in ways that respect certain security principles. Screen-scraping software, for instance, is undesirable because it runs with access to all parts of the PC, including the video being processed by the graphics card, and because its output must be streamed over the computer network connection, which is unworkable in a multi-classified environment where content must come from multiple, separate networks.

For environments requiring separation between mission networks and the visual-access layer, hardware-based KVM architectures can provide a clearly defined signal path independent of software running on the mission computer. Security properties still depend on the selected technology, configuration, and approved system architecture. This also serves performance: dedicated hardware achieves lower latency and avoids the compression penalties of software-based alternatives. Because routing also carries USB for mouse, keyboard, and other human-machine devices, performance and latency receive particular attention; end users will not tolerate a lagging mouse pointer.

Operators often need to interact with multiple computers from the same desk, so fast, secure, and simple switching is a key criterion. Operators want a seamless experience: moving the mouse between monitors should automatically route mouse and keyboard input to the correct computer.

Management of Rules

Beyond the logic defined in operator-desk and room control systems, the KVM system should reflect the environment's operating rules. As a critical security layer, KVM should define how sources are allowed or disabled for specific operator desks, screens, or video walls. e.g.:

- Read-only access sources: where an operator or other user can see but not interact with a source, particularly relevant for shared resources such as a large video wall.
- Routing logic: for instance, blocking a particular source from being routed to a particular destination.
- Exclusive access sources: ensuring that a source can only be routed to a single destination at a time.

Administrative access to the KVM environment should be restricted to authorised, authenticated users in accordance with the customer's security policy and the capabilities of the selected KVM platform.

Secure Transmission

Beyond the operator's experience, the underlying architecture must route signals securely without compromising the integrity of the underlying IT networks. Three broad variants of signal-routing technology exist, each with distinct trade-offs in price, performance, flexibility, and security. See table.

Variant	Signal Path	Typical Trade-off
Native	Computer → native signal cable → KVM → native signal cable → destination	Lowest latency and no protocol conversion; distance and scale are limited by native cabling.
Encoded over TCP/IP	Computer → encoder → network switch → decoder → destination	Highly scalable and flexible over standard network infrastructure; requires securing and segregating the IP layer from IT networks.
Encoded over optical	Computer → encoder → fibre cable → KVM → fibre cable → decoder → destination	High performance over long distances and potential architectural benefits where electrical isolation is required; security depends on the complete KVM architecture and configuration.

Accreditation / Validation

Accrediting and validating these complex systems requires a thorough understanding of, and clear communication about, the underlying architecture and how security is managed throughout the signal chain. Certain KVM products may hold independent Common Criteria certification at EAL4 or other applicable assurance levels. EAL4 provides assurance that the defined Target of Evaluation has been methodically designed, tested, and reviewed against its specified Security Target. Evaluated components can provide supporting assurance evidence for the customer's wider system security assessment and accreditation process.

User Interaction / Integration

Cyviz solutions are designed with a strong focus on ease of use and a human-centric approach, which extends to the KVM components within our comprehensive solutions. A room's success hinges on its operability from a user perspective, and a consistent user experience is paramount: all Cyviz rooms function identically from a user's standpoint, from standard meeting rooms to complex command and control environments. Cyviz maintains close relationships with its KVM vendors to keep this consistency integral to the overall solution.

OPERATOR DESKS

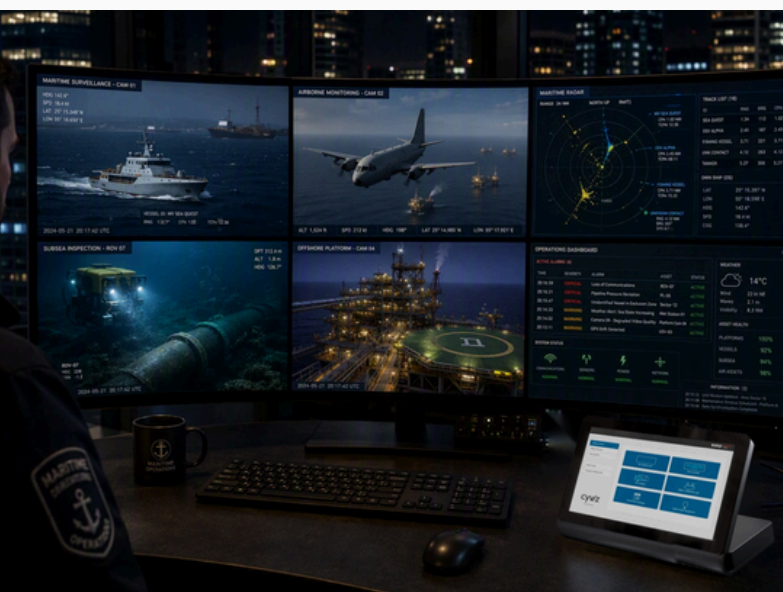
At operator desks, humans interact with the computers. A KVM creates a route between the operator's video, audio, and USB devices and one or more computers, allowing one operator to securely access multiple computers on different networks at the same time.

The KVM system allows an operator to view and control multiple workstations from a single desk with multiple screens and one keyboard and mouse. Traditionally, operators relied on hotkeys to manage routing; some KVM systems now offer intuitive "mouse-over-display" switching, where moving the mouse over a monitor automatically routes keyboard and mouse to that PC source, giving operators a seamless experience and enhancing their ability to respond quickly and accurately.

Define and communicate operator roles and responsibilities based on how the room will operate, so the system can prevent the wrong action (intended or not) and help operators do the right thing. Considerations include: Will the same person sit at the same desk every day? How does the system verify an operator is at the correct seat? Do role requirements at a desk change depending on the situation?

Cyviz uses authentication and role-based access control to ensure the right operators can access the right information at the right time. A Cyviz Controller deployed at each operator desk defines which computers are available to that operator, and whether access is video-only or video-plus-USB.

Operators can define different setups and save them as presets for easy retrieval.





THE CYVIZ SOLUTION

A Cyviz Collaboration Solution typically includes a large video wall, where decoders pull video from the KVM layer so the video processor can compose an image from multiple computers simultaneously. In this scenario, sources are treated as read-only for compositing on the shared display wall, creating a common operating picture.

Cyviz Controller

The Cyviz Solution includes a Cyviz Control system that lets users control the room from a single touch panel. A designated individual, often a shift leader or similar role, typically manages shared resources on the large screen or controls an integrated video-conference system.

The Cyviz Controller is a standardized, configurable control system providing:

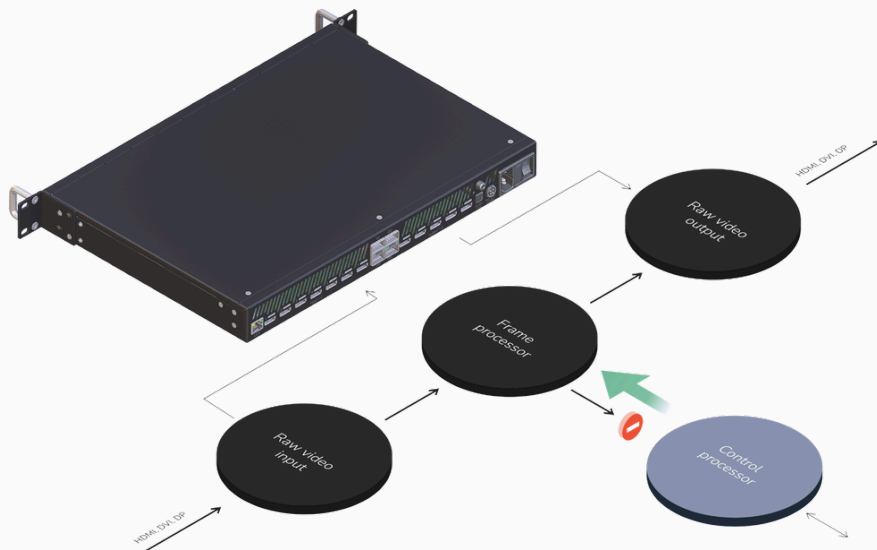
- A configurable control system for all room and operator-station functions.
- Control over how video sources are placed on the video wall or on stand-alone screens.
- Simplified "snap to grid" control for LCD panel display walls.

- The ability to save and recall different screen layouts as presets.
- Seamless integration with video-conference technology from Cisco, Poly and Microsoft.
- Integration with building management systems for control of lights, curtains and similar.
- Integrated, intuitive help functions.
- The Cyviz Controller is TEMPEST B certifiable.

Cyviz Video Processor

The video processor combines video from multiple sources into a single large image. Cyviz' video-wall architecture separates video processing, signal routing, and system control: the processor operates on raw video signals rather than PC graphics cards or grabber cards, minimizing latency and avoiding pixel loss; the KVM system routes video signals from computing devices to the processor; and the controller orchestrates the operation.

The Cyviz Video Processor (TEMPEST B certifiable) is built so the control software can't access the video signals (pixels) flowing through the processor, maintaining architectural separation between system control and video processing.



Display Solution

Display technology selection (LCD, LED or projection) is influenced by the need to support both high-performance visualization and multi-discipline team collaboration; each option carries distinct trade-offs and the right choice depends on end-user requirements, including any need to meet TEMPEST certification requirements for minimizing electromagnetic radiation.

The Cyviz CP10 projector has low power consumption, low heat dissipation, and low noise, requires minimal maintenance, and has a light-source lifetime of 100,000 hours (over 11 years of 24/7 use).

The only serviceable part is the fan cartridge, typically replaced every five years. CP10 projectors blend seamlessly into large video walls and are TEMPEST A-certifiable.

OTHER DESTINATIONS

Read-only content can route to other destinations, such as a separate breakout meeting room or display, so key stakeholders stay informed without disrupting the control room's focus on primary activities.

A designated individual (typically the shift leader), supported by system rules, must control what others see.

Conversely, some scenarios require sending data back into the control room, and these routes are also supported.



MANUFACTURER INFORMATION

A Cyviz system typically combines Cyviz hardware and software with third-party components (for example, the KVM layer) to provide a turnkey solution. Cyviz onboarded all third-party equipment used in a Cyviz solution into the Cyviz Platform, meaning Cyviz validates supported third-party equipment for integration, interoperability, and compatibility with the Cyviz Platform.

- The Cyviz Software is owned and developed by Cyviz AS, the Norwegian parent entity.
- The Cyviz Controller and Cyviz Touch Panel are designed by Cyviz and manufactured in Taiwan.
- The Cyviz Video Processor is designed by Cyviz and manufactured in Edinburgh, Scotland.
- The Cyviz CP10 DLP projector is manufactured in Norway.

Cyziv' solutions are protected by several patents and trademarks, ensuring exclusive rights to its intellectual property. Cyviz complies with all applicable export-control regulations; depending on the destination country, it may require export licenses to transfer its technology internationally.

SOLUTION STRENGTHS

Platform Design — Standardization & Stability

Cyziv is differentiated from competitors by offering highly standardized advanced visualization and collaboration solutions. Traditional AV integrators' lack of standardization has historically led to high total cost of ownership, vendor lock-in, complex lifecycle management, reduced reliability, and user experiences that decline over time.

Cyziv pioneered platform standardization to improve predictability, reliability and cost of deployment and management, with easier integration and evolution over time.

The Cyviz Platform replaces bespoke, custom-programmed systems, shifting from customized, non-scalable deployments to standardized, scalable ones. A consequence of this approach is an extended lifecycle with higher return on investment: solutions are upgradable at every tier and can be modernized as new technology becomes available, with the lifecycle viewed in the context of the expected lifecycle of the physical space or building itself, delivering higher ROI, lower total cost of ownership, and a more durable, environmentally sound solution.

The centralized Cyviz Monitoring and Management Server, used for management and support, can be deployed on-premises and operated within the customer's controlled network environment, subject to the customer's approved security architecture and applicable requirements.

Flexibility and Futureproofing

The Cyviz solution supports many use cases and can evolve rapidly in response to changing needs and modes of use, as well as improvements in operational processes, workflows and digitalization. The Cyviz technology model allows rooms and their associated technology stack to be reconfigured without the costly on-site reprogramming typical of other AV platforms, keeping customers futureproofed and able to adopt new technology quickly, without long development cycles in bespoke systems.

Maintenance

Cyziv operates a remote service desk based in Europe, available 24/7, with varying priority levels, subject to secure access to the relevant system. Different Service Level Agreements are available to suit each location, room, or configuration. The Cyviz Global Support team is based in Edinburgh, UK; the next section summarizes typical service tiers.

Tier	Description
Tier 1	On-site / first-line response by trained local staff, supported by Cyviz Monitoring and Management diagnostics.
Tier 2	Remote engagement from the Cyviz Global Support desk (Edinburgh, UK), 24/7, subject to secure access arrangements.
Tier 3	Engineering escalation and, where required and approved by the end customer, dispatch of a Cyviz engineer to site.

The Cyviz Monitoring and Management Server dashboard offers authorized support personnel advanced diagnostics and debugging capabilities, including interactive debug sessions and live support, with multiple operators able to join the same system for joint debugging.

Cyziv' architecture enables users and support staff to self-help with many incidents using in-house resources, supported by a professional Cyviz service desk; the solutions are IT-mature, meaning many issues can be addressed from an IT-operations perspective. With minimal training, internal staff can manage day-to-day operations and support, while the support architecture gives authorized personnel access to system health, configuration, and diagnostic information without exposing the visual content the system processes. This is a newer support model for secure deployments; the team agrees on the exact implementation during early workshops to deliver the highest availability. When support is needed beyond the internal first line, the Cyviz Global Support team provides a single point of contact for help and IT support.

QUALITY ASSURANCE

All solutions undergo multiple internal checkpoints during the design process before the client provides final sign-off. In a multi-classification system context, Cyviz applies

secure-by-design principles, and its solutions conform to control frameworks. Cyviz can:

- Demonstrate adherence to general IT best practices, including support for strong authentication and multi-factor authentication as part of role-based access control and system administration.
- Assist the client with relevant penetration testing and audit reports.
- Show a viable software maintenance program that mitigates security issues over time.
- Demonstrate the Cyviz Monitoring and Management Server's ability to securely log all relevant events for analysis.
- Demonstrate the Cyviz network architecture and how the system is isolated from production and video-conferencing networks.
- Demonstrate the defined direction of video-signal flow within applicable parts of the Cyviz architecture and the architectural separation between video processing and system control.
- Demonstrate and prove recovery processes.
- Provide relevant assurance evidence covering applicable organizational controls, governance processes, and incident-management procedures.

Cyziv' approach also provides additional assurance through risk management. Cyviz maintains a SOC 2 assurance report, is Cyber Essentials certified, and is registered with JOSCAR (Joint Supply Chain Accreditation Register).



ABOUT CYVIZ CONTROLLER

Cyziz Controller is a comprehensive control, orchestration, and management platform for advanced collaboration, operations, and mission-critical room environments. Built on a standardized and upgradeable software architecture, the platform abstracts underlying AV, KVM, visualization, video-conferencing, and room-control technologies into a consistent operational layer, enabling organizations to control sources, displays, audio, USB routing, conferencing workflows, presets, and room states through a unified user experience, while maintaining separation between control, signal routing, and secure IT networks.

- Intuitive multi-touch user experience for room control, source selection, layout management, conferencing and operator workflows.
- Consistent operational model across rooms and sites, reducing retraining, configuration drift and support variability over time.
- Dynamic picture-in-picture and layout composition for flexible multi-source visualization across displays, video walls and shared operational views.
- Integrated video-conferencing workflows supporting hybrid collaboration, operational briefings and controlled sharing of visual content to remote participants.
- Enterprise integration with Microsoft Active Directory and Exchange to support identity-aware access, scheduling and room availability.
- Support for wireless presentation systems and interoperable collaboration technologies through pre-integrated, validated device profiles.
- Efficient deployment based on repeatable system templates, reducing bespoke engineering effort, implementation risk and commissioning time.
- Configuration-led operation with minimal bespoke programming, enabling predictable room changes, device updates and workflow adjustments across the estate.
- Built-in monitoring, diagnostics and debug capabilities across AV, KVM, display, conferencing and room-control assets, supporting proactive service management.
- Predictable operating costs through standardized platform management, validated integrations and lifecycle governance across rooms and sites.

Case Study

UK Ministry of Defence

The Challenge

The Cyber & Specialist Operations Command within the UK Ministry of Defense needed a secure command-and-control environment to support mission-critical decision-making in a complex operational setting. The requirement was to:

- Consolidate multiple data feeds into a single, coherent operational picture;
- Enable secure collaboration across different classification levels;
- Support rapid analysis and decision-making in a controlled environment; and
- Deliver within a tight timeframe while meeting strict defense-sector requirements.

The Solution

Cyviz delivered a secure command-and-control environment built on the Cyviz Software Platform, giving operators a single operational view while supporting controlled collaboration across multiple classification levels.

Cyviz consolidated authorized information from multiple sources into a common visual environment, enabling personnel to access and compare relevant information while maintaining the defined separation between security domains.

Because the design embedded security considerations from the outset, deployment also gives the customer a secure-by-design foundation for future accreditation, compliance, and security reviews, and a basis for wider deployment across other defense and government use cases.

Outcome and Key Learnings

- Integration creates value: bringing multiple information sources into one operational view gave teams a clearer, more complete picture, reducing reliance on fragmented inputs and improving coordination.
- Security must be built into every layer: operational efficiency and information protection were treated as inseparable requirements, not competing ones, throughout delivery.
- Agility matters: close collaboration between the customer and the project team, with clear priorities and regular communication, allowed delivery within a demanding timeframe without relaxing the standards expected in a secure defense environment.

This deployment is an established UK defense-sector reference for Cyviz, demonstrating its ability to deliver complex, secure-by-design command-and-control environments for customers operating in highly regulated, mission-critical settings.

Secure Command and Control for Mission-Critical UK Defense Operations

Industry	Defense	Products	Cyviz Software Platform; visualization and command & control solutions, multi-classification collaboration capabilities.
Location	United Kingdom	Customer	Cyber & Specialist Operations Command, UK Ministry of Defence

CONCLUSION

Defense command-and-control environments require more than the integration of discrete AV, KVM and control-system components. They require a coherent, security-led architecture that separates control, signal routing, and classified IT domains while enabling operators to access, visualize, and act on mission-critical information with speed, confidence, and control. In this context, Cyviz provides a platform-led approach that combines secure system design, validated technology integration and consistent user interaction across briefing rooms, operations centers, secure collaboration spaces and multi-domain operational environments.

The Cyviz Platform is central to this approach. By abstracting complex underlying technologies into a standardized control and orchestration layer, Cyviz Controller enables defense customers to manage source routing, display composition, conferencing workflows, operator access, presets, diagnostics and lifecycle support through a repeatable and supportive model, reducing bespoke engineering, limiting configuration drift, improving operational consistency and

supporting secure governance across classified and mission-critical environments. For defense, government, and critical-infrastructure organizations, Cyviz delivers secure, scalable, future-ready solutions without compromising usability, resilience, or operational performance.

The combination of platform standardization, security-by-design principles, validated integrations, and global lifecycle support positions Cyviz as a strategic partner for customers who need resilient technology environments that can evolve with operational, security, and digital transformation requirements.

Ultimately, Cyviz enables defense organizations to move beyond fragmented room-by-room technology deployments towards an integrated platform model for secure collaboration, visualization, and operational control, creating long-term mission value through improved decision-making, reduced operational complexity, stronger supportability, and greater confidence in environments where information integrity, availability, and operator effectiveness are essential.

Suggested next steps

We welcome the opportunity to discuss how the Cyviz Platform could support your program.

- A scoping workshop to map your operational spaces, classification boundaries, and accreditation requirements against the Cyviz Platform.
- A written response to a Request for Information (RFI) or Request for Proposal (RFP).
- A site visit or live demonstration of a comparable Cyviz deployment.

Contact us: cyviz.com