DATACENTRE SECURITY SERIES | 2026 EDITION

Securing the Core: Why Air-Gap Solutions Matter

Addressing the risk of PHP vulnerabilities

A practical, hardware-first approach to separating the management plane, governing privileged console access, and preserving a trusted route to recovery for critical systems.



16 / 32
KG CONSOLE PORTS
FOR PROTECTED MANAGEMENT

BIOS
LEVEL ACCESS WHEN
IN-BAND TOOLS FAIL

31
CC2000 SECONDARY
SERVERS SUPPORTED

ATEN PRODUCT FEATURE SET

Physical separation
Separate switching and cabling for the KVM management plane—not merely a VLAN label.

Out-of-band management
Video and USB console access can remain available when production access or the host OS is unavailable.

Accountable privilege
Identity integration, role controls, encryption, logging and optional session recording support governed access.

Recovery readiness
Validate the boundary and rehearse approved BIOS, virtual-media and break-glass recovery workflows.

CONTENTS

Table of Contents

01 **Executive Summary** — 03
Threat context · hardware-first value proposition · scope and assurance

02 **What Is an Air Gap?** — 04
Foundational concept · physical separation · trust boundaries

03 **Software Remote Access vs. Hardware KVM** — 05
Architectural comparison · limitations and controls

04 **The ATEN Air-Gap Architecture** — 06
Reference design · Figure 3 deployment diagram · no-bridge rules

05 **What Is PHP?** — 07
Runtime, application and deployment risk—why the distinction matters

06 **PHP and the Attack Chain** — 08
PHP2Shell CVEs · exposure conditions · patch and containment priorities

07 **Assess PHP Exposure at Both Layers** — 09
Product applicability · customer deployment exposure · UK resilience context

08 **Turn Isolation into Resilience** — 10
Contain the route · recovery when in-band tools fail · controlled transfers

09 **Recovery and Deployment Proof** — 11
Control model · validation checklist · measurable outcomes

10 **Conclusion** — 12
A governed, recoverable management plane

11 **ATEN KG & Secure KVM** — 13–14
KVM adapters · secure KVM · control-room access

12 **CC2000 Management Platform** — 15
KVM · serial console · PDU · access governance

13 **CCVSR Recording Platform** — 16
LiveView · session recording · investigation · resilient storage

14 **Datacentre Power Oversight** — 17
eco DC · intelligent PDU · metering · controlled power

15 **Complete Solution Summary** — 18
IP KVM · PDU · CC2000 · CCVSR · resilience use cases

16 **Consolidated References & Sources** — 19
Product documentation · threat data · standards and advisories

Solution design & demonstrations

For a tailored architecture assessment, bring the critical-server list, console interfaces, authentication requirements and recovery objectives.

Contact ATEN UK

sales@aten.co.uk
01753 539121
www.aten.com/gb/en

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

OVERVIEW

Executive Summary

Critical systems need more than a stronger front door. They need fewer reachable paths from a compromised production environment to the privileged management plane. ATEN's Air-Gap approach combines a separately protected KVM management path with accountable console access, allowing authorised teams to retain BIOS-level visibility and control when in-band tools are unavailable. [1] [3] [4]

> **"The objective is a physically separate management path and a tested route to recovery—not an assertion that any single product prevents every attack."**

THE RESILIENCE CASE

31k+	£3.74m	43 days	16 / 32
SECURITY INCIDENTS EXAMINED IN VERIZON'S 2026 DBIR	ILLUSTRATIVE GBP EQUIVALENT OF IBM'S GLOBAL AVERAGE BREACH COST	VERIZON-REPORTED MEDIAN TIME TO FULLY RESOLVE CRITICAL VULNERABILITIES	KG0016 / KG0032 KVM PORT DENSITY CHOICES

DBIR, IBM and conversion figures are context—not a prediction of an individual breach or an ATEN risk-reduction measure. The GBP figure uses a Bank of England reference rate and is not a UK-only average. **[1] [2] [24]**

WHY SOFTWARE-ONLY ACCESS IS NOT ENOUGH

In-band dependency

Remote-control tools share the infrastructure they manage. A production-network compromise can become a management-plane problem.

OS dependency

If the operating system is crashed, locked or unsafe to use, normal software access may fail at the moment it is needed most.

Privileged pathway

Management sessions, credentials and transfers deserve stronger boundary controls, audit evidence and deliberate recovery procedures.

Scope discipline. A KVM-over-IP gateway remains an IP-addressable appliance. The protection comes from the designed boundary, controlled operators and verified deployment—not from treating KVM as a data diode, cross-domain guard or universal security control.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

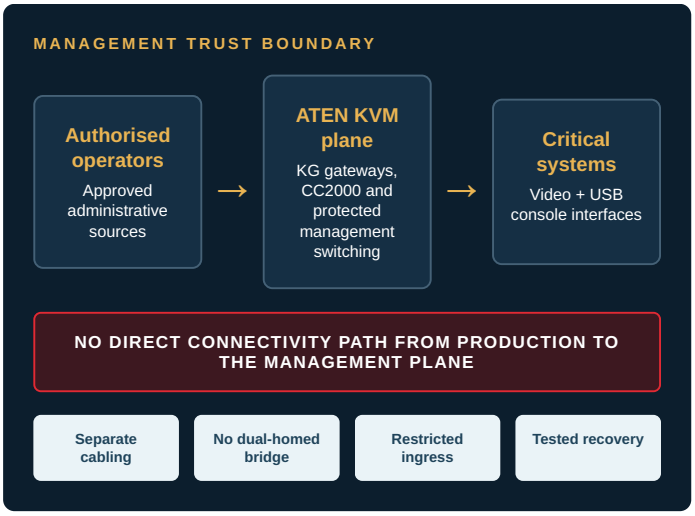
FOUNDATIONAL CONCEPT

What Is an Air Gap?

An air gap is a security measure in which a secure system or network is physically isolated from other domains. In strict form, it has no network connection to another domain. A VLAN or firewall policy can be valuable segmentation, but it is not a physical air gap.

For the ATEN Air-Gap Solution, the defensible objective is a **separate management path**: dedicated management switching and cabling reach critical servers through video and USB console interfaces while server business Ethernet remains on production infrastructure. KG gateways themselves remain networked devices. [3] [5] [6]

> **Separate the management plane without accidentally creating a production-to-management route.**



WHERE THE ARCHITECTURE ADDS VALUE

Critical infrastructure

Operations that need an independently governed route to inspect, contain and recover critical systems.

High-trust IT & OT

Compatible server and industrial-computing environments where console access has appropriate safety controls.

KEEP THE BOUNDARY HONEST

Define it

Document every NIC, cable, switch, gateway, directory service, log destination and update path.

Protect it

Treat administrative workstations, console accounts and management services as high-trust assets.

Prove it

Test that production hosts cannot reach KG, CC2000 or their administrative interfaces—including failover states.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

CRITICAL ANALYSIS

Software Remote Access vs. Hardware KVM

Software remote-management tools can be fast to deploy and highly useful for many tasks. For business-critical infrastructure, however, the management plane should be designed so that failure or compromise of ordinary production access does not automatically remove the operator's route to the console.

IN-BAND VS. OUT-OF-BAND MANAGEMENT

In-band

In-band management uses the same normal production network that carries business traffic and typically depends on the server's operating system, software services or network reachability. Examples include remote desktop, VNC and web-based administration over the production LAN.

Out-of-band

Out-of-band management uses a separate, dedicated management path to reach the server console—typically video and USB—so authorised access can remain available when the production network or host operating system is unavailable.

Important boundary: "Out-of-band" does not automatically mean "air-gapped." KVM over IP is still IP-enabled; the stronger protection comes from separate management switching and cabling, controlled administrative access and no route or bridge from production to the protected management plane.

Important distinction. Hardware KVM reduces selected dependencies and can support an independently protected console path. It does not make a compromised host safe, replace endpoint protection, or eliminate the need for incident response and patch management.

HEAD-TO-HEAD CONTROL MODEL

SECURITY ATTRIBUTE	TYPICAL IN-BAND REMOTE ACCESS	ATEN KVM OVER IP IN A PROTECTED MANAGEMENT PLANE
Network relationship	**Depends on** production network reachability	**Separately designed** management network and cabling
OS dependency	Host OS and in-band services must be operational	**Video / USB console** can support BIOS-level access
Server-side agent	Often uses a remote-control service or OS feature	**No remote-control agent** required on the managed server
Privileged access	Identity and audit controls vary by platform	KG and CC2000 capabilities can support users, groups, filtering, encryption and logs [5] [6] [7]
Outage response	**May be unavailable** when production or OS access fails	**Separate console path** can aid approved diagnosis and recovery
Risk boundary	Management and business traffic can share reachable infrastructure	Boundary strength depends on actual segmentation, cabling, policies and operator controls

WHAT KVM DOES NOT SOLVE

Not a data diode

Keyboard input and virtual media are powerful bidirectional capabilities. Apply high-trust operator and media controls.

No automatic remediation

Isolation can constrain selected attack paths; vulnerable runtimes and applications still require remediation.

Not a guarantee

Availability depends on the broader system: power, switching, identity, endpoint and recovery design.

Design principle: retain a tightly governed console route for authorised recovery while making it demonstrably harder for a production foothold to reach privileged management services.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

ATEN SOLUTION

The ATEN Air-Gap Architecture

ATEN's reference pattern combines authorised personnel, a controlled enterprise access layer, a protected KVM management plane and critical systems. The management plane includes KG uplinks, CC2000 (where selected) and administrative workstations; server business Ethernet remains on production infrastructure. [3] [5] [6] [7]

ARCHITECTURE RULES

1. No accidental bridge

Do not route or bridge production and management domains through a gateway, dual-homed host or temporary convenience connection.

2. Restrict permitted remote access

Where external administration is required, terminate at a tightly controlled enterprise access layer with approved users, sources and destinations.

3. Keep redundancy within the trust zone

Use the redundant LAN port and redundant power supply to improve availability without opening an unintended production path.

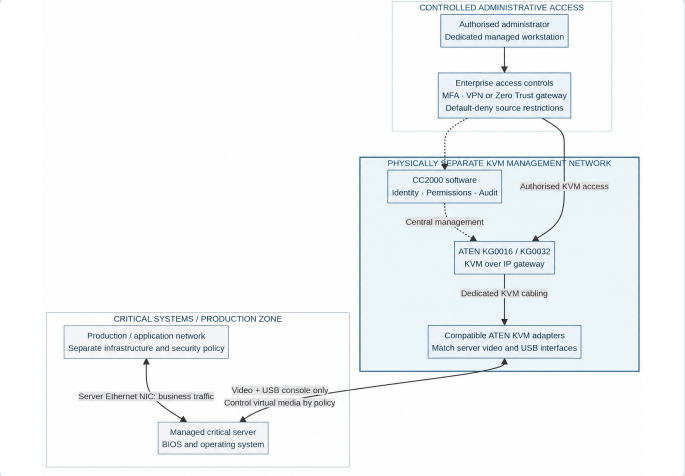


Figure 3. Illustrative deployment, not a factory-default configuration or certification. Solid links show access/console paths; dashed links show central management. Enterprise gateways and MFA are surrounding controls, not claims that all are built into KG hardware. **[3]–[6]**

Who can access what?

Use named users and constrained roles. Validate MFA at the supported product or enterprise-access layer; select trusted certificates and a current cipher policy; retain independent approval for transfers and software changes.

KEY SECURITY PRINCIPLES

01
Agentless server access

Console operation uses server video and USB interfaces rather than a remote-control agent.

02
Separate management plane

Dedicated cabling and switching reduce shared network dependencies.

03
Encryption & identity

Use supported TLS 1.3, AES-256 and military-grade FIPS 140-3 encryption where specified, alongside enterprise identity integration.

04
Evidence & recovery

Logs, reports, recording options and rehearsed procedures make privileged access accountable.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

PHP FOCUS

What is PHP?

PHP is a server-side programming language used to process requests and generate dynamic content. It commonly handles web requests, application logic and database interactions behind websites, portals and services. [14]

PHP is a technology. Vulnerabilities are the threat.

PRODUCT SECURITY

Verify the product's actual dependency

ATEN's global Security Advisory 40, released on 21 October 2026, states that its assessment of CVE-2026-109618 and CVE-2026-109619 covers all currently supported versions of its products. ATEN reports no use of the affected PHP components, no identified product impact and no current product-specific remediation requirement.

This is the vendor's stated applicability assessment—not an independent guarantee of immunity for every legacy installation, third-party tool or customer application. ATEN advises customers using PHP to review their own installations and the relevant official advisories, and says it will update its assessment if new information emerges. [18]

UK RESILIENCE CONTEXT

Prepare for service disruption

BBC News reported on 22 October 2026 that Wes Streeting warned about increasingly sophisticated cyber-attacks on businesses and disruption to supply chains. Referring to the recently discovered PHP flaw, he said incidents of this kind would happen "more and more". [25]

The BBC article also reported 32 UK government services offline while potential cyber-security issues were addressed. That was a point-in-time report—not a count of confirmed breaches or evidence that services remained offline at publication.

THE DISTINCTION THAT MATTERS

Runtime and platform issues

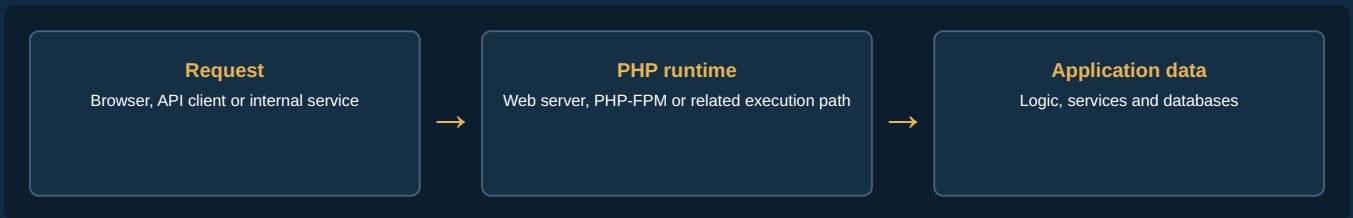
Memory-safety flaws in the PHP runtime or an installed extension can affect a web-request-serving environment independently of an application's business logic.

Application-layer issues

SQL injection, unsafe file handling, flawed authentication and other application vulnerabilities arise from code and deployment choices; they require their own remediation.

THE REQUEST PATH

Where PHP can sit in a critical service



A weakness in one layer can create exposure in the next. Patching, hardening, access control, monitoring and recovery planning all have a role; no single control is a substitute for the others.

Scope of this section. The following pages use the October 2026 PHP2Shell advisories as a dated, evidence-led example. They do not assert that every PHP deployment is exploitable or that PHP is inherently unsafe.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

PHP FOCUS

PHP and the Attack Chain

PHP2Shell illustrates why a vulnerability is not simply a patching ticket: a flaw in a web-request-serving runtime can become an entry point into an application environment, subject to the deployment's exposure, permissions and triggering conditions. The technical detail matters because it determines which systems need urgent review. [14] [15] [16]

CVE-2026-109618

Failure during memory exhaustion

When PHP runs out of memory, some execution paths can leave internal request data only partly initialised. Cleanup may then use invalid data. Under exploitable conditions, an unauthenticated attacker can cause remote code execution in the PHP process, subject to that process's privileges.

The PHP Group assigns CVSS v4.0 9.2, Critical. ATEN's advisory lists 9.8, Critical under CVSS v3.1; the values use different scoring versions. [15] [18]

CVE-2026-109619

Stale state after memory is freed

Internal PHP state can retain pointers to request memory after that memory is released. A later request handled by the same worker may use those stale pointers before they are reinitialised. This use-after-free condition can also enable unauthenticated remote code execution under triggerable conditions.

The PHP Group assigns CVSS v4.0 9.2, Critical. The relevant runtime, service configuration and exposure must be assessed for each environment. [16]

WHERE URGENCY COMES FROM

Known exploited vulnerabilities

Both CVEs were added to CISA's Known Exploited Vulnerabilities catalogue on 26 October 2026. [17]

Web-serving exposure

The PHP project identifies web-request-serving installations as relevant, including PHP-FPM and Apache *mod_php*.

Early execution risk

The supplied guidance identifies *mod_php* as especially exposed because demonstrated exploitation can occur before application code runs. [14] [17]

REMEDIATION PRIORITY

Patch the runtime; do not mistake isolation for remediation.

Fixed PHP releases are 8.2.35, 8.3.36, 8.4.27 and 8.5.12. Use an appropriate fixed supported release or a verified vendor backport. Inventory bundled PHP in appliances and management tools, and prioritise exposed services without overlooking internal systems. [14] [19]

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

PHP FOCUS

Assess PHP Exposure at Both Layers

Establishing whether a product uses an affected component is one question. Assessing the customer's own PHP applications, runtimes, network paths and privileged operations is another. Both matter—but product applicability and deployment exposure should not be conflated.

DEPLOYMENT SECURITY

Assess reachability and privilege

Identify which runtimes are deployed, who can reach them, which services and identities are shared, what privilege a compromised process might gain, how activity is detected and whether recovery still functions during a production outage.

Map public, supplier and internal exposure separately. A service can be important even when it is not internet-facing, particularly where it holds sensitive data, supports administration or shares identity services with critical systems.

OPERATIONAL RESILIENCE

Plan for disruption as well as prevention

A separately protected management path can support authorised inspection and recovery when production access is unavailable. This is an architectural recommendation—not a claim that it patches PHP, makes a compromised host safe or replaces application remediation.

Design the recovery model around named operators, protected administrative workstations, bounded privileges, evidence and tested procedures. [3] [5] [6]

THE CUSTOMER ASSESSMENT CHECKLIST

1. Runtime & applications

Inventory PHP versions, extensions, bundled components, application owners and patch or backport status.

2. Exposure & pathways

Identify external, internal and supplier access routes, shared dependencies and connections to privileged services.

3. Privilege & recovery

Assess what a compromised process could do, how misuse is detected, and whether recovery is rehearsed.

MANAGE BOTH LAYERS TOGETHER

QUESTION	PRODUCT APPLICABILITY	DEPLOYMENT EXPOSURE
What is being assessed?	Whether a specific model and supported release uses an affected component.	Whether an actual customer runtime, application and service path is exposed, exploitable or over-privileged.
Primary evidence	Vendor advisory, model, version, firmware/software lifecycle and verified product scope.	Asset inventory, configuration, access paths, logs, identity relationships, testing and recovery evidence.
Practical outcome	Confirm the vendor statement and retain it with change records.	Patch or backport, harden, restrict reachability, monitor and rehearse response.

Read together with page 7. The ATEN Advisory 40 applicability statement and the UK resilience context are presented on the "What is PHP?" page so the reader can distinguish evidence about a product component from actions needed in the customer's wider deployment.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

RESILIENCE

Turn Isolation into Resilience

Contain the route. Keep recovery available. A separately protected console path is most valuable when ordinary production access is unavailable, unsafe or deliberately shut down.

A PHP compromise should not automatically expose KVM

Consider an attacker exploiting a PHP web application in the production zone. With no production-to-management route, that foothold should not directly reach the protected KVM management plane over IP. An approved administrator can use the independent console path to inspect the affected host, coordinate approved containment and prepare recovery.

That benefit comes from the deployed boundary—not from KVM repairing PHP. The compromised host remains compromised and may still expose data or execute malicious software. [3] [5] [6]

Use BIOS access when in-band tools fail

Video and USB console access can support diagnosis when a server cannot boot normally or the production network is down. Controlled virtual media can support approved installation, diagnostic and recovery workflows; measure any recovery-time improvement locally.

THE OPERATOR BOUNDARY

KVM is still powerful access.

If an attacker also controls the management workstation or an authorised console account, KVM can become an attack tool. Preserve endpoint protection, incident response, forensics and tested restoration alongside the separate management network.



TREAT EVERY TRANSFER AS A CHANGE TO THE BOUNDARY

Virtual media is an exceptional privilege. Permit it only when necessary and supported permissions allow it. Validate images, scan transfer media, restrict file sources, record approvals and remove temporary access afterwards. Protect firmware-update packages and management backups with the same care. If policy prohibits cross-domain transfer, do not enable it for convenience. [5] [6] [9]

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

DEPLOYMENT & PROOF

Recovery and Deployment Proof

A separate console path is most valuable when ordinary production access is unavailable, unsafe or deliberately shut down. The deployment should be commissioned as a measurable control model rather than accepted as a diagram or product claim.

1 Prove separation before enabling access

Document NICs, cables, switches, gateways and services. Test that production hosts cannot reach KG, CC2000 or their admin interfaces; include redundant-link and failover states. [3]

2 Make privileged access accountable

Use named accounts, least-privilege roles, strong authentication and MFA at supported product or enterprise-access layers. Time-limit supplier access and test revocation. [3] [5] [6] [7]

3 Harden the software and evidence trail

Maintain firmware and asset inventory, validate updates under change control, use trusted certificates and current ciphers, and test event delivery during a production outage.

4 Rehearse maintenance and recovery

Demonstrate BIOS access with the OS unavailable; exercise approved virtual media, link/power redundancy, CC2000 recovery and break-glass procedures. [5] [6] [7] [9]

MEASUREMENT THAT DEMONSTRATES A DEPLOYED BOUNDARY

Path metrics

Number of unapproved production-to-management paths and undocumented dependencies found during validation.

Privilege metrics

Privileged accounts, exceptions, supplier-access revocation time and completion of access reviews.

Recovery metrics

Tested log delivery, firmware currency, time to reach BIOS and evidence from planned recovery exercises.

Use the first controlled exercise as a baseline. Do not invent a pre-deployment improvement percentage.

Start with an assessment. Bring a network diagram, critical-server list, console interfaces, authentication requirements and recovery objectives. Ask for a KG0016/KG0032 and CC2000 demonstration that proves isolation, constrained privilege, audit visibility and an approved recovery task.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

CONCLUSION

A Governed, Recoverable Management Plane

Critical infrastructure needs a management path that remains available when ordinary production access cannot be trusted. The ATEN Air-Gap approach gives teams a practical framework: physically separate the management plane, govern the people and software that operate it, and prove the recovery workflow against the systems that matter most.

> **"The air-gap advantage is not a marketing absolute. It is an architecture that reduces reachable administrative paths and preserves a trusted route to recovery—when the boundary is designed, governed and tested."**

THE EXECUTIVE CHECKLIST

1. Separate the path

Keep production traffic, protected KVM management services and administrator access within explicitly defined trust zones.

2. Govern privileged operation

Apply named roles, supported identity controls, current cryptography, logging, recording where required and change control for virtual media.

3. Rehearse recovery

Validate the actual system—not just its architecture diagram—through controlled tests of separation, failure, recovery and evidence.

READY TO SECURE YOUR CRITICAL INFRASTRUCTURE?

Ask ATEN UK for an Air-Gap architecture assessment.

We can help shape a solution-design workshop around:

- Critical-system and console-interface inventory
- KG0016 / KG0032 density and KVM adapter compatibility
- Protected management switching, resilient hosting and access paths
- CC2000, optional CCVSR, eco DC and power-management scope
- Identity, audit, recovery and commissioning requirements

ATEN UK
01753 539121
sales@aten.co.uk
www.aten.com/gb/en

Product capabilities depend on deployed model, firmware, software release, compatible devices, licensing and regional specification. Confirm the proposed configuration before purchase and publication.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

ATEN PRODUCT PORTFOLIO

ATEN “KG” Series for Datacentre Security

Choose the KVM density that fits the estate, then apply the same protected-management architecture. KG0016 and KG0032 use compatible KVM adapters at the server side; validate video, USB, client and console compatibility for each system before deployment. [5] [6]



KG 0032

32-Port KVM over IP OmniBus Gateway (DigiKVM™)

For higher-density critical estates. ATEN’s current specification table lists 32 KVM ports and 32 remote console connections in a 1U platform. Use the protected management-plane design to keep its IP interfaces within the approved trust zone.

32 KVM ports | 1U | FIPS 140-3 | Panel Array Mode | Dual 10G interfaces | Dual power



KG 0016

16-Port KVM over IP OmniBus Gateway (DigiKVM™)

For compact and mid-scale server rooms. The same architectural considerations apply: isolated cabling and switching, named administrators, carefully governed virtual media and tested recovery access.

16 KVM ports | 1U | FIPS 140-3 | Panel Array Mode | Dual 10G interfaces | Dual power

COMMON GATEWAY CONTROLS

Identity

RADIUS, LDAP/LDAPS and Microsoft Active Directory integration; user and group permissions. [5] [6]

Access restriction

IP/MAC filtering and constrained source access; validate the exact operating mode. [5] [6]

Protected transport

TLS 1.3 and configurable AES-256 video/virtual-media encryption. Avoid legacy configuration choices such as DES, 3DES or RC4. [5] [6]

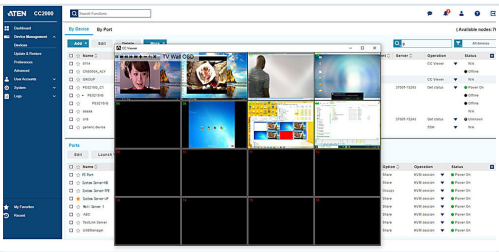
Visibility

Event logging, Syslog destinations and Panel Array Mode for diagnosis. [5] [6]

Selection principle: port count is only the first choice. Size the KVM layer alongside the number of compatible KVM adapters, remote operators, redundant links, power protection, identity dependencies, licensing, audit needs and recovery scenarios.

PANEL ARRAY MODE™ LIVE+ AT A GLANCE

Panel Array Mode available on KG, KN series and through CC2000 management software.



Monitor more. Select one to control.

Panel Array Mode™ Live+ presents livestreamed video feeds from multiple server ports in a configurable multi-screen layout. Operators can scan the estate at a glance, identify a system that needs attention and then select the relevant server for an approved console workflow.

Operational value: faster visual diagnosis across a group of critical systems, while access permissions and the protected management boundary still apply. [5] [6]

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

ATEN PRODUCT PORTFOLIO

Wider KVM Choices for High-Assurance Estates

The Air-Gap architecture centres on a protected management plane. ATEN's wider portfolio can extend the design where control-room workflows, multi-site estates or high-assurance separation requirements call for different form factors or product categories.

KN SERIES

Multi-port KVM over IP

Models including KN1108VA, KN2132VB and KN4064VB offer an 8- to 64-port range, with model-specific concurrent remote sessions, HTML5 WebClient, Panel Array Mode and out-of-band management facilities. Scale and client compatibility must be confirmed by model. [10]

SECURITY & ACCESS FEATURES

High-grade security: TLS 1.3 and an embedded FIPS 140-2 certified OpenSSL cryptographic module (Certificate #4282).
Remote authentication: RADIUS, LDAP, LDAPS and Microsoft Active Directory.
Browser login protection: TLS 1.3 data encryption and RSA 2048-bit certificates.
Source controls: IP / MAC filter support.

8–64 ports | HTML5 client | Panel Array Mode | TLS 1.3 | FIPS 140-2 | IP / MAC filter

SECURE KVM

NIAP PP 4.0 ranges

ATEN secure KVM switches, including CS1188DP4 and PSD PP v4.0 series, are positioned for environments requiring separation between systems at differing trust levels. Evaluate the exact certified configuration, peripheral policy and video requirement. [11] [21]

NATO-listed

Selected ATEN Secure KVM products are listed in NATO's KVM product category. Confirm current inclusion and scope by part number through the NATO catalogue. [26]

NATO listed | NIAP PP 4.0 | USB filtration | Channel isolation

CONSOLE OPERATIONS

Local & control-room access

Console Stations and supported KVM extensions can bring the same operating model closer to the people who need to act. Design human workflows, session ownership and safety procedures alongside the network architecture. [13]

Control-room workflow | Role-based operations | Local resilience

ARCHITECTURE ALIGNMENT, NOT PRODUCT SUBSTITUTION

REQUIREMENT	PRIMARY CONSIDERATION	PROOF POINT
Remote KVM density	Ports, concurrent users and compatible KVM adapters	Connect, authenticate and operate a representative sample of critical systems
Trust separation	Whether separate console channels, peripheral control or distinct system domains are needed	Validate the model and certified/approved operating configuration
Operations workflow	Who monitors, owns and escalates console sessions	Rehearse shift handover, break-glass and supplier-access revocation
Business continuity	Power, network and identity dependencies around each management component	Test recovery when production access is unavailable

Portfolio caveat. Broader KVM products, secure KVM switches, environmental management and power products are adjacent components—not all are automatically part of the core Air-Gap architecture. Confirm the required model, firmware, licence, compatibility and security controls in the proposed design.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

ATEN PRODUCT PORTFOLIO

CC2000: Make Isolated Access Governable

Separate network infrastructure is necessary, but it is not sufficient. Privileged access still needs a clear operating model: a controlled way to discover assets, grant access, monitor status, act on alerts and retain evidence across the management estate.

CC2000 4.0

A single pane of glass for management and access

CC2000 is separately deployed and licensed central-management software—not a capability automatically embedded in a KG gateway. It brings supported KVM over IP devices, serial console servers, intelligent PDUs and other enrolled infrastructure into one secure, unified portal for local and distributed estates. [7]

Instead of moving between individual device interfaces, authorised teams can use one platform to find a managed asset, launch approved access, view its health and act under consistent identity and policy controls.

WHAT THE PLATFORM BRINGS TOGETHER

One operational view—without collapsing trust boundaries

KVM over IP — Remote console access

+

Serial console — Network-device access

+

Intelligent PDU / UPS — Power visibility & control

The dashboard can consolidate device status, events, task results, online users, licensed-node usage and logs, with notification for issues requiring action. [7]

WHAT CC2000 MANAGES

KVM access

Manage supported KVM over IP switches and give authorised teams an organised route to console sessions.

Serial consoles

Bring supported serial console servers into the same portal for network-device and infrastructure access.

Power & environment

Manage supported intelligent PDUs, UPS devices and monitoring data alongside access workflows.

Wider infrastructure

Extend visibility to supported service processors, blade chassis and physical or virtual servers. [7]

BENEFITS FOR SECURITY AND OPERATIONS

Govern privileged access

Use central role-based policies, external identity sources, 2FA, lockout settings and IP/MAC filtering to apply access requirements consistently. [7]

Improve response and visibility

Use the dashboard, event notification, task results and Panel Array capabilities to see what needs attention and reach authorised management functions faster. [7]

Strengthen audit and recovery

Consolidate supported Syslog events and reports; protect backups and test the primary-secondary architecture used for service resilience. [7]

Evidence and recording. CC2000 can consolidate events and generate user, device and port-access reports. Where replayable video evidence of compatible remote sessions is required, CCVSR is a separate product; event logs are not a recording of every operator action. [7] [8]

Boundary statement. CC2000 helps govern the management plane; it does not create physical separation, patch vulnerable applications or guarantee upstream network and identity-service availability. Confirm device support, licence scope, configuration and regional availability for the proposed deployment.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

ATEN PRODUCT PORTFOLIO

CCVSR: Turn Privileged Sessions into Evidence

CCVSR is separately deployed recording software for compatible ATEN KVM over IP switches and serial console servers. It turns privileged access into reviewable evidence by combining live operational monitoring with video-session recording, search and playback. [8]

CONTROL CENTER VIDEO SESSION RECORDER

See access as it happens. Investigate it afterwards.

CCVSR automatically records compatible local and remote sessions from the pre-boot BIOS stage onwards. Recorded sessions can include the video display, keystrokes, mouse clicks and supported audio operations—creating a richer audit trail than a device-event log alone. [8]

It is an independent server deployment, so no recording agent is installed on target computers and their CPU, disk or memory resources are not used for the recording workload.



THE OPERATIONAL VALUE

LiveView supervision

Monitor multiple KVM ports in real time using configurable layouts, so authorised administrators can see active operations and respond to anomalies. [8]

Fast incident investigation

Search captured sessions by time, port name and username, then play back the relevant recording to support problem tracing and review. [8]

Evidence with access controls

Use role and port-level permissions, password-protected video export and central controls to govern who can view or handle recording evidence. [8]

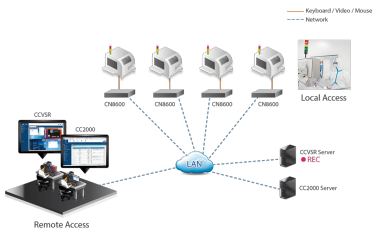
Designed for recording continuity

CCVSR supports a primary-secondary architecture with up to three secondary servers for storage expansion, load balancing and service failover. Define recording retention, protected storage and recovery tests as part of the design. [8]

Protect access to the evidence platform

CCVSR documents IP/MAC filtering, configurable user and group permissions, external authentication options and TLS v1.2 with AES-256-bit support for browser-access protection. Confirm the required configuration before deployment. [8]

WHERE CCVSR FITS



Record compatible console access without changing the target system.

CCVSR sits alongside the supported KVM and serial-console estate, collecting session evidence for authorised review. Use it where the business needs live oversight, auditable access history, investigation support or operational backtracking—not as a substitute for access control, network segmentation or incident response.

Deployment discipline. Validate device compatibility, recording scope, storage sizing, retention, user permissions, export handling and legal or policy obligations before enabling session capture. [8]

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

ATEN PRODUCT PORTFOLIO

Datacentre Power Oversight

Protected console access is only part of a resilient datacentre operating model. Teams also need clear, attributable insight into energy consumption, outlet status and environmental conditions—plus tightly governed options to act when a power or environmental issue threatens critical services.

ECO DC

Turn PDU data into operational visibility

ATEN positions eco DC as its energy and DCIM-management software for qualifying PDU deployments. It brings power distribution, energy and environmental data into a web-based management view, supporting scheduled power operations, detailed reporting and oversight of power use. ATEN UK states that eco DC is included with qualifying ATEN PDU purchases; confirm eligibility and compatibility in the commercial scope. [12]

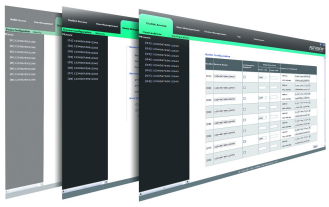
Energy & kWh insight | Scheduled operations | Reporting | DCIM visibility

INTELLIGENT ECO PDU

Measure, monitor and control the rack power layer

ATEN's intelligent PDU range provides models with outlet-level metering and switching, network management, status alerts and sensor connectivity. The PG98330 is a high-density 0U example with 30 outlets, precise kWh metering, environment-sensor support and eco DC integration; select the actual model, feed and outlet type for the installation. [27]

Outlet metering | Switched outlets | Environment sensors | eco DC integration



eco DC: make energy and environment data easier to act on.

Use a consolidated view of qualifying PDU information to identify abnormal consumption, support reporting and plan approved power schedules. The value is not merely a dashboard: it is faster context for an authorised operator to decide whether a change, escalation or investigation is needed.

Selling point: eco DC connects the power layer to a practical management workflow without requiring operators to work through individual PDU interfaces one at a time. [12] [27]

Intelligent PDU: protect and control the power path.

Outlet-level measurements, real-time alerts and environmental-sensor connections help operations teams understand conditions at the rack. Secure power-cord locking, dual LAN ports and PDU cascading are available on selected PG models; validate the required configuration rather than assuming every capability applies to every PDU.

Selling point: a properly specified PDU can improve visibility at the same point where power actions must remain carefully authorised. [27]



POWER-MANAGEMENT CAPABILITIES

Meter at the outlet

Track current, voltage, power factor and kWh where supported, to establish a usable consumption baseline.

Control with purpose

Use remote switching, schedules and sequencing through approved change procedures—not ad hoc convenience commands.

Monitor the environment

Connect compatible sensors for temperature, humidity, airflow, pressure and leak monitoring, with alerts for potential threats.

Scale the rack layer

Use network and cascade capabilities where appropriate; selected PG models support cascades of up to 64 PDUs. [27]

Power-control discipline

Power actions can be disruptive. Define ownership, approvals, timing, rollback plans and incident evidence before enabling remote outlet control. The desired outcome is better context and controlled response—not simply more remote buttons.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

SOLUTION REFERENCE

Complete Solution Summary

ATEN's datacentre portfolio can be combined into a practical operating model: retain a separately protected route to the console, understand the rack power and environment, govern management access centrally, and preserve replayable evidence of privileged activity. Each layer has a distinct job and should be specified, licensed and governed accordingly.

ONE REFERENCE PAGE: FOUR OPERATIONAL LAYERS

01
IP KVM

Protected console access. KG and compatible KVM solutions provide remote video/USB access for approved management and recovery, including BIOS-level workflows where supported. [5] [6]

02
Intelligent PDU & eco DC

Power and environment context. Meter, monitor and control qualifying rack power assets, then use eco DC to bring relevant data into the operational view. [12] [27]

03
CC2000

Central management. Bring supported KVM, serial-console and PDU assets into a unified portal with access policy, dashboard visibility and operational governance. [7]

04
CCVSR

Session evidence. Monitor and record compatible KVM and serial-console sessions for live oversight, investigation and accountable review. [8]

HOW THE LAYERS WORK TOGETHER

Operate
Protected IP KVM console access

Power context
PDU and eco DC insight

Govern
CC2000 policies and management view

Evidence
CCVSR recording and review

Together, these layers help an authorised team operate critical systems, understand rack conditions, apply management policy and retain session evidence. This is a reference architecture, not an assertion that every component must be deployed in every estate or that any single product creates an air gap by itself.

OPERATIONAL RESILIENCE USE CASES

Government & defence
Separate trusted systems, preserve governed console recovery and assess secure KVM choices where assurance requirements apply.

Financial services
Maintain accountable out-of-band administration for core platforms when normal production access is disrupted.

Healthcare
Design recovery access around operational safety, privacy, change approval and continuity requirements.

Utilities & CNI
Combine IT/OT boundary discipline with realistic console compatibility and controlled emergency procedures.

Design and prove the full workflow. Start with critical assets, interfaces, power feeds, approved operators, evidence needs and recovery objectives. Then validate the deployed paths, device compatibility, access controls, licensing, configuration and failure modes in the proposed design.

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en

REFERENCES

Consolidated Sources & Publication Notes

Sources consolidated from the original ATEN Air-Gap white paper and the supplied ATEN Airgap Solution white paper. Sources checked to the stated 2026 edition date. Product capabilities, licensing, certifications and security posture can vary by deployed model, firmware, software release, compatible devices, configuration and region; validate all scope before publication or purchase. ATEN product names and marks belong to their respective owners. Product and interface images are sourced from the original ATEN paper. This white paper does not imply third-party certification or regulatory compliance.

[1] Verizon. 2026 Data Breach Investigations Report executive summary, pp. 5, 9–10.
https://www.verizon.com/business/resources/executivebriefs/2026-dbir-executive-summary.pdf

[2] IBM. Cost of a Data Breach Report 2026, official findings.
https://www.ibm.com/reports/data-breach

[3] CISA et al. Enhanced Visibility and Hardening Guidance, 4 December 2024.
https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

[4] ATEN UK. Air-Gap Solutions.
https://www.aten.com/gb/en/atenukairgapped/

[5] ATEN. KG0016 official product features and imagery.
https://www.aten.com/us/en/products/kvm/kvm-over-ip-switches/kg0016/

[6] ATEN. KG0032 official product features and imagery.
https://www.aten.com/us/en/products/kvm/kvm-over-ip-switches/kg0032/

[7] ATEN. CC2000 4.0 official product features and imagery.
https://www.aten.com/us/en/products/kvm/management-software--control-center/cc2000-4.0/

[8] ATEN. CCVSR video-session recording product.
https://www.aten.com/us/en/products/kvm/management-software--control-center/ccvsr/

[9] ATEN. KG0016 / KG0032 user manual—virtual-media write setting.
https://assets.aten.com/product/manual/kg0016-kg0032-user-manual-w.pdf

[10] ATEN. KVM over IP switches / KN Series official product pages.
https://www.aten.com/gb/en/products/kvm/kvm-over-ip-switches/

[11] ATEN. NIAP PP v4.0 Secure KVM Switches.
https://www.aten.com/global/en/products/kvm/secure-kvm-switches/psd-pp-v4.0-secure-kvm-switches/

[12] ATEN UK. Datacentre / eco DC information.
https://www.aten.com/gb/en/datacentreatenuk/

[13] ATEN UK. Server-room and KVM-over-IP Console Station solution pages.
https://www.aten.com/gb/en/solutions/applications/server-room/

[14] PHP Group. 2026 archive: PHP2Shell advisory and fixed releases.
https://www.php.net/archive/2026.php

[15] NVD. CVE-2026-109618 technical record.
https://nvd.nist.gov/vuln/detail/CVE-2026-109618

[16] NVD. CVE-2026-109619 technical record.
https://nvd.nist.gov/vuln/detail/CVE-2026-109619

[17] CISA. Critical Vulnerabilities in PHP Require Immediate Patching.
https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching

[18] ATEN Global. Security Advisory 40: CVE-2026-109618; assessment also covers CVE-2026-109619 (released 21 October 2026).
https://www.aten.com/global/en/supportcenter/info/security-advisory/40/

[19] UK NCSC. Critical security issue affecting PHP.
https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php

[20] CVE Program. CVE-2024-49714—TeamViewer Remote Client privilege escalation.
https://www.cve.org/CVERecord?id=CVE-2024-49714

[21] NIAP. National Information Assurance Partnership / product-compliance resources.
https://www.niap-ccevs.org/

[22] NIST. Special Publication 800-53 Rev. 5: Security and Privacy Controls.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[23] ISO. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—information security controls.
https://www.iso.org/standard/75652.html

[24] Bank of England. Daily spot exchange rates against sterling; 26 October 2026 observation. Used for illustrative IBM USD-to-GBP conversion only.
https://www.bankofengland.co.uk/boeapps/database/Rates.asp?Travel=NIxAZx&into=GBP

[25] BBC News / Tara Mewawalla. Prepare for supply chain disruption from cyber or climate emergencies, Streeting warns, 22 October 2026.
https://www.bbc.co.uk/news/articles/cwd094x57p32o

[26] NATO Information Assurance Product Catalogue. KVM product category; catalogue notes that approved product information changes over time.
https://www.ia.nato.int/niapc/Category/KVM_52

[27] ATEN. PG98330 30-outlet three-phase outlet-metered and switched eco PDU—official features and specifications.
https://www.aten.com/gb/en/products/power-distribution/rack-pdu/pg98330/

© 2026 ATEN Technology. All rights reserved. | www.aten.com/gb/en