Security, Privacy, and Compliance with the Smartvue® Cloud

White Paper
Executive Summary

The adoption of cloud services worldwide continues to accelerate, yet many organizations are wary of trusting a third party with their video surveillance data, security applications, and visual business intelligence infrastructure. Smartvue® Cloud helps customers achieve the economic benefits of cloud services while furthering security and compliance through:

- **Experience** providing trustworthy software and services, resulting in a foundation on which customers can easily run their own secure and compliant solutions.

- **Transparency** and third-party verifications to provide insight into Smartvue security controls and confidence that compliance standards are being met.

With Smartvue Corporation, organizations benefit from over a decade of experience in cloud video surveillance and our partnership with Microsoft for an industry-leading approach to cloud video security, privacy, and compliance while minimizing cost and complexity.
Introduction: The Advantages of the Right Cloud Video Services

According to an IDC study, 70% of CIOs will embrace a cloud-first strategy in 2016, meaning they will consider cloud-based delivery the preferred choice when implementing new services. Organizations are adopting cloud computing at this rapid pace to achieve speed, scale, and economic benefits. Smartvue Cloud is a cloud service that helps organizations deploy superior video surveillance and visual business intelligence by providing a simple to use platform with global scale and enterprise-grade reliability as well as unmatched speed. Customers can instantly provision video surveillance and visual business intelligence on a camera by camera or server by server basis, and save money with monthly billing and built-in auto-scaling to meet changing requirements.

Smartvue can also help reduce the cost, complexity, and risk associated with security and compliance. A survey conducted by ComScore demonstrates that while many organizations have initial concerns about moving to the cloud, a majority of cloud adopters achieve significant security benefits:

Few organizations can replicate the technology and operational processes that the Smartvue Cloud uses to help safeguard enterprise services and comply with a wide range of international standards. When companies use Smartvue Cloud, they benefit from Smartvue and Microsoft’s scale and experience running highly secure and compliant online services around the globe. This partnership delivers the stability and reliability to which customers can trust their most critical enterprise surveillance and visual intelligence requirements.

1 (IDC CIO Agenda webinar)
**Expertise, Partnership, and Transparency**

**Expertise through Experience**

Smartvue Cloud runs on the Microsoft Azure platform because Microsoft has decades of unmatched experience building enterprise software and running some of the largest online services around the globe. Today, the Microsoft cloud infrastructure supports over 1 billion customers and 200 million businesses running in 76 markets worldwide. Microsoft has leveraged this expertise to create and implement industry-leading secure software development, operational management, and threat mitigation practices, helping it to deliver services that achieve higher levels of security, privacy, and compliance than most customers could achieve on their own.

**Microsoft experience**

- MS Cloud Infrastructure supports over **1 billion** customers, **200 million** businesses running in **76** markets worldwide
- Windows Azure itself has **240 million** user accounts from companies & organizations in **127 countries**
- Windows Azure cloud storage which holds more than **4 trillion** objects and handles on average **270,000** requests/second, with a peak of **880,000** requests/second.

**Sharing Responsibility**

Smartvue believes that security, privacy, and compliance for its enterprise cloud services are a shared responsibility. Smartvue helps reduce the security and compliance burden for customers by providing trustworthy enterprise cloud services, while also offering the security capabilities and flexibility customers need to use the services in accordance with their own standards.
Transparency and Independent Verification

Smartvue Cloud undergoes regular verification by third-party audit firms through Microsoft and Smartvue shares audit report findings and compliance packages with customers to help them fulfill their own compliance obligations. By verifying that its services meet compliance standards and demonstrating how compliance was achieved, Smartvue makes it easier for customers to attain compliance for the infrastructure and applications they run utilizing Smartvue Cloud Services.
How Smartvue Helps Keep Video Surveillance Data Safe

Design and Operational Excellence

Smartvue security, privacy, and compliance begin with a trustworthy technology foundation. Smartvue and Microsoft create, implement, and continuously improve security-aware software development, operational, and threat mitigation practices. This helps customers reduce the time and money they spend on implementing and maintaining the security of their computing platform.

Security Centers of Excellence. Microsoft engages in industry-leading security efforts through the creation of centers of excellence, including the Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center.

Designing for security from the ground up. Microsoft development adheres to the Security Development Lifecycle (SDL). The SDL became central to Microsoft’s development practices a decade ago and is shared freely with the industry and customers. It embeds security requirements into systems and software through the planning, design, development, and deployment phases.

Keeping operations safe. Smartvue adheres to a rigorous set of security controls that govern operations and support. The Smartvue team works with other entities within Microsoft such as the Microsoft Operational Security Assurance (OSA) group to identify risks and share information, supporting continuous improvement in operational controls. This increases the ability to prevent, detect, contain, and respond to operational security threats.

“We don’t have to worry about data center infrastructure. (They take care of) maintenance tasks so we can focus on what we do best—designing innovative mailing solutions.”

- Paul Aronson, Director of Engineering, Pitney Bowes
Assume breach. One key operational best practice that Smartvue leverages is known as the “assume breach” strategy. A dedicated “red team” of software security experts simulates real-world attacks at the network, platform, and application layers, testing the ability to detect, protect against, and recover from breaches. By constantly challenging the security capabilities of the service, Smartvue and Microsoft can stay ahead of emerging threats.

Incident response. Smartvue, through its partnership with Microsoft, has a global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity. The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces internally and externally to its customers.

Infrastructure Protection

Smartvue Cloud infrastructure includes hardware, software, administrative and operations staff, and physical data centers from Microsoft. Smartvue addresses security risks across its infrastructure with continuous intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. With Smartvue, customers can reduce the need to invest in these capabilities on their own and benefit from economies of scale in the Microsoft datacenter infrastructure.

24-hour monitored physical security. Microsoft data centers are physically constructed, managed, and monitored 24 hours a day to shelter data and services from unauthorized access as well as environmental threats.

Monitoring and logging. Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Smartvue environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Patch management. Security patches help protect systems from known vulnerabilities. Integrated deployment systems manage the distribution and installation of security updates for Smartvue.
**Anti-Virus/Anti-Malware protection.** Microsoft Anti-malware is an integrated part of Smartvue Cloud Services and helps identify and remove viruses, spyware and other malicious software and provide real time protection.

**Intrusion detection/Distributed Denial of Service (DDoS) Defense.** Smartvue Cloud uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to protect against DDoS attacks. The Smartvue Cloud DDoS defense system is designed to withstand attacks from outside the system as well as attacks staged by other customers.

**Penetration testing.** Smartvue and Microsoft conduct regular penetration testing to improve security controls and processes. Customers can carry out their own authorized penetration testing on the Smartvue Cloud.

**Network Protection**

Microsoft blocks unauthorized traffic to and within the global Smartvue Cloud data centers using a variety of technologies such as firewalls, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces.

**Network isolation.** Network isolation prevents unwanted tenant-to-tenant communications, and access controls block unauthorized users from the network. Smartvue Cloud does not receive inbound traffic from the Internet unless specifically configured to do so.

**Encrypting communications.** Built-in cryptographic technology enables encrypted communications within Smartvue deployments, between Smartvue regions, and from Smartvue to on-premises data storage. Access to the Smartvue Cloud is encrypted using HTTPS.

**Using Express Route.** Customers can optionally select the Smartvue Cloud Express Route private fiber link into the Smartvue Cloud data centers to keep their traffic off the Internet.
Identity and Access

Smartvue offers its own secure and custom user database with custom groups for privileges and access. Optionally customers can control access to their video surveillance using a comprehensive and federated identity and access management solution from Microsoft called Active Directory. It helps customers simplify the management of video security and control user access across applications.

Enterprise cloud directory. Active Directory is a comprehensive identity and access management solution in the cloud and works with the Smartvue Cloud. It combines core directory services, advanced identity governance, security, and application access management.

Access monitoring and logging: Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Smartvue and Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Smartvue also uses third-party monitoring tools to detect additional threats and manage cloud performance. Customers can request reports from Smartvue that provide information about user access to their environments.

“We are delivering greater value because we are able to cut down on costs, (and) complexity, by taking advantage of Active Directory.”

– Rick Hinton
Vice President Products
Portal Solutions
Data Protection

Both technological safeguards, such as encrypted communications, and operation processes help keep Smartvue Cloud video data secure.

Data in transit. Smartvue uses industry-standard transport protocols such as SSL and TLS between Smartvue cameras, Smartvue servers and the data centers, and within the data centers themselves.

Data at rest. Recorded Smartvue Cloud video data can optionally be secured using 256 bit SHA key to insure the video is not tampered with after recording.

Data segregation and private cloud. Smartvue offers a multi-tenant service, meaning that multiple customers’ deployments are stored on the same physical hardware. Smartvue Cloud uses logical isolation to segregate each customer’s data from that of others. This provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another’s data. Optionally Smartvue offers a private cloud service for a unique cloud instance for each customer.

Data destruction. When video is deleted, Smartvue follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware.

Privacy

Smartvue recognizes that cloud services raise unique privacy challenges for businesses. That is why it implements strong privacy protections in services and makes commitments to safeguard the privacy of customer data. In addition, Smartvue provides customers with visibility into who has access to it and optionally where it resides.

“Smartvue offers the fastest, easiest and most secure cloud video surveillance platform in the market today.”

- Robert Harper CEO, ACS Security Integrations USA
**Privacy by Design.** With Smartvue and Microsoft, customers can expect Privacy by Design, a policy that guides building of products and services, how services are operated, and how internal teams are organized.

**Contractual commitments.** Smartvue is unique among the major cloud providers in offering cloud-service-specific privacy statements and strong contractual commitments to safeguard customer data and protect privacy. Smartvue makes the standard contractual clauses created by the European Union (“EU Model Clauses”) available to enterprise customers to provide additional contractual guarantees concerning transfers of personal data.

**Control over data location.** For many customers, knowing and controlling the location of their data can be an important element of data privacy compliance and governance. Smartvue customers can specify the geographic areas where their customer data is stored. Data may be replicated within a geographic area for redundancy, but will not be transmitted outside it. For more information, including exceptions to this policy, see the Azure Trust Center.

**Restricted data access and use.** Access to customer video data by Smartvue personnel is restricted. Customer Data is only accessed when necessary to support the customer’s use of Smartvue software or services. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of Smartvue and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is carefully controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. Options which prevent all access to video by Smartvue, resellers, partners and anyone except the end user using unique tokens, premise IDs and MAC address system are also available.

**“Smartvue is by far the best cloud video surveillance product on the market.”**

— Andy Rubin
Senior VP at Google,
Founder & CEO of Android
No use for advertising. Smartvue does not share Customer Data with advertiser-supported services, nor is customer data mined for advertising.

Compliance

Smartvue maintains a team of security, privacy, and compliance experts who help customers meet their own compliance obligations. The compliance team also represents the “customer voice,” working with Smartvue engineering and operations teams as well as external regulatory bodies to help ensure customers’ needs are met.

Smartvue and Microsoft invest heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve.

The Smartvue and Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Smartvue and Microsoft to maintain and expand a rich set of third-party certifications. These help demonstrate compliance readiness to customers, auditors, and regulators. As part of its commitment to transparency, Smartvue and Microsoft share third-party verification results with customers.

The Smartvue Cloud through Microsoft is certified for ISO 27001, a broad international information security standard, and undergoes annual audits for ISO compliance. The Smartvue Cloud through Microsoft has also been audited against the Service Organization Control (SOC) reporting framework for SOC 1 Type 2, attesting to the design and operating effectiveness of its controls. In addition, the Smartvue Cloud through Microsoft has been audited for SOC 2 Type 2, which includes a further examination of Smartvue controls related to security, availability, and confidentiality. Microsoft undergoes annual SOC audits.
The Smartvue Cloud through Microsoft is also available with many industry-specific certification options, including:

- **Payment Card Industry (PCI) Data Security Standard (DSS):** The Smartvue Cloud through Microsoft is available as validated for PCI-DSS compliance by an independent Qualified Security Assessor (QSA). Designed to help prevent fraud through increased controls involving credit card data, certification is required for all organizations that store, process, or transmit credit card information. Customers can reduce the complexity of their PCI-DSS certification by using compliant services.

- **United States FedRAMP:** The Smartvue Cloud through Microsoft is available with Provisional Authorization to Operate from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB), having undergone the assessments necessary to verify that it meets FedRAMP security standards.

- In the **United Kingdom**, Microsoft has been awarded **Impact Level 2 (IL2)** accreditation, further enhancing Microsoft and its partner offerings on the current G-Cloud procurement Framework and CloudStore.

- **Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH):** To help customers comply with HIPAA and HITECH Act security and privacy provisions, the Smartvue Cloud through Microsoft is available under a HIPAA Business Associate Agreement (BAA) to healthcare entities with access to Protected Health Information (PHI).

For more details on the scope of compliance certifications, visit the Azure Trust Center. It is important to note that Microsoft generally treats verifications as a baseline and frequently goes far beyond them in its commitment to deliver trustworthy, compliance-ready services.

**Cloud Security Alliance.** Microsoft participates in industry-wide transparency initiatives, especially through its association with the Cloud Security Alliance (CSA). An independent industry organization, the CSA has developed a controls framework called the Cloud Controls Matrix (CCM). The CCM
provides organizations with a standards-based, industry-vetted, framework that incorporates cloud services. Microsoft publishes information about how it addresses the CSA CCM in the publicly accessible CSA Security, Trust & Assurance Registry (STAR).

Cloud Risk Assessment Tools, Smartvue customers have access to tools that help them achieve compliance on their own terms such as the Cloud Risk Decision Framework and Cloud Risk Assessment models, both of which are based on the globally-recognized Enterprise Risk Management standard ISO 31000. Organizations wishing to evaluate their IT security state, evaluate the benefits of cloud computing, and plan for adoption can use the Cloud Security Readiness Tool. Using the answers to a few short questions, it generates a report tailored to the needs of the organization.

For more information, read the white paper “The Microsoft Approach to Cloud Transparency.”
Transform Video Security and Compliance with the Smartvue Cloud

Smartvue Cloud provides a deep, tenured commitment to security, privacy, and compliance, which helps Smartvue customers maximize the security and compliance benefits of the cloud. Smartvue delivers a trusted platform that enables companies to move to the cloud more quickly while leveraging years of expertise to reduce risk.