Syncrofy

Secure, Protected, Reliable EDI Visibility Software from CoEnterprise

Hybrid Cloud Deployment Option

To learn more about the power of Syncrofy, visit: www.coenterprise.com

Table of Contents

A CoEnterprise White Paper

This white paper will provide an in-depth look at the security features and policies of CoEnterprise and detail how they interoperate with our flagship software, Syncrofy™.

A Culture of Strong Security

At CoEnterprise we take security very seriously, and it's reinforced throughout our culture. Our information security team instructs new engineers on topics like secure coding practices, product design, and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, and mitigation techniques.

We run daily operational security checks to be proactive and minimize vulnerability. The vulnerability management team actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews, and external audits. Once a vulnerability requiring remediation has been identified, it's logged, prioritized according to severity, and assigned an owner. The team tracks and follows up on issues frequently until they can verify they have been remedied.

We monitor our entire production system 24/7 for internal network traffic, employee actions, and outside knowledge for vulnerabilities. Internal traffic is inspected for suspicious behavior at several points across our global network, such as traffic that might indicate botnet connections. This analysis is performed using a combination of opensource and commercial tools for traffic capture and parsing. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. We actively review inbound security reports and monitor public mailing lists, blog posts, and wikis.

- **Daily operational security checks**
- **24/7 Monitoring**
- **Continuous learning & education on new threats**

System Service Patching Cycles

We pride ourselves upon the self-assessment of our production system quickly and efficiently and have a proven track record of patching our system in under 24 hours to eliminate vulnerabilities.

Data Integrity and Encryption

Our security practices follow industry cryptographic standards such as TLS (Transport Layer Security) and AES to protect the confidentiality and integrity of customer data. All customer-facing servers negotiate a secure session using TLS (Transport Layer Security) with client machines to secure the data in transit.

This applies to various protocols such as HTTP(S) and TCP connections on any device. We support and deploy strong encryption using TLS v. 1.2 across all workloads. The use of TLS establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center.

Certifications & Best Practices

When we started developing Syncrofy we began with the network's core and focused on utilizing best-of-breed technology. We wanted to provide an enterprise system that eased the burden of compliance substantiation and minimized the length and severity of non-compliance instances for the enterprise class. Our application and security follow a distinctive framework for those that require autonomous administrative control over their security policies. We use only bare-metal cloud servers and a private cloud infrastructure to ensure our workloads are never shared with other companies.

- **Guided by industry standards**
- **Users have autonomous control over their security**
- **Bare-metal cloud servers and a private cloud infrastructure**

Our network consists of three distinct areas; encryption public access points, internal private support network, and highly private internal LAN communication. All network partitions are monitored 24/7.

We are guided by the following industry standards:

- **ISO 27001-27002** — The basis of our security practices. Provides control structures for risk analysis, physical security, emergency planning, investigations, information protection, education, and more.
- **SAS 70/SSAE 16** — Independent organizations audit the connections service to verify that our data centers are in compliance with defined control points. Effectiveness of these controls are tested annually using a SAS70/SSAE 16 business controls audit.
- **EU Data Privacy** — Connections adhere to the U.S.-EU Safe Harbor framework and our data centers work with customers to execute model clause agreements where legally required.
- **Payment Card Industry Data Security Standards (PCI-DSS)** —These standards incorporate best practices to protect cardholder data.
- **National Institute of Standards and Technology (NIST) 800-53 framework**
- **HIPAA** — The SaaS cloud is managed according to HIPAA security and privacy controls and our data center enters into a BAA (Business Associate Agreement) for our healthcare customers in cloud.
- **ISO 27018** — Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO 29100 for the public cloud computing environment.
- **Safe Harbor** — Assurance that EU organizations know we provide "adequate" privacy protection, as defined by the directive.
- **Data Privacy Directives** (e.g., US Department of Commerce's Safe Harbor directive)
- **Cloud Security Alliance's Security, Trust, and Assurance Registry (STAR) Self-Assessment**

Your Data Belongs to You

We know how important your data is to your business. That's why Syncrofy has been designed to ensure your information is kept secure and treated with the utmost discretion and care. Your sensitive information is never at rest on our side and is always on your side of the firewall.

Our hybrid cloud architecture ensures that you remain in control of your data. Your data is processed locally within your network, behind your firewall with a small segment transmitted back to Syncrofy. It's just enough to ensure that we know it exists so we can retrieve it when you need it.

When a user accesses data from their web browser, a request is made to your network from our servers to retrieve it on behalf of the user. It is immediately forwarded to the user's browser without ever being at rest on our servers. This approach enables us to maximize real-time visibility while ensuring the data remains secure behind your own firewall and under your control.

- **Information stored or created within Syncrofy is yours**
- **No advertising or data mining**
- **Access, download, or remove data anytime**

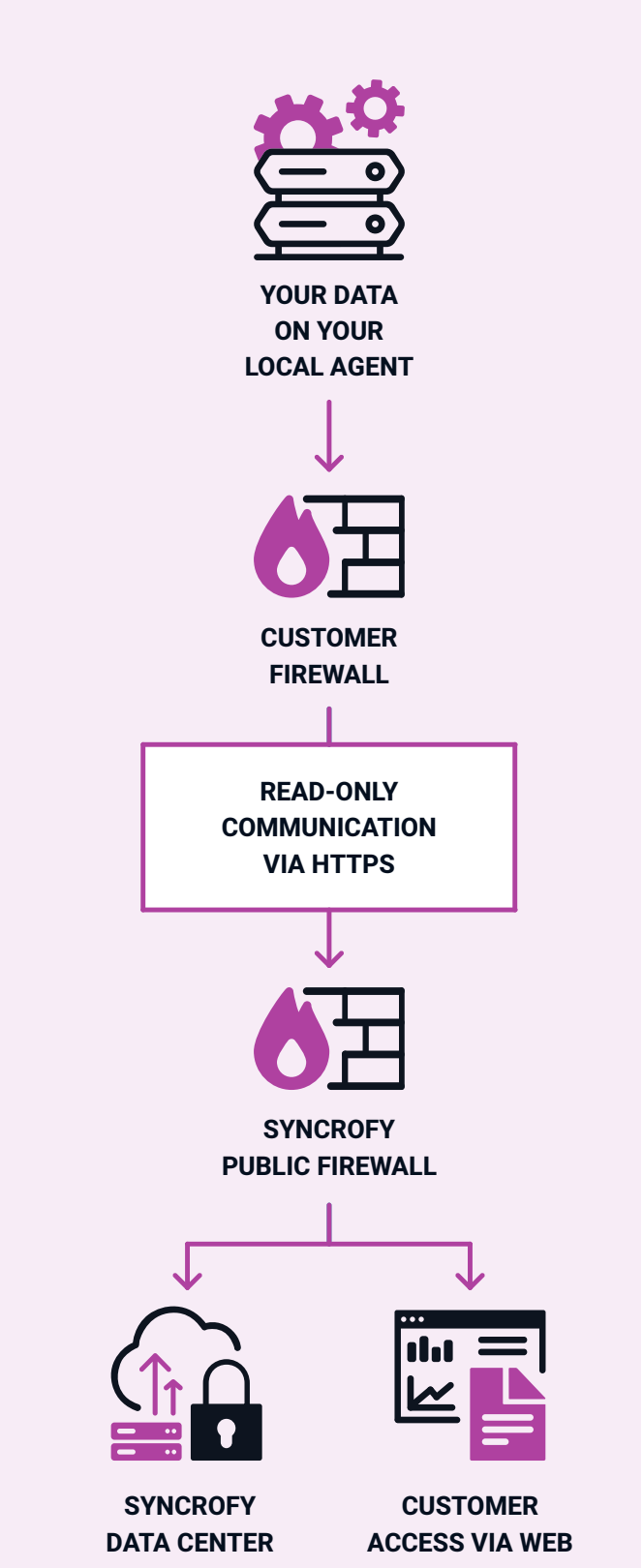

Figure 1: Hybrid Cloud Architecture

A 24/7 Mindset

We designed Syncrofy with an emphasis on maintaining a security rich physical infrastructure, configuration, architecture, business processes, and operations. From code development to the physical security of our data centers and through all of our customer support interactions, our service is designed with security in mind.

Policy and Process

Our company follows security policies that are reevaluated annually. Our practices take a broad range of factors into consideration, including technological, human, and natural; and threats from both outside as well as inside of an organization. The connections service maintains a security team uniquely trained and focused on information security. Modifications to applications and the operating environment are governed by a strict change management process.

Physical Security

Physical security standards are designed to restrict unauthorized physical access to data center resources. Our data centers are guarded with biometric controls on all physical access points, CCTV monitors and recordings, redundant components, network and power sources, and firewalls. Access is restricted to authorized individuals and is based on multifactor authentication (MFA) involving a unique code and biometric scan. IBM partitions the connections infrastructure into security zones with flow control devices, such as firewalls and routers, governing the allowable flows between security zones. WiFi usage is not allowed in the data centers.

- **Constantly improving and refining security**
- **Strong physical security at data centers**
- **Emphasis on detecting & resolving potential risks**

Service Integrity & Availability

Our data center resources are monitored 24/7 and strong encryption protects data that is in transit. Internal and external vulnerability scanning is conducted regularly by authorized administrators to help detect and resolve potential system security exposures. Our highly available infrastructure protects services from single points of failure and from data tier or data center failure. We create a full system backup of your data multiple times per day to ensure no data is lost in the event of hardware, software, or network failure.

Conclusion

The practices and standards outlined in this paper reflect our commitment to security and we have worked to develop a software solution in Syncrofy that mirrors the values and beliefs of our organization. Our customers can rest assured that the security of their data and sensitive information will always be our top priority.

coenterprise

This White Paper Was Created by CoEnterprise

CoEnterprise is a transformative, problem-solving enterprise software and services company. Founded in 2010, we are recognized as a leader in the supply chain and business analytics space, delivering innovative solutions and services that empower people with the resources to analyze their data to make faster, smarter decisions. Fueled by our commitment to people and building lasting relationships, we've helped over 250 customers on over 1,000 projects. Visit **www.coenterprise.com** for more information.