InterVision
INNOVATION DELIVERED

Cloud Solutions

Cloud Security

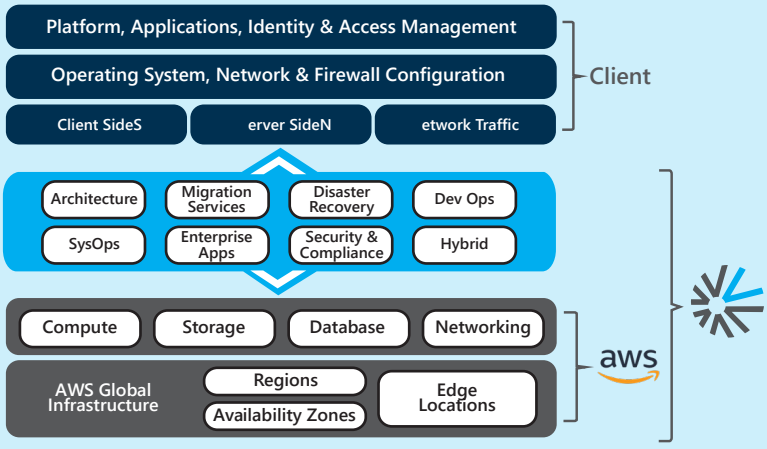
Protect Your Business-Critical Assets in the Cloud

Organizations today face a myriad of cybersecurity threats with real business impacts. Moving IT systems to the cloud can enhance security but understanding how to capitalize on the scale, compliance and capabilities of the cloud involves a shared responsibility posture. Our deep bench of cloud and on-premise security experts collaborate with you to design and implement a multi-layered security environment. Combined with broad capabilities for SIEM, DevSecOps and compliance, we deliver cloud security that simplifies risk management for optimum availability.

A Comprehensive Security Strategy

The flexibility of cloud enables security solutions to easily scale alongside your environment as it grows or shrinks. InterVision and Cloud Service Providers (CSPs) (AWS, Azure, etc.) manage the underlying infrastructure and clients secure the applications, infrastructure and data using a multitude of built-in security features of the cloud. Leveraging a partner in conjunction with a CSP affords you the confidence that you are fully leveraging the CSP's security capabilities, while simultaneously securing the non-CSP parts of your environment, including your organization's network, users and data. This shared-responsibility model allows clients to manage many familiar areas of their security, while also reaping the benefits of the public cloud's extensive security features. Plus, you only pay for what you use.

Cloud Security - Shared Responsibility Model



Our clients retain complete control and ownership of their data, and all data is secured in-transit and at-rest. Since there are no physical servers or storage devices to manage, clients use software-based security tools to remotely monitor and protect the flow of information into and of out their cloud resources. Network traffic between cloud regions, availability zones, and individual datacenters travels over private network segments by default, and every instance, load balancer and private segmentation contains a firewall.

To keep your account and resources safe, you can:

GAIN a unified view of your security posture across both on-premise and cloud workloads

MAINTAIN control of your guest operating system and applications, keeping them updated with the latest security patches

SET UP multiple layers of additional protection, including subnets, three-tier architectures with demilitarized zones (DMZs), and hardware VPNs from your office or datacenter

MANAGE HTTPS endpoints for encrypted data transmission

CREATE distinct user accounts with individualized access credentials and MFA, all from a central portal

ENCRYPT data automatically in the cloud or on-premises before it's uploaded to the cloud

ESTABLISH regular penetration testing and proactively respond to vulnerabilities

LEVERAGE machine learning and advanced analytics for real-time threat management

APPLY policies and adjust controls to meet standards of compliance

Business benefits:

REDUCE your exposure to an increasing number of sophisticated threats

TRANSFORM your business faster with proven security methodologies and processes

FREE your IT staff to focus on moving your business forward

PLAN proactively and prepare for security incidents

EMPOWER rapid action in response to threats

OPTIMIZE your business productivity and IT investments

POSITION your organization for regulatory compliance

Compliance, prevention and reacting to events is the responsibility of your organization but given IT burdens and cybersecurity complexity, it is easy to fall behind. This is where InterVision's expertise can help.

Why InterVision for Security?

EXPERIENCE: Security experts with decades of experience creating security environments for leading organizations across industries, along with a deep understanding of underlying vendor technologies and workflows within the datacenter technology stack and cloud

24X7X365 SUPPORT: Our Security Operations Center (SOC) contains a team of security experts to monitor and manage your security environment and respond when incidents occur

PROVEN METHODOLOGY: Utilizing nationally-recognized cybersecurity frameworks and methodologies, our battle-hardened processes drive discovery, architecture, planning, and implementation

BUILT FOR COMPLIANCE: Our two SOC-certified datacenters allow us to assist all clients in their regulatory demands, whether it's FISMA, ISO, ISO 27018, NIST 800-53, P2PE, PA-DSS, PCI-DSS, SOC, HIPPA/HITECH, GDPR or others

LOWERED COSTS: Reduce or eliminate dedicated security staff, as a result pay only for the security services you need

HIGHEST AVAILABILITY AND DISASTER RECOVERY: Leveraging a CSP's cost-effective model, geographic footprint and automation, we deliver organizations superior availability to meet their goals and an unprecedented level of backup and recoverability

SIEM AS A SERVICE: Our experts not only proactively manage your cloud posture; we also tackle security incident and event management (SIEM) should anything occur to your cloud-based IT systems. We notify you of the incident, then keep you updated on progress as we resolve it

Security Certifications

- Federal Risk and Authorization Management Program (FedRAMP)
- ISO 20000:27001
- ISO 9000 (in process with audit completed as of this publication)
- Top Secret Facilities Clearance
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO)
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) security impact levels 2 and 4
- Federal Information Security Management Act (FISMA)
- US Health Insurance Portability and Accountability Act (HIPAA)
- FBI Criminal Justice Information Services (CJIS)
- National Institute of Standards and Technology (NIST) 800-171
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- Family Educational Rights and Privacy Act (FERPA)

Infiniti powers InterVision's Cloud Services. To detect, protect and remediate your business in the cloud, visit www.intervision.com & www.infiniticloud.com or contact your InterVision sales representative. Central HQ 844.622.5710 | West HQ 800.787.6707

powered by infiniti® AN INTERVISION COMPANY