conxport | *Architecture & Security Overview*

The following document is intended to provide the reader with an overview of Conxport's infrastructure, application architecture and Conxeo's organizational philosophy regarding security, best practices and methodology.

INTRODUCTION

Conxport is a Software-as-a-Service (SaaS) solution that provides organizations with a robust and flexible means of collecting and managing data from a diverse community of users.

Conxport is entirely hosted on our infrastructure so there is no need for your IT department to invest in hardware or maintain software. All you need is a modern browser (IE 7 or above, Firefox, Chrome, Safari or Opera) and an internet connection.

ORGANIZATIONAL PHILOSOPHY

Conxport may be a new product, but we have over a decade of experience building and supporting applications for some of the world's largest companies, including banks and financial institutions such as Bank of America and Wells Fargo. These organizations do not take their security lightly and neither should you. As a Conxport customer, you will benefit from our team's extensive knowledge and experience in serving these brands; knowledge that is built directly into Conxport.

INFRASTRUCTURE

Our production environment is hosted by Peer1 Managed Hosting. Our servers at PEER1 are located in a full-service, Tier 1 data center in Atlanta, Georgia.

PEER1 guarantees the following:

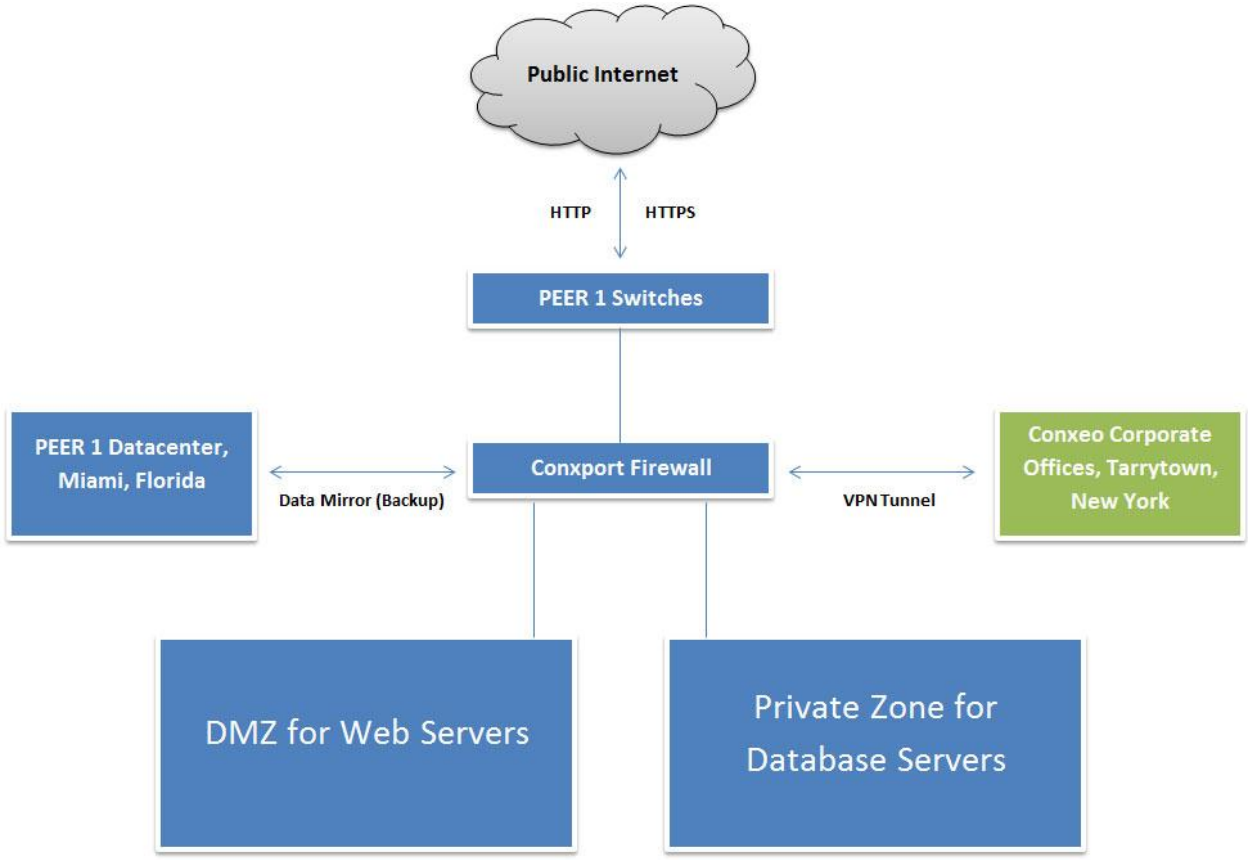
- 100% Network Uptime SLA & 100% Power SLA
- SAS 70 Type II Certified
- 24x7x365 On-Site NOC
- Smart Monitoring

All of our servers operate on a **private network segment**. This is an important point of distinction between Conxport and other SaaS providers that host their services in "shared" environments. By

definition, an application that shares its services with other applications is only as secure as its weakest link.

Access to our production environment is achieved through a **secure firewall-to-firewall VPN tunnel** between PEER1 in Atlanta and our corporate headquarters in Tarrytown, New York. This means that all traffic between our office and PEER1 originates from a **known physical end-point and is encrypted** to prevent eaves-dropping. **We do not operate any back-end management tools on public-facing websites.** The only management functions that are accessible through the web are those built into Conxport that allow our clients to manage their Conxport applications.

Our hardware at PEER1 sits behind a **dedicated firewall with two (2) separate security zones**. Our web servers reside in a DMZ that allows public to access Conxport through a web browser. Our database servers operate in a private zone that is not accessible to the public (*It should be noted that many SaaS providers not only allow their servers to operate in the same zone, but oftentimes on the same server*).



In addition we employ **HTTP filtering** on our web servers to block requests that may seem legitimate to our firewall but are not needed for our application to function properly. We also disable unnecessary services on our servers to prevent access to sensitive areas of the operating system. This is consistent with a **multi-layered defense strategy** to prevent unauthorized access.

Finally, your data is safe and secure because it's continuously backed up and stored at PEER1's Atlanta facility. As an added measure of safety and security, your data is also stored at PEER1's Miami, Florida facility and it is transmitted via a secure Storage Area Network (SAN). Both data centers are SAS 70 Type II certified.

APPLICATION ARCHITECTURE

Conxport is written from the ground up with security in mind. It's built on Microsoft's **ASP.NET** platform using **C#** and **JavaScript** on the front end, and **Microsoft SQL Server** on the back end.

We adhere to industry best practices to secure Conxport, such as **validating data input on both the client side AND the server side** and encrypting data with **Secure Socket (SSL) Layer** technology. All database calls are achieved through the use of **stored procedures** in order to prevent hackers from initiating SQL injection attacks.

Conxport users authenticate using a standard web form (username/email address and a minimum 6-character alpha-numeric password). We utilize **.NET session state and our own access token** to ensure that each user is authenticated before we grant them access to protected resources. We set our access token in a session cookie and **encrypt** it to insure that hackers cannot manipulate it to impersonate another user. Furthermore, each access token has an expiration date so even if a hacker was able to capture another user's cookie, his ability to use it for replay attacks is limited.

If a user accumulates several failed login attempts, **we lock that user's account to prevent brute force login attacks**. After an account is locked, a user must enter a randomly generated series of characters displayed in a **CAPTCHA** control along with proper login credentials in order to unlock their account. This ensures that a "live person" initiates the login rather than an automated program. Each user account is associated with a unique email address during registration. If a user forgets his password, **the only way to gain a new password is to have access to the email account that was used during registration**. Taken together, these mechanisms help prevent unauthorized access to Conxport.

Within Conxport, we implemented a robust **role-based permission system** that allows users to delegate access to Conxport resources in a granular and flexible manner that maps precisely to an organization's internal management structure. This ensures that Conxport maps to your organization structure; not the other way around.

Another important security feature embedded into Conxport is the **encryption of all query strings**. Many SaaS providers include identifiers in their URLs such as client ID or user ID. We encrypt that type of information in order to prevent users from attempting to gain access to protected areas.

It should also be noted that we maintain discrete environments for development, testing and production. Each line of code is created and tested in our development environment, tested again in our testing environment and then moved to our production environment after it's met our standards.

SUMMARY

If you have any questions or concerns about Conxport, its security or architecture, please contact your sales representative.