/// BLUEFABRIC ARCHITECTURE

Technical Overview
Security framework to protect cyber assets.

The bluefabric architecture is a comprehensive security framework specifically designed from the ground-up to make regulatory compliance reliable and cost-effective, for both the initial audit and ongoing maintenance.

The bluefabric data protection landscape is comprised of risk-adjusted security controls embedded in all layers of the enterprise architecture: physical, network, infrastructure, platform and application. These controls apply to people, processes and technology that transmit, process or store sensitive business-critical information.

In addition to providing complete coverage, a significant differentiator of the bluefabric architecture is its low impact on the existing systems and infrastructure, often built at great expense. Similar to Google and Amazon, a standards based, web service API is offered for application integration. In complex legacy scenarios, a "zero impact" option can provide in-transit data protection without any need for modifications to your client or server applications.

Key Benefits

- All-in-one integrated compliance framework
- Meets all prevalent data compliance standards
- Enables secure, flexible access to sensitive data
- Alleviates the risk of critical data breach or loss

Key Features

- Complete blueprint for compliance certification
- Data-centric security ecosystem for digital assets
- Well-defined set of business and system services
- Modular portfolio of financial network endpoints
- Logging, analytics, alerting and archiving facilities

An attack on an environment aligned with the bluefabric architecture will not suffer financial, reputational or legal damages. Incentives for hackers are eliminated, prompting them to seek out other assets worth stealing. The cost and complexity of audits are dramatically reduced.

Enable "zero trust" model with secure data services in your current environment.

The bluefabric architecture is a combination of business services and financial network endpoints based on the fundamental cyber security principles that feed into regulatory compliance.

Package	Core	Full
Tokenization	●	●
Encryption	●	●
Key Management	●	●
Payment Gateway	○	●
Credit Scoring	○	●
Address Verification	○	●
Digital Wallet	○	●
Archiving	○	●

1-888-414-5739 info@bluezonex.com www.bluezonex.com

Compliance Architecture

Layered security mitigating advanced threat.

Security Principles

- **Authentication** – system or user sign-in/validation.
- **Authorization** – access control of restricted resources.
- **Accountability** – audit trail to transaction originators.
- **Confidentiality** – data exposure to authorized users.
- **Integrity** – data consistency over its entire lifecycle.
- **Non-repudiation** – assurance of data integrity/origin.
- **Availability** – continuous access to critical services.
- **Flexibility** – agility in security control vs. operation.
- **Compliance** – security assessment and certification.

Compliance Standards

- **Payment Security** – addresses all 12 areas of PCI Data Security Standard (DSS) requirements.
- **Federal Cloud Security** – provides FedRAMP based, agency-specific security and privacy controls.
- **Financial Cyber Security** – maintains OSFI regulated information security practices and controls.
- **Healthcare Privacy** – de-identifies and secures HIPAA governed protected health information (PHI).
- **Security Techniques** – provides ISO/IEC 27000 based model for managing security of information assets.

Security Controls

- **Intrusion Prevention** – prevent network attacks.
- **Transport Layer Security** – manage X.509 certificates.
- **Web Application Firewall** – block web layer exploits.
- **Advanced Threat Protection** – mitigate DoS attacks.
- **Security Patch Management** – install critical patches.
- **Centralized Log Management** – externalize log data.
- **Security Event Management** – review critical events.
- **Virtual Private Network** – encrypt operational path.
- **Two-factor Authentication** – secure remote access.
- **File integrity Monitoring** – guard critical system files.
- **Vulnerability Scanning** – identify system weaknesses.
- **Penetration Testing** – examine possibility of a breach.
- **Time Synchronization** – synchronize system clocks.
- **Network Management** – report on system errors.
- **Physical Security** – restrict access to data facilities.
- **Policy Management** – maintain security policies.

The bluefabric architecture offers a control framework that goes above and beyond 9 prevalent regulatory standards.

Improve your data security landscape with bluefabric.

A blueprint to ultimate compliance.

Security Essentials

Network access: NG firewall, IPS, VPN
Threat blocking: TLS proxy, WAF, DDS
Secure routing: financial services broker
Data protection: tokenization, encryption
Centralized security: device access control, directory service, two-factor authentication

Additional Controls

Centralized logging: secure audit trail
Event analytics: security event manager
Time synchronization: secure NTP service
Network management: SNMP, e-mail alerts
Data archiving: long-term record retention, real-time data replication, disaster recovery

75% Average increase in service flexibility. Data integrity and confidentiality maintained.