



myDW Health Monitoring Service Whitepaper

Contents

1. Executive Summary	4
2. Industry Challenges	5
2.1 Dispersed Customer Sites and Remote Needs	5
2.2 User Management and Scalability	6
2.3 Cybersecurity and Compliance Requirements.....	6
3. myDW Platform Overview (Technical Framing)	7
3.1 Platform Scope and Design Boundaries.....	7
3.2 Supported Systems and Integration Model	8
3.3 Data Types and Cloud Interaction	8
3.4 User Access and Client Applications	8
4. System Architecture and Data Flow.....	9
4.1 System Registration and Organizational Association.....	9
4.2 Communication Model and Secure Connectivity.....	9
4.3 Telemetry Collection and Health Monitoring.....	9
4.4 Event Handling and Clip Sharing Workflows	10
5. Identity, Authentication, and Access Control.....	11
5.1 Centralized Identity Management	11
5.2 Authentication and Multi-Factor Authentication	11
5.3 Role-Based Access Control and Permission Scope.....	11
5.4 Single Sign-On Across Supported Applications	12
5.5 Access Revocation and Lifecycle Control	12
6. Operational Monitoring, Alerting, and Reporting	13
6.1 Centralized Health Visibility	13
6.2 Alerting and Notification Workflows.....	13
6.3 Proactive Maintenance and Operational Impact	14
6.4 Reporting and Trend Analysis	14
7. Security and Privacy Considerations	15
7.1 Secure Communication and Data Protection	15
7.2 Authentication, Authorization, and Access Control	15
7.3 Data Handling and Privacy Boundaries	15
7.4 Administrative Access and Support Considerations	16
7.5 Cloud Infrastructure and Service Reliability	16
8. Subscription Management and Licensing.....	17



8.1 Organizational Ownership and Administrative Control.....	17
8.2 Subscription Activation and System Association.....	17
8.3 License Keys and Subscription Management	17
8.4 Scalability, Renewal, and Expansion Considerations	18
8.5 Subscription Co-Termination and Continuity Considerations	18
9. Conclusion.....	19

1. Executive Summary

The needs of modern video surveillance environments have grown increasingly distributed and critical to professional and domestic safety. Organizations who manage multiple sites often have customers (e.g., retail, healthcare, education, etc.) who face growing challenges in maintaining system uptime, ensuring camera and recorder health, and enforcing consistent access control. Traditional surveillance deployments, which rely heavily on localized management and reactive maintenance, often lack the centralized visibility and control required for effective operations on an enterprise scale.

myDW is Digital Watchdog's cloud-based health monitoring service that unifies DW recording servers and appliances into a single, online dashboard. Providing a centralized and visible control layer for cloud-optimized recording systems, myDW augments existing deployments with a secure, cloud-hosted management plane that enables proactive health monitoring, centralized user and access management, event visibility, and remote system oversight.

The platform collects operational telemetry, health metrics, and system events from registered devices and securely transmits this data to myDW for visualization, alerting, and reporting. This enables IT and security teams to identify system degradation, device failures, storage risks, and connectivity issues before they result in extended recording gaps or operational downtime.

Security and access control are core design considerations of the myDW platform. User authentication is centralized through a cloud-based identity system with support from Multi-Factor Authentication (MFA), role-based access control, and system-level permissions. This approach reduces credential sprawl, simplifies user lifecycle management, and helps organizations enforce privilege access across distributed surveillance environments. All communication between devices, users, and cloud services is encrypted and protected using security tools and models such as MFA, token-bearing, salt-hashing, minimizing attack surface and simplifying network deployment. Connectivity is established without requiring inbound firewall rules, or open inbound ports, using encrypted, cloud-initiated session management.

myDW introduces a health monitoring solution designed to scale from single-site deployments to large, multi-site organizations managed by IT teams, security operation centers, and managed service providers. By consolidating monitoring, notifications, access control, and system visibility into a single cloud-based interface, the platform reduces operational complexity and improves system reliability, security posture, and response times.

This whitepaper provides a technical overview of the myDW platform, including its architecture, security model, operational capabilities, and deployment considerations. It is intended for IT professionals, security architects, and operations leaders to evaluate cloud-enabled approaches to managing distributed video surveillance systems.

2. Surveillance Industry Challenges

As video surveillance systems expand across multiple locations, they increasingly resemble distributed IT infrastructure rather than isolated security devices. Retail chains, healthcare networks, educational campuses, and security organizations often operate numerous recorders and cameras across geographically dispersed sites, each with varying network conditions, operational requirements, and local constraints. Managing these environments at scale introduces a set of challenges that traditional, site-centric surveillance models struggle to address.

For such cases, the following users may benefit from the myDW platform:

- Security integrators and MSPs who manage separate customer sites.
- Enterprise and multi-site end users (e.g. retail, QSR, banking, logistics, education, healthcare).
- IT and security operations teams who need visibility into system uptime, storage, and camera health.

2.1 Dispersed Customer Sites and Remote Needs

Traditional surveillance deployments rely on localized management and manual health checks. In multi-site environments, this model limits an organization's ability to maintain continuous awareness of system health, camera availability, storage utilization, and system performance across all locations. As a result, failures such as offline cameras, storage degradation, or recording interruptions may go undetected until an incident occurs.

myDW addresses these limitations by introducing a centralized, cloud-based visibility layer for distributed surveillance systems. Operational data from registered recorders is aggregated into a single management interface, enabling administrators to monitor system health across multiple sites without direct onsite access.

Key capabilities include:

- **Centralized Web-Based Monitoring**
The myDW Web Portal provides a unified dashboard for viewing recorder health, storage status, and system connectivity across registered sites. Administrators can access system information, manage subscriptions, and launch recorder web clients from a single interface.
- **Mobile Remote Access**
Compatible mobile applications, such as DW Mobile Plus, extend remote access to live and recorded video streams for supported VMAX and COVA recorders. This enables authorized users to verify system status and review video without requiring local network access.
- **Health Monitoring and Notifications**
myDW continuously monitors system health indicators and generates alerts for conditions such as offline cameras, visual obstructions, failing drives, and storage capacity risks. Notifications are delivered through the web portal and supported



mobile applications, supporting proactive maintenance workflows and faster issue resolution.

2.2 User Management and Scalability

Requirements for onsite investigations to diagnose and resolve issues can create increased operational overhead, service visits, and additional support costs. myDW's organizational structure supports enterprise scaling and compartmentalization of registered sites by assigned administrators.

- **Organizational Structure**
myDW's organizational structure provides a tiered hierarchy and a user interface (UI) for security technicians to prioritize and assign response based on user role; divides myDW user roles into Channel Partner (CP) and End User (EU) levels.
- **Role Management**
myDW users can be assigned Channel Partner (CP), Sub-Channel Partner (Sub CP), or End User (EU) roles, each varying in level of access and user permissions.
- **User Management**
myDW users have individual profiles that organization administrators (CP or EU level) can enable or revoke system permissions and viewing rights without the need for locally managed credentials.

2.3 Cybersecurity and Compliance Requirements

Historically, video surveillance systems were often deployed as isolated physical security tools, managed locally and accessed within trusted networks. As these systems have become network-connected and operationally critical, they are increasingly treated as part of an organization's broader IT and security infrastructure. This shift introduces new expectations around authentication, access control, data protection, and auditability.

Modern IT and security increasingly require surveillance platforms to support centralized identity management, strong authentication mechanisms, and encrypted communication between sites and users.

Surveillance systems and components were often treated as isolated physical security tools. However, they are now recognized as part of network-connected infrastructure that must align with broader cybersecurity policies.

- **Multi-Factor Authentication (MFA)**
myDW uses centralized credential control and encrypted communication to ensure secure endpoints between servers and client connections. When remotely logging in, users must authenticate their access using a unique, temporary code.
- **Private User Data**
Digital Watchdog, its employees and its affiliates do not have access to private user data, system control, or recorded video without direct permission and assistance from system owners.

3. myDW Platform Overview (Technical Framing)

myDW is a cloud-based monitoring platform designed to extend visibility and operational oversight across distributed DW surveillance sites. The platform functions as a centralized management layer for supported cloud-optimized recording systems (e.g., DW Spectrum, VMAX, and COVA), enabling remote system monitoring and user management without replacing or bypassing local recording infrastructure.

myDW is intended to complement onsite recording systems, rather than act as a primary VMS platform. Video is recorded locally on supported recorders, while the operational telemetry, system health data, and event information are securely transmitted to the myDW cloud for aggregation, visualization, and alerts. This design preserves local recording performance and retention policies while enabling centralized oversight across multiple sites.

3.1 Platform Scope and Design Boundaries

To properly evaluate myDW within an IT or security architecture, it is important to clearly define the platform's scope and operational boundaries.

myDW Does Provide:

- Centralized visibility into recorder health, camera connectivity, storage utilization, and system status
- Cloud-based user and access management across registered systems
- Cloud-based clip storage
- Event alerts and reporting
- Secure access to DW Mobile Plus clients

myDW Does Not:

- Replace local video recording or storage
- Require continuous cloud video streaming
- Function as a general-purpose video analytics engine
- Require inbound network access to onsite recorders

By maintaining a clear separation between local recording operations and cloud-based management functions, myDW minimizes operational disruption and reduces architectural risk when introduced into existing surveillance environments.



3.2 Supported Systems and Integration Model

myDW integrates with supported Digital Watchdog recording platforms using native plugins and built-in cloud configuration options, depending on the recorder model and software version.

Supported Systems Include:

- DW Spectrum Professional Servers
- DW VMAX G4 Recorders
- DW COVA Recorders

Once registered, each system is associated with an organization within myDW. Registration occurs within the server/recorder's user interface and establishes a secure communication path between the recorder and the cloud, allowing system health data and event information to be collected without exposing the recorder to direct inbound connections.

3.3 Data Types and Cloud Interaction

myDW is designed to collect and process operational data rather than full video streams. Data transmitted to the myDW cloud include:

- Recorder and camera health metrics
- Storage utilization and capacity indicators
- System status and connectivity events
- User-initiated event and clip metadata

Video recordings remain stored locally on the recorder/server. When video clips are explicitly shared through myDW workflows, selected clips can be uploaded to cloud storage for controlled access and sharing. This approach limits cloud data exposure while enabling secure event sharing when required.

3.4 User Access and Client Applications

Authorized users access myDW through a web-based portal. The platform serves as a centralized entry point for system visibility and management, while integrating with existing DW client software for live viewing and playback.

Single Sign-On (SSO) is supported with DW Mobile Plus, allowing users to authenticate once and view video streams from their VMAX G4 or COVA series recorders without managing separate credentials. This model simplifies access management and reduces credential sprawl across distributed surveillance environments.

4. System Architecture and Data Flow

The myDW platform is designed to introduce centralized monitoring and management capabilities into distributed surveillance environments without disrupting local recording operations or requiring invasive network changes. This section describes how systems are registered, how data flows between components, and how operational information is processed and presented to users.

4.1 System Registration and Organizational Association

Supported recording systems are registered to an organization within myDW using a recorder-specific plugin or built-in cloud configuration option via recorder firmware. During registration, each system is logically associated with an organization and can apply user roles and access control policies.

Registration establishes a secure communication relationship between the recorder and the myDW cloud services. Once registered, the recorder becomes visible within the organization's online dashboard and can participate in health monitoring.

This organizational association enables multi-site environments to be managed as a single logical deployment while preserving separation between different customers, business units, or administrative domains.

4.2 Communication Model and Secure Connectivity

After registration, recorders periodically transmit operational telemetry and system status information to the myDW cloud over encrypted connections. Data exchanged between recorders and the myDW cloud is limited to information required for system visibility, alerts, and event management. Local recording operations continue independently, and recorders remain functional in the event of temporary cloud connectivity interruption.

By centralizing monitoring and management functions in the cloud while keeping recording and storage local, the architecture reduces exposure of onsite systems and simplifies deployment in environments with restrictive firewall policies.

4.3 Telemetry Collection and Health Monitoring

myDW collects operational telemetry from registered systems to provide insight into the health and status of surveillance infrastructure. Collected data includes:

- Recorder operational status and health
- Camera connectivity and availability
- Storage utilization and capacity indicators
- System performance metrics (CPU and memory)
- Current recorder firmware version



This telemetry is aggregated within the myDW cloud to generate dashboards, reports and alerts. Administrators can view the status of individual systems or assess trends across multiple sites, supporting proactive maintenance and site planning.

Alert rules can be configured to notify users when defined conditions are met, such as device failures, storage risks, or changes in camera status. Notifications are delivered through the myDW Web Portal and the DW Mobile Plus application.

4.4 Event Handling and Clip Sharing Workflows

In addition to system health telemetry, myDW supports centralized handling of events generated by connected recording systems.

When users initiate clip sharing, selected video clips may be uploaded from local recorders to secure cloud storage for controlled access and distribution. These workflows are user-driven and do not require continuous cloud video streaming. Access to shared clips is governed through user permissions, organizational access controls, and set time limits for viewing.

This model enables secure collaboration and incident response workflows while maintaining local control over primary video storage.



5. Identity, Authentication, and Access Control

As surveillance systems become integrated into broader IT environments, effective identity and access management are essential to maintaining security, operational consistency, and regulatory alignment. Distributed deployments that rely on locally managed credentials and ad-hoc user provisioning often struggle to enforce consistent access policies or quickly revoke access when roles change.

myDW addresses these challenges by centralizing identity, authentication, and authorization within a cloud-based access management model designed for distributed surveillance environments.

5.1 Centralized Identity Management

User identities within myDW are managed centrally at the organizational level rather than on individual recorders. Users are invited to an organization by an Organization Administrator and assigned roles that determine their level of access across registered systems. This approach eliminates the need to create and manage local user accounts on each recorder and reduces the risk of configuration drift or orphaned credentials.

Centralized identity management enables administrators to:

- Onboard users consistently across multiple systems and sites
- Modify access permissions as roles change
- Revoke access immediately without accessing individual recorders
- Maintain clearer visibility into who has access to which systems

5.2 Authentication and Multi-Factor Authentication

myDW uses a centralized authentication mechanism to verify user identities before granting access to platform resources. Authentication policies can include Multi-Factor Authentication (MFA), adding an additional layer of protection beyond username and password credentials.

By enforcing MFA at the platform level, organizations can apply consistent authentication requirements to registered systems. This reduces the reliance on locally enforced security controls and helps align surveillance access with broader organizational cyber security policies.

5.3 Role-Based Access Control and Permission Scope

Access within myDW is governed by role-based access control (RBAC), allowing organizations to define and enforce permissions based on user responsibilities. Roles determine what actions users can perform, what systems they can access, and what information they can view or manage.



myDW supports hierarchical role structures that distinguish between channel partners, sub-channel partners, and end users, as well as recorder-level permission scoping. This enables fine-grained control over access in environments where multiple organizations, customers, or administrative domains are managed within a single platform.

Role-based controls help organizations:

- Enforce access privileges
- Limit administrative actions to authorized personnel
- Segregate and assign alerts across operational and security roles
- Reduce accidental or unauthorized configuration changes

5.4 Single Sign-On Across Supported Applications

myDW supports single sign-on (SSO) with compatible DW applications, allowing users to authenticate once and access multiple tools without managing separate credentials for multiple sites.

Centralized authentication also simplifies auditing and access reviews by consolidating identity information into a single system, rather than distributing credentials across individual recorders and client applications.

5.5 Access Revocation and Lifecycle Control

Effective access control includes not only granting permissions but also revoking them when no longer required. myDW allows administrators to disable or remove user access at the organizational level, immediately affecting all associated systems and services.

This centralized lifecycle control supports:

- Rapid response to personnel changes
- Reduced exposure from inactive or unused accounts
- Improved alignment with internal security policies and access review processes

6. Operational Monitoring, Alerting, and Reporting

Maintaining reliable video surveillance across distributed environments requires continuous visibility into system health and timely response to operational issues. In the absence of centralized monitoring, organizations often rely on manual checks or user-reported failures, increasing the likelihood of undetected outages, recording gaps, and prolonged downtime.

myDW introduces a centralized operational monitoring model that aggregates system health data across registered devices and presents actionable information through dashboards, alerts, and reports. This enables IT and security teams to shift from reactive troubleshooting to proactive system management.

6.1 Centralized Health Visibility

myDW continuously collects operational telemetry from registered recording systems to provide real-time insight into the status of surveillance infrastructure. Health data is aggregated and presented through a centralized interface, allowing administrators to assess system availability and performance across multiple sites without accessing individual recorders.

Monitored health indicators may include:

- Recorder operational status
- Camera connectivity and availability
- Storage utilization and capacity thresholds
- System performance and service state indicators
- Connectivity-related events

By consolidating this information into a single management plane, myDW reduces the operational effort required to maintain situational awareness across distributed deployments.

6.2 Alerting and Notification Workflows

Operational monitoring is most effective when issues are surfaced automatically and routed to the appropriate personnel. myDW supports configurable alerting workflows that notify users when defined conditions or thresholds are met.

Alerts can be generated for conditions such as:

- Offline or unreachable cameras
- Storage capacity risks or disk health issues
- Recorder availability changes
- Visual obstructions or changes in camera view



- System or service interruptions

Notifications are delivered through the myDW Web Portal and supported client applications, enabling administrators and operators to respond quickly regardless of location. Alert configurations can be tailored to align with operational schedules, maintenance windows, or organizational priorities.

6.3 Proactive Maintenance and Operational Impact

By detecting issues early and centralizing alert delivery, myDW supports proactive maintenance workflows that reduce operational disruption. Administrators can address developing issues—such as declining storage capacity or intermittent device connectivity—before they result in recording gaps or service outages.

This proactive model contributes to:

- Reduced mean time to detection (MTTD)
- Faster mean time to resolution (MTTR)
- Fewer on-site service visits
- Improved system uptime and reliability

For organizations managing large or geographically dispersed deployments, centralized monitoring enables more efficient use of technical resources while improving overall service quality.

6.4 Reporting and Trend Analysis

In addition to real-time monitoring, myDW supports the generation of operational reports based on collected health and event data. Reports provide historical visibility into system performance, device availability, and operational trends across sites.

Reporting capabilities support:

- Ongoing system health reviews
- Capacity planning and storage forecasting
- Documentation of operational status over time
- Support for service-level objectives or internal compliance requirements

By retaining historical operational data in a centralized system, organizations gain the ability to identify recurring issues, assess long-term trends, and make informed decisions about system maintenance and expansion.



7. Security and Privacy Considerations

As surveillance systems become increasingly integrated into enterprise networks, their security posture and data handling practices are critical considerations for IT and security teams. myDW is designed to support centralized monitoring and management while maintaining clear security boundaries between cloud services, onsite recording systems, and user access.

This section outlines key security and privacy considerations relevant to organizations evaluating myDW within regulated or security-conscious environments.

7.1 Secure Communication and Data Protection

Communication between registered recording systems, client applications, and the myDW cloud is protected using encrypted channels. This ensures that operational telemetry, system status information, and user interactions are protected from unauthorized interception or modification while in transit.

By limiting cloud communication to management and monitoring data rather than continuous video streams, the platform reduces the volume and sensitivity of data transmitted outside the local environment.

7.2 Authentication, Authorization, and Access Control

Access to the myDW platform is governed by centralized authentication and role-based authorization mechanisms. User access is restricted based on assigned roles and scoped permissions, supporting least-privilege access across distributed environments.

Multi-Factor Authentication (MFA) can be enforced to reduce the risk of credential compromise. Centralized user lifecycle management enables administrators to quickly revoke access when roles change or access is no longer required.

These controls help reduce common risks associated with distributed surveillance deployments, such as unmanaged credentials, inconsistent access policies, and delayed access revocation.

7.3 Data Handling and Privacy Boundaries

myDW is designed to minimize exposure of recorded video and sensitive system data. Primary video recording and long-term storage remain local to the recorder, under the control of the system owner.

Operational data collected by the platform is limited to information required for monitoring, alerting, and event management. When users explicitly initiate clip-sharing workflows, selected video clips may be uploaded to cloud storage for controlled access and distribution.



Access to cloud-stored clips is governed by organizational permissions and user roles. Clip sharing is an intentional, user-driven action rather than an automated or continuous process.

7.4 Administrative Access and Support Considerations

Administrative access to surveillance systems is controlled by the organization's assigned roles and permissions. myDW does not require routine administrative access by the platform provider to customer systems.

Digital Watchdog employees, agents, and affiliates do not have access to private user data or systems. Directly expressed access must be provided by a myDW Organization Administrator for DW to have access to Channel Partner or End User data.

When technical support is requested, access is performed under the direction of the system owner and within the scope required to address the issue. This model helps organizations maintain control over their environments while still enabling effective support workflows.

7.5 Cloud Infrastructure and Service Reliability

myDW is hosted on secure cloud infrastructure designed to support high availability and operational resilience. Cloud services are monitored for performance and availability, and platform status visibility is provided to users through public status resources.

By centralizing monitoring and management functions in the cloud while preserving local recording autonomy, the platform balances reliability with operational independence at the site level.

8. Subscription Management and Licensing

myDW is delivered as a cloud-based subscription service, with licensing and entitlements managed at the organizational level. This model enables administrators to control system access, capacity, and service activation centrally, without requiring changes to recorder-level configurations or local user accounts.

Subscription management is designed to align operational control with organizational responsibility, supporting scalable deployments across single-site and multi-site environments.

8.1 Organizational Ownership and Administrative Control

Subscriptions within myDW are associated with an organization and managed by designated organization administrators. These administrators are responsible for assigning entitlements, activating subscription keys, and maintaining visibility into subscription status across registered devices.

Centralized subscription ownership allows organizations to:

- Track active subscriptions and licensed capacity across sites
- Maintain clear administrative accountability
- Prevent unauthorized system activation or use
- Align service usage with internal governance policies

This approach supports both end-user organizations and channel partners managing multiple customer environments.

8.2 Subscription Activation and System Association

myDW subscriptions are activated through administrator-controlled workflows that associate licensed device capacity with specific recording systems. Once activated, entitlements enable monitoring, management, and supported cloud services for the associated system.

Subscription activation does not alter local recording behavior or storage policies. Instead, it enables participation in myDW's cloud-based workflows such as health monitoring, alerting, and centralized user access.

By separating licensing controls from recorder configuration, myDW simplifies system onboarding and reduces the risk of misconfiguration during deployment.

8.3 License Keys and Subscription Management

Administrators can generate and manage subscription keys or entitlements within the myDW platform. These keys are used to associate licensed services with eligible recording systems and to control the scope of enabled features.



Entitlement management supports:

- Allocation of licensed capacity to specific systems or sites
- Reassignment of licenses as deployments change
- Expansion of capacity as additional cameras or systems are added
- Renewal of subscriptions without disrupting active systems

This centralized model enables organizations to adapt their surveillance infrastructure over time while maintaining consistent administrative oversight.

8.4 Scalability, Renewal, and Expansion Considerations

The subscription-based licensing model is designed to support incremental scaling as operational needs evolve. Organizations can expand licensed capacity or extend service terms without redesigning their deployment or modifying existing access controls.

Renewal and expansion workflows are handled at the organizational level, ensuring continuity of service while preserving existing system associations and user permissions.

By treating licensing as an administrative layer rather than a device-level dependency, myDW supports long-term scalability and operational continuity in distributed environments.

8.5 Subscription Co-Termination and Continuity Considerations

myDW subscriptions are provisioned for defined service terms and are tracked at the organizational and entitlement level. Active subscriptions enable access to cloud-based monitoring, management, and reporting capabilities for associated systems.

Subscription status does not affect local recording operations or onsite video storage. In the event of a subscription expiration, access to cloud-based services may be limited until the subscription is renewed, while local system functionality remains unchanged.

Organizational administrators are responsible for monitoring subscription status and ensuring timely renewal to maintain uninterrupted access to cloud-based capabilities. This model allows organizations to manage service continuity without introducing risk to core recording operations.

myDW uses a Subscription Co-Termination model to determine the validity period of an organization's subscription. Multiple licenses can be applied to create a single, common expiration date, simplifying management and budgeting for businesses by consolidating renewals into one annual event.



9. Conclusion

As video surveillance environments continue to expand in scale and complexity, organizations must manage them with the same rigor applied to other forms of distributed IT infrastructure. Maintaining visibility, availability, and security across multiple sites requires centralized oversight, consistent access control, and proactive operational management—capabilities that traditional, site-centric surveillance models were not designed to deliver.

myDW introduces a cloud-based management and monitoring layer that addresses these challenges while preserving the autonomy and performance of local recording systems. By separating recording operations from centralized visibility, identity management, and operational workflows, the platform enables organizations to modernize their surveillance infrastructure without disrupting existing deployments or network architectures.

Through centralized identity and access control, proactive health monitoring, secure event workflows, and organization-level governance, myDW supports improved operational reliability and reduced administrative overhead across distributed environments. Its architecture aligns with modern security principles, including privilege access, encrypted communication, and controlled data exposure, making it suitable for integration into security-conscious and regulated environments.

For IT leaders, security teams, and operational stakeholders, myDW provides a structured approach to managing surveillance systems as part of the broader enterprise technology ecosystem. By improving visibility, consistency, and control, the platform enables organizations to reduce operational risk while supporting scalable growth and long-term system resilience.

For More Information or Technical Support

DW Technical Support: <https://www.digital-watchdog.com/contact-tech-support/>

DW Sales: sales@digital-watchdog.com | www.digital-watchdog.com

