Security Position For Hybrid Cloud

iBRIDGE
iBridge Cloud Technologies

iBridge Cloud Technologies Follows NIST Protocols

The NIST Cybersecurity Framework provides a comprehensive set of guidelines for improving cybersecurity across all industries. By leveraging the framework, organizations can develop a comprehensive approach to cybersecurity that includes risk management, threat identification and protection, and incident response.

One key component of the NIST Cybersecurity Framework is the development of a security platform that can help organizations manage and monitor their security posture. This platform should be designed to support the various functions and processes outlined in the framework, including:

Identify: The platform should be able to identify and catalog all assets, both hardware and software, that are critical to the organization's operations. This should include mapping data flows, identifying vulnerabilities, and assessing risks associated with each asset.

Protect: The platform should support the implementation of security controls and safeguards to protect critical assets from threats and vulnerabilities. This could include implementing access controls, encrypting sensitive data, and monitoring user activity for signs of suspicious behavior.

Detect: The platform should have the ability to detect and alert security events and incidents in real-time. This could include monitoring network traffic, user activity, and system logs for signs of intrusion or compromise.

Respond: The platform should provide a framework for responding to security incidents and breaches, including defining roles and responsibilities, documenting incident response procedures, and testing incident response plans.

Recover: The platform should support the recovery of critical systems and data in the event of a security incident or disaster. This could include backup and restore processes, business continuity planning, and disaster recovery testing.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

By leveraging the NIST Cybersecurity Framework and building a comprehensive security platform that supports the framework's core components, organizations under the iBridge Cloud Technologies' umbrella can improve their overall security posture, reduce risk, and ensure compliance with relevant regulations and standards.

Identity & Access Management (IAM)

Identity and Access Management (IAM) is the process of managing and controlling user identities and their access to resources in a cloud environment. IAM is critical for ensuring that only authorized users have access to sensitive data and applications, and that those users only have access to the specific resources they need to perform their job. As part of each client's basic cloud the overall security portfolio that iBridge offers.

Here are some technical details and examples of IAM:

Multi-factor authentication (MFA):
MFA is a security mechanism that requires users to provide two or more forms of authentication to access a resource. This adds an additional layer of security beyond just a password. There are several types of MFA, including:

- **SMS-based:** In this type of MFA, the user receives a one-time code via SMS that they must enter along with their password to access the resource.
- **App-based:** In this type of MFA, the user installs an app on their phone that generates a one-time code they must enter along with their password to access the resource. Examples of app-based MFA include Google Authenticator and Microsoft Authenticator.
- **Hardware-based:** In this type of MFA, the user has a physical device, such as a security token or USB key, that they must insert or tap to generate a one-time code they must enter along with their password to access the resource.

Role-based access control (RBAC):
RBAC is a method of assigning permissions to users based on their role in the organization. RBAC can help ensure that users only have access to the resources they need to do their job. RBAC typically involves three main components:

- **Roles:** These are collections of permissions that are assigned to a group of users based on their job function. For example, a role might be "developer" or "admin".
- **Permissions:** These are the specific actions that a user is allowed to perform on a resource. For example, a permission might be "read", "write", or "delete".
- **User assignments:** These are the assignments of users to specific roles. For example, User A might be assigned to the "developer" role, which grants them permission to read and write code, but not delete it.

Privilege escalation management:
Privilege escalation management is the process of managing how users can escalate their privileges to access higher levels of permission. Privilege escalation is typically granted on a temporary basis for specific tasks and is typically controlled through a "least privilege" approach. Some common examples of privilege escalation include:

- **sudo:** On Unix and Linux systems, sudo is a command that allows a user to run a command with elevated privileges. The user must enter their password to run the command.
- **Windows User Account Control (UAC):** In Windows, UAC is a feature that prompts users for permission before allowing them to perform certain actions that require elevated privileges.

IAM is a critical component of cloud security, and encompasses several technical controls, such as MFA, RBAC, and privilege escalation management, to ensure that only authorized users have access to sensitive data and applications.

Encryption

Encryption is the process of encoding data so that only authorized parties can access it. Encryption is an important security mechanism in cloud computing as it helps protect data at rest and in transit. iBridge has subject material expertise in the Federal Information Processing Standards (FIPS), which are a set of guidelines and standards for information security published by the National Institute of Standards and Technology (NIST) in the United States. FIPS specifies the requirements for cryptographic modules used in information security systems to protect sensitive information.

FIPS-approved encryption protocols include:

- **Advanced Encryption Standard (AES):**
  AES is a symmetric encryption algorithm that uses a block cipher to encrypt data. AES is used to protect classified information and is approved for use by the U.S. government.
- **Triple Data Encryption Standard (3DES):**
  3DES is a symmetric encryption algorithm that uses a block cipher to encrypt data. 3DES is used to protect sensitive but unclassified information and is approved for use by the U.S. government.
- **Secure Hash Algorithm (SHA):**
  SHA is a family of cryptographic hash functions used to verify the integrity of data. SHA-2 and SHA-3 are approved for use by the U.S. government.
- **RSA:**
  RSA is a public-key encryption algorithm used to encrypt and digitally sign data. RSA is used to protect sensitive but unclassified information and is approved for use by the U.S. government.

Encryption at Rest:
Encryption at rest refers to the process of encrypting data when it is stored on disk or in a database. In cloud computing, encryption at rest is typically managed by the cloud service provider. Here are some technical details of encryption at rest:

- Encryption Algorithms: Encryption algorithms are mathematical formulas that are used to scramble data. In cloud computing, strong encryption algorithms such as Advanced Encryption Standard (AES) with 256-bit keys are used to encrypt data at rest.
- Key Management: Encryption requires the use of keys to lock and unlock data. In cloud computing, keys are typically managed by the cloud service provider. Cloud providers may use different key management approaches such as key rotation, key wrapping, and key splitting.
- Encryption Key Storage: Encryption keys are sensitive data that must be protected. Cloud service providers may store encryption keys in a separate location from the data they encrypt to ensure that they are protected from unauthorized access.

Encryption in Transit:
Encryption in transit refers to the process of encrypting data as it travels across a network. In cloud computing, encryption in transit is typically managed by the application or service that is sending the data. Here are some technical details of encryption in transit:

- Transport Layer Security (TLS): TLS is a protocol that provides secure communication over a network. TLS uses certificates to authenticate the identity of the server and encrypts data in transit to prevent eavesdropping and tampering. In cloud computing, TLS is commonly used to encrypt data in transit.
- Secure Sockets Layer (SSL): SSL is a predecessor to TLS and is still used in some cloud applications. SSL also uses certificates to authenticate the identity of the server and encrypts data in transit.

Encryption plays a crucial role in cloud computing security by protecting data at rest and in transit. Cloud service providers offer encryption services and options to help customers secure their data in the cloud. Encryption algorithms, key management, and key storage are some of the technical details involved in encryption in cloud computing.

Network Security

Network security is a crucial component of cloud computing security as it helps protect the cloud infrastructure from unauthorized access, attacks, and data breaches. Network security involves several technical controls, such as firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs), that work together to create a secure cloud environment. In this answer, I will explain the technical details of network security in cloud computing, along with examples of its crucial role. iBridge Cloud Technologies utilizes Palo Alto as its Firewalling Partner.

Palo Alto Networks is a leading provider of network security solutions, including firewalls, intrusion prevention systems, and advanced threat detection and prevention solutions. Palo Alto Networks' firewalls are designed to provide advanced network protection by offering a range of features that go beyond traditional firewalls. Here are some ways in which Palo Alto Networks' firewalls excel in network protection:

1. ***Application-aware firewalling:***
   Palo Alto Networks' firewalls are application-aware, meaning they can identify and control application traffic on the network. This enables fine-grained control over which applications are allowed to run on the network, and how they are allowed to behave. For example, an organization might choose to allow access to certain applications, but block others based on their risk level.
2. ***Threat prevention:***
   Palo Alto Networks' firewalls are designed to prevent known and unknown threats from entering the network. The firewall uses a combination of signature-based and behavior-based techniques to detect and prevent threats in real-time. The firewall can also automatically update its threat detection and prevention capabilities through regular updates.

3. ***Advanced sandboxing:***
   Palo Alto Networks' firewalls feature advanced sandboxing capabilities, allowing them to analyze suspicious files and traffic in a safe, isolated environment. This enables the firewall to detect and prevent new and unknown threats that may not be caught by traditional signature-based detection techniques.
4. ***User-based policy enforcement:***
   Palo Alto Networks' firewalls allow organizations to create policies based on user identity, as well as device and location. This enables organizations to provide appropriate access to resources based on the user's role and responsibilities within the organization. The firewall can also apply policies based on the user's behavior, such as limiting access if the user is exhibiting suspicious activity.
5. ***Centralized management:***
   Palo Alto Networks' firewalls can be managed centrally through a single pane of glass, making it easy for organizations to manage their network security across multiple locations and devices. The centralized management also provides real-time visibility into network activity, allowing administrators to quickly detect and respond to security incidents.

Palo Alto Networks' firewalls excel in network protection by providing application-aware firewalling, advanced threat prevention, advanced sandboxing, user-based policy enforcement, and centralized management. These features provide a comprehensive security solution for organizations looking to protect their network against a range of threats. Intrusion Detection and Prevention Systems (IDPS):

IDPS are security systems that monitor network traffic for signs of an attack and take action to prevent the attack. IDPS can be host-based or network-based and can use several techniques to detect and prevent attacks. Palo Alto Networks offers an Intrusion Detection and Prevention System (IDPS) called Threat Prevention, which is part of the Palo Alto Networks Next-Generation Security Platform. Threat Prevention provides advanced threat detection and prevention capabilities for cloud, on-premises, and hybrid environments.

Here are some of the features and capabilities of Palo Alto Networks Threat Prevention:

1. ***Advanced threat detection and prevention:***
   Threat Prevention uses a combination of signature-based and behavior-based techniques to detect and prevent threats in real-time. This includes detecting malware, viruses, and other malicious activity, as well as blocking known threats and unknown threats.
2. ***Network segmentation:***
   Threat Prevention enables network segmentation, allowing organizations to segment their network into smaller, more manageable segments. This helps to reduce the attack surface and prevent lateral movement of threats across the network.
3. ***Integration with other security solutions:***
   Threat Prevention integrates with other security solutions, such as Palo Alto Networks WildFire, to provide additional threat intelligence and advanced malware analysis. This enables organizations to quickly detect and respond to advanced threats.
4. ***Automated threat response:***
   Threat Prevention provides automated threat response capabilities, allowing organizations to quickly respond to threats in real-time. This includes automated blocking of malicious traffic, as well as automated containment of infected devices.

5. ***Centralized management:***
   Threat Prevention can be managed centrally through the Palo Alto Networks Panorama management platform. This provides real-time visibility into network activity, and enables administrators to quickly detect and respond to security incidents.
6. ***Customizable policies:***
   Threat Prevention allows administrators to create customizable policies based on user identity, device, and location. This enables organizations to provide appropriate access to resources based on the user's role and responsibilities within the organization.
7. ***Cloud-based deployment:***
   Threat Prevention can be deployed in the cloud, providing advanced threat detection and prevention for cloud environments. This includes support for public, private, and hybrid cloud environments.

Palo Alto Networks Threat Prevention provides advanced threat detection and prevention capabilities for cloud, on-premises, and hybrid environments. With features such as network segmentation, integration with other security solutions, automated threat response, and centralized management, Threat Prevention enables organizations to quickly detect and respond to threats, and protect their network against potential security breaches.

Virtual Private Networks (VPNs):
Palo Alto Networks' firewalls provide a range of security features for securing VPN access to cloud environments. Here are some ways in which Palo Alto Networks' firewalls secure VPN access to the cloud environment:

1. ***Two-factor authentication (2FA):***
   Palo Alto Networks' firewalls support 2FA, which requires users to provide two forms of authentication to access the VPN. This adds an extra layer of security beyond just a password and helps to prevent unauthorized access to the cloud environment.
2. ***Granular access control:***
   Palo Alto Networks' firewalls provide granular access control for VPN users. Administrators can define policies that restrict VPN access to specific resources based on the user's role and responsibilities within the organization. This ensures that users only have access to the resources they need to perform their job and helps to prevent unauthorized access.
3. ***Threat prevention:***
   Palo Alto Networks' firewalls provide threat prevention for VPN traffic. The firewall uses a combination of signature-based and behavior-based techniques to detect and prevent threats in real-time, protecting the cloud environment from potential security breaches.
4. ***User-based policy enforcement:***
   Palo Alto Networks' firewalls allow administrators to create policies based on user identity, device, and location. This enables organizations to provide appropriate access to resources based on the user's role and responsibilities within the organization. The firewall can also apply policies based on the user's behavior, such as limiting access if the user is exhibiting suspicious activity.
5. ***Centralized management:***
   Palo Alto Networks' firewalls can be managed centrally through a single pane of glass. This provides real-time visibility into VPN activity and enables administrators to quickly detect and respond to security incidents.

6. ***Virtual private network (VPN) tunneling protocols:***
   Palo Alto Networks' firewalls support a range of VPN tunneling protocols, including IPsec, SSL, and L2TP. These protocols provide strong encryption and authentication for VPN traffic, ensuring that data is protected in transit between the remote user and the cloud environment.

Palo Alto Networks' firewalls provide a comprehensive range of security features for securing VPN access to cloud environments. These features include two-factor authentication, granular access control, threat prevention, user-based policy enforcement, centralized management, and support for strong VPN tunneling protocols.

Network security is a critical component of cloud computing security and involves several technical controls, such as firewalls, IDPS, and VPNs. These controls work together to create a secure cloud environment and protect the cloud infrastructure from unauthorized access and attacks.

Vulnerability Management

Vulnerability Management: Vulnerability management is the process of identifying, prioritizing, and remediating security vulnerabilities in the cloud infrastructure. An advanced security offering should have a robust vulnerability management program that includes regular vulnerability scanning, patch management, and penetration testing. iBridge Cloud Technologies has chosen Mandiant as our Vulnerability Management partner.

Mandiant is a cybersecurity company that provides a range of services, including vulnerability management. Here are some ways in which Mandiant excels in vulnerability management:

Comprehensive vulnerability scanning:
Mandiant uses a comprehensive vulnerability scanning tool to identify vulnerabilities in an organization's network, servers, and applications. The tool scans for known vulnerabilities and uses behavioral analysis to identify unknown vulnerabilities that may be exploited by attackers.

Customizable reporting:
Mandiant provides customizable reporting that enables organizations to view vulnerabilities based on different criteria, such as severity level, risk rating, and criticality. This enables organizations to prioritize their remediation efforts based on the most critical vulnerabilities.

Automated vulnerability remediation:
Mandiant's vulnerability management service includes automated vulnerability remediation, which can automatically apply patches or configurations to fix vulnerabilities. This reduces the time and effort required to remediate vulnerabilities, while also reducing the risk of human error.

Integration with other security solutions:
Mandiant's vulnerability management service integrates with other security solutions, such as Mandiant's incident response and threat intelligence services. This enables organizations to quickly detect and respond to security incidents, as well as to proactively identify vulnerabilities before they are exploited.

Expert analysis and recommendations:
Mandiant's vulnerability management service includes expert analysis and recommendations for remediation, which can help organizations to prioritize their remediation efforts and reduce the risk of exploitation. Mandiant's extensive experience in cybersecurity and its deep understanding of attacker techniques and tactics bring a level of elevation strategy that allows iBridge to offer the most complete security platform in Cloud.

Continuous monitoring:
Mandiant's vulnerability management service includes continuous monitoring to detect new vulnerabilities as they are discovered. This ensures that organizations are always aware of the latest threats and vulnerabilities, and can take action to protect their systems and data.

Mandiant excels in vulnerability management by providing comprehensive vulnerability scanning, customizable reporting, automated vulnerability remediation, integration with other security solutions, expert analysis and recommendations, and continuous monitoring. By using these features, organizations can reduce their risk of exploitation by attackers and proactively identify and remediate vulnerabilities before they are exploited.

Threat Detection & Response

Threat Detection and Response: Threat detection and response involves identifying and responding to security incidents and threats in real-time. On top of the incredible live innovative security offered by Palo Alto. An advanced security offering should have a security operations center (SOC) that is staffed by trained security professionals and equipped with advanced security tools and technologies, such as security information and event management (SIEM) systems, security analytics, and threat intelligence feeds. iBridge Cloud Technology currently uses our partner Mandiant as our 24/7 SOC. iBridge is building our own SOC practice and will continue to utilize Mandiant.

A 24-hour Security Operations Center (SOC) or Network Operations Center (NOC) with Mandiant as an escalation partner enables continuous threat detection by providing round-the-clock monitoring and response to security incidents. Here are some ways in which this setup allows for continuous threat detection:

24/7 monitoring:
A 24-hour SOC/NOC with Mandiant as an escalation partner provides continuous monitoring of an organization's network and systems for security incidents. This ensures that any potential threats or vulnerabilities are detected as soon as possible, even outside of regular business hours.

Rapid incident response:
In the event of a security incident, Mandiant can be quickly escalated to provide expert analysis and recommendations for remediation. This enables organizations to respond to security incidents rapidly, reducing the potential impact of the incident.

Proactive threat hunting:
Mandiant can perform proactive threat hunting to identify potential threats and vulnerabilities that may not be detected through regular monitoring. This involves using advanced analytics and threat intelligence to search for potential indicators of compromise and other security risks.

Integration with other security solutions:
Mandiant can integrate with other security solutions, such as SIEM and endpoint detection and response (EDR) systems, to provide a more comprehensive view of an organization's security posture. This enables Mandiant to detect and respond to threats across multiple platforms and identify potential security gaps.

Expert analysis and recommendations:
Mandiant provides expert analysis and recommendations for remediation, based on its extensive experience in cybersecurity and deep understanding of attacker techniques and tactics. This enables organizations to respond to security incidents effectively and reduce the risk of future incidents.

Our 24-hour SOC/NOC with Mandiant as an escalation partner enables continuous threat detection by providing round-the-clock monitoring and response to security incidents, rapid incident response, proactive threat hunting, integration with other security solutions, and expert analysis and recommendations. This setup can help organizations to reduce their risk of security incidents and proactively identify and remediate potential threats and vulnerabilities.

Compliance/Governance as a Service

Compliance: Compliance refers to adhering to regulatory and industry standards for data security and privacy. An advanced security offering should be compliant with relevant regulations and standards, such as HIPAA, PCI-DSS, and GDPR. iBridge Cloud Technologies has partnered with Omnistruct, a leading Governance/Compliance as a Service Provider. Omnistruct builds, maintains and provides proof of cybersecurity compliance for companies in a way that helps them develop a comprehensive cybersecurity program that’s not just an afterthought or a failsafe, but an essential and integrated part of their company culture.

Omnistruct guides iBridge Clients in:

Vulnerability Assessments: Frequent low-impact tests create actionable items to reduce risks.

NIST Compliance: Prove to your customers that your organization is capable of handling data to a set of current guidelines.

Compliance Desk: Get quick, expert answers to questions about compliance, regulatory, or insurance matters.

vCISO Solutions: When your customer wants to talk security controls, we are here to help.

Penetration Testing: Want to see how well you can defend against hackers? Our in-depth knowledge and security tools can help.

Dark Web Monitoring: We provide continuous monitoring of your domain for any data breaches containing your company's data.

Questionnaire Handling: Your biggest customers are trying to decide if doing business with you is a risk. Our automated system helps you answer these questions and give your clients confidence.
Incident Response Services: Despite doing everything right, risks still exist. We help manage the response to retain forensics, reduce risks and keep a defensible space.

Third-Party Technology Partner Network: We only sell risk mitigation and privacy solutions. We rely on third parties for technology and services. That means we're impartial when discussing your organization's needs.

SANS Employee Training: SANS is a collaborative professional organization dedicated to creating a safer global community. To achieve this goal, they run multiple programs to draw more talent into the cybersecurity field and empower those people with the skills and knowledge needed to enter the workforce, accomplish important tasks, and lead the way. They offer interactive, live-stream courses taught by real-world practitioners.

Compliance Tracking and Audits: Utilizing third party tools, iBridge/Omnistruct have the ability to query clients' environments and compare against compliance standards in order to mitigate vulnerabilities and compliance shortcomings which could hurt there upstream and downstream partnerships.

Data Protection

Data Protection is at the forefront of all private and private cloud providers. Jetstream Software is at the forefront of Data Protection, iBridge's strategic alliance with Jetstream exists on the innovation between the two engineering teams, Cloud Development and Data Protection.

JetStream is a software company that provides cloud-native data management solutions for enterprise-level organizations. Their software solutions are designed to help organizations easily migrate, protect, and manage their data across multiple clouds, including public, private, and hybrid clouds.

JetStream was founded in 2016 by a team of industry veterans with extensive experience in cloud infrastructure and storage technologies. The company's headquarters are located in San Jose, California, and they have additional offices in Bulgaria and India.

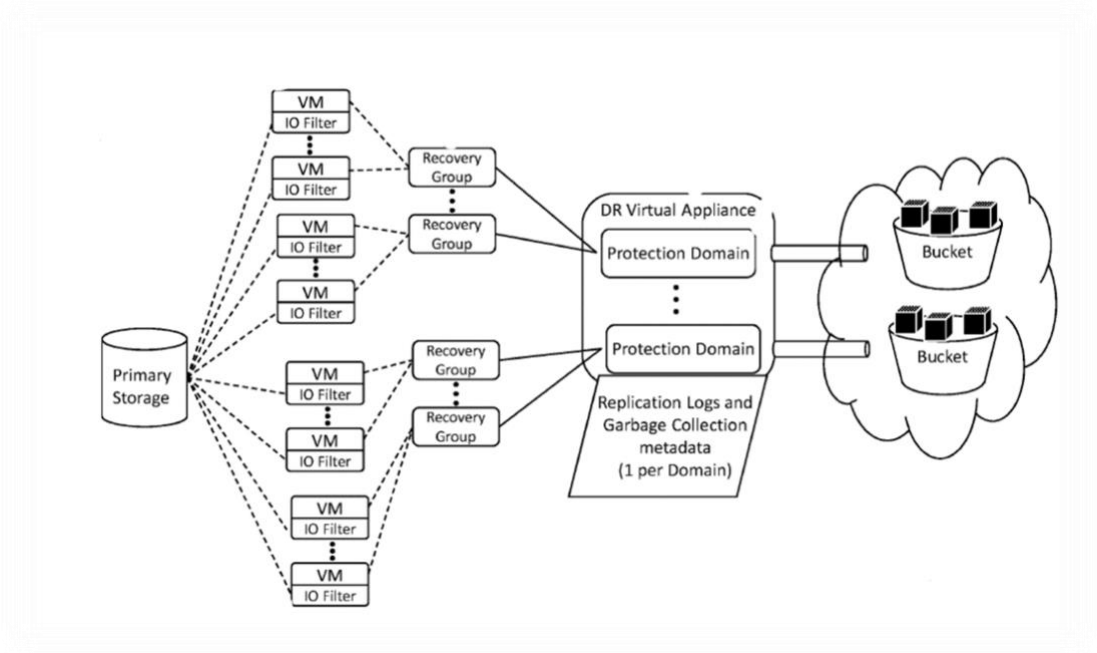
JetStream's flagship product is JetStream Migrate, which is a solution that enables organizations to easily migrate workloads to the cloud while minimizing downtime and disruption. The solution automates the migration process and provides real-time monitoring to ensure that the migration is successful. JetStream Migrate is fully compatible with leading cloud providers, such as iBridge Cloud Technologies, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

In addition to JetStream Migrate, the company offers other cloud-native data management solutions, such as JetStream DR, which enables organizations to protect their data and workloads in the cloud with continuous replication and point-in-time recovery.

JetStream's solutions are designed to be highly scalable, flexible, and efficient, with a focus on minimizing disruption to business operations during the migration and protection of data. Their solutions leverage advanced technologies, such as virtualization, software-defined storage, and machine learning, to deliver high-performance data management capabilities.

JetStream is a leading provider of cloud-native data management solutions that enable organizations to easily migrate, protect, and manage their data across multiple clouds. With a focus on scalability, efficiency, and ease-of-use, JetStream's solutions are helping organizations to leverage the full potential of the cloud while minimizing disruption to business operations.

The collaboration between our newest NVMe on PCIe of optical fabric storage and the Jetstream Software patented object storage disaster recovery will offer recovery point objective (RPO) and recovery time objective (RTO) that will be better, faster and cheaper than all cloud providers.



SOC/NOC

iBridge Cloud Solutions Inc. runs a 24-hour Network Operations Center (NOC) for its facilities and hosted clients. We will launch our 24-hour Security Operations Center (SOC) in Q3 2023.

A Security Operations Center (SOC) and Network Operations Center (NOC) play critical roles in maintaining the security, stability, and performance of our data centers and environments. Some of the key duties of a SOC/NOC include:

Monitoring: SOC/NOC teams are responsible for monitoring the data center infrastructure and network for any anomalies or potential security threats. This includes monitoring logs, alerts, and performance metrics to identify and respond to any issues.

Incident response: In the event of a security incident or network outage, SOC/NOC teams are responsible for responding quickly and effectively to mitigate the impact of the incident. This includes identifying the root cause of the incident and implementing remediation measures to prevent similar incidents from occurring in the future.

Security: SOC teams are responsible for ensuring the security of the data center and the data stored within it. This includes implementing and maintaining security protocols, such as firewalls, intrusion detection and prevention systems (IDPS), and encryption.

Patching and updates: SOC/NOC teams are responsible for ensuring that the data center's software and hardware are up to date and secure. This includes applying software patches, updates, and security fixes as necessary to protect against vulnerabilities.

Compliance: SOC/NOC teams are responsible for ensuring that the data center adheres to industry and regulatory compliance requirements. This includes maintaining documentation, auditing procedures, and implementing security controls to ensure compliance.

Capacity planning: SOC/NOC teams are responsible for monitoring the performance of the data center and planning for capacity increases or upgrades as necessary. This includes monitoring resource utilization, network traffic, and storage capacity to ensure that the data center can handle the demands placed on it.

SOC/NOC plays a critical role in ensuring the security, stability, and performance to the iBridge data centers. Their duties include monitoring, incident response, security, patching and updates, compliance, and capacity planning.

The iBridge Cloud SOC is backed by our partnership with Sandia Labs and Mandiant.

Mandiant is an extremely strategic partner for iBridge because it provides a range of cybersecurity services that are critical for protecting organizations against increasingly sophisticated cyber threats. Some of the key reasons why Mandiant is such a valuable partner include:

Expertise: Mandiant has a team of highly skilled cybersecurity professionals with extensive experience in responding to security incidents and managing security operations. This expertise is critical for helping organizations to detect, analyze, and respond to security threats.

Innovation: Mandiant is known for its innovative approach to cybersecurity, using advanced technologies and techniques to detect and respond to threats. This includes machine learning, artificial intelligence, and advanced analytics to help identify patterns and anomalies that could indicate a potential security threat.

Reputation: Mandiant has built a strong reputation for providing high-quality cybersecurity services to organizations across a range of industries. Their reputation for excellence has helped to establish them as a trusted partner for organizations looking to improve their cybersecurity posture.

Comprehensive services: Mandiant provides a wide range of cybersecurity services, including incident response, threat intelligence, risk assessments, and managed security services. This comprehensive approach allows organizations to address their cybersecurity needs in a holistic manner.

Global reach: Mandiant has a global presence, with offices and customers around the world. This global reach allows them to provide cybersecurity services to organizations of all sizes and in all industries, regardless of their location.

Mandiant's expertise, innovation, reputation, comprehensive services, and global reach make it a vital partner in the cybersecurity industry. Their services are critical for protecting our key assets and clients against cyber threats and helping to ensure the security and integrity of their systems and data.

Our 7-layers of Protection