A Total Digital Solution

Security Whitepaper

Impetus

www.impetusdigital.com

Introduction

The purpose of this document is to explain which measures Impetus takes in order to secure data on all of its portals. Impetus only uses technologies that have been rigorously tested by thousands of others in the software profession. At Impetus' disposal are a variety of technologies, procedures, development practices, audits and logical/physical controls that ensure your data's safety.

About Us

Impetus Digital, focused exclusively on healthcare, builds private, regulatory-compliant online communities and programs for stakeholder engagement, learning and collaboration. Community features are continuously enhanced, incorporating state-of-the-art technology advances. Communities are implemented, managed and sustained by Impetus. As an always-accessible, global communications channel, online community programs foster robust clinical discussions while providing operational efficiencies and scalability.

Impetus Security Framework

At Impetus, we believe that security is a continuous process that adapts to new vulnerabilities and an ever-changing software environment. As such, we only choose technology that improves its security measures on a regular basis, both for hardware and software.

The aspects of your portal and their respective security practices can be thought as:

Section 1: How We Secure Our Hardware

All of the hardware that runs every portal is owned and managed by **Google Cloud Platform** via the Pantheon website management service wrapper. Google Cloud Platform is a service provider that hosts hundreds of thousands of cloud based solutions for their various clients and Google's own services.

Numerous security measures included within our hardware are:

Redundancy - RAID

All hardware uses industry-standard practices for on-disk storage, including writing to multiple physical disks with hardware-level RAID.

Redundancy - Power

We at Impetus also take into account power outages by equipping our data center machines with Uninterruptible Power Supplies and N+1 redundant Uninterruptible Power Supplies for every server and on-site diesel generators in the event of prolonged power outages. All of this equipment will ensure that your portal is up and running no matter what.

Physical Security

Impetus and our Google Cloud Platform partners make sure that there are a number of physical security measures put in place to ensure that no unauthorized people get into our datacenter premises.

These measures include:

- Keycard protocols, biometric scanning protocols, and around-the-clock interior and exterior surveillance.
- Access limited to authorized data center personnel.
- Stringent security background checks on data center employees.

An addition to this, our facilities are equipped with advanced fire suppression systems to make sure that none of your data is lost.

Section 2: How We Secure Our Data

In the event that we need to restore portal data to a time in the past, or dig into past data that was accidentally deleted, our infrastructure is well equipped to provide this kind of functionality. We provide the following services that protect your data:

Regular Backups

Impetus makes sure that data recovery is simple, timely and one that provides the most up to date data. These backups scheduled to be performed at least daily, are kept for at least 2 weeks while ongoing, and are shipped to Amazon S3's highly redundant infrastructure. A second set of backups are also maintained through Google Cloud Platform and Pantheon that go through the same security protocols as the rest of Pantheon.

Our backups have over 99.99% durability and availability.

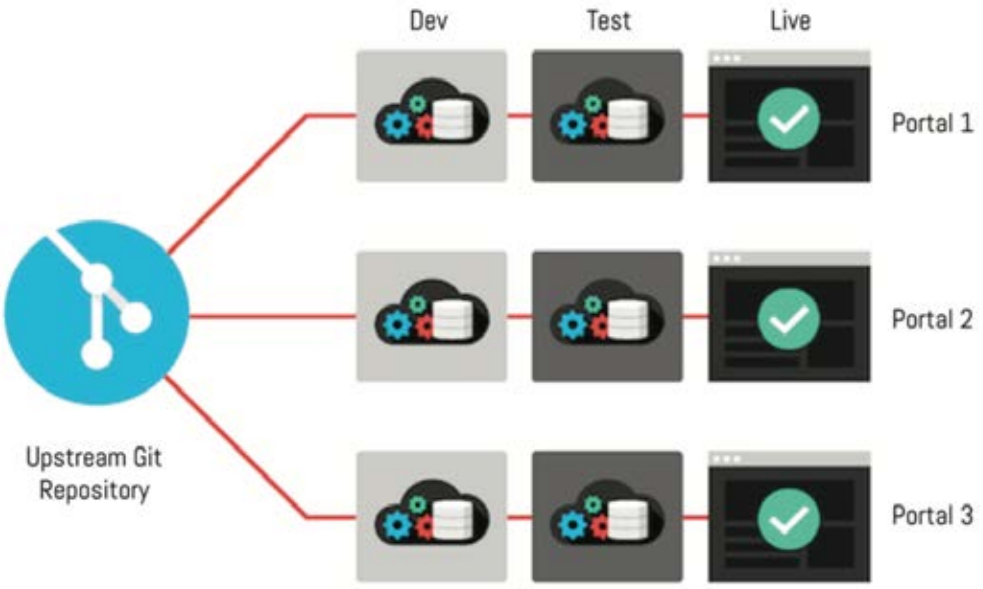
Backup Security

To make sure that nobody unauthorized gets a hold of these backups, read-only access is granted via signed, expired URLs that are only available to Impetus staff and server staff.

Additionally, these backups are encrypted with 256-bit advanced encryption.

Data Separation

Customer data is logically separated from other customer data using separate databases and portal instances. Therefore, it would not be possible for one of Impetus' customers to access your portal's data or stored files. The only aspect common to all portals is SOME computer code. Customer specific customizations are separated from other portals using git and other code versioning techniques.



Section 3: How We Secure Our Network

Impetus secures its network infrastructure from all networking attacks that one would typically face at work or at home. These include viruses, worms, malware, spyware, etc. This infrastructure boasts a 99.9% average uptime throughout the year. We secure our network infrastructure by using the following tools.

Software Whitelist

Through Linux operating systems, Impetus uses only established vendor repositories for software, and software package signature verification. It is only through these repositories that we get our server software. If any executable files were to make it past the portal's built in security Impetus also prevents direct execution of files uploaded through the portal.

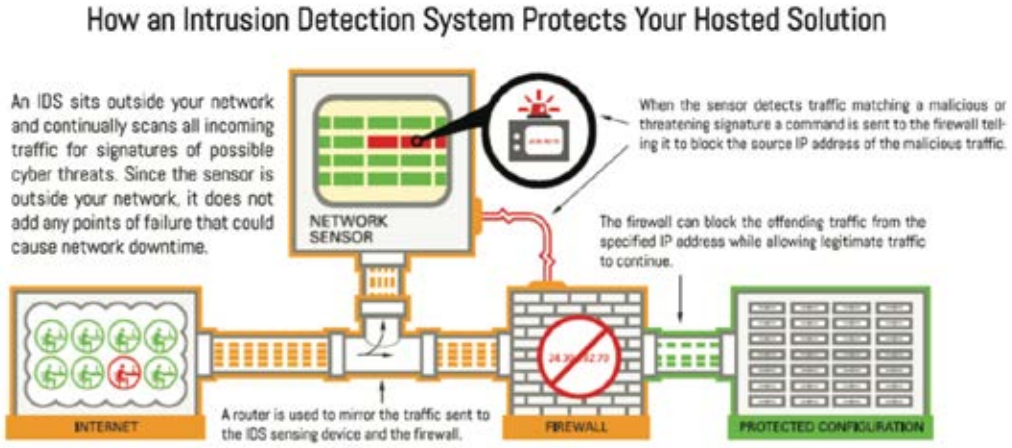
Antivirus

Impetus utilizes ClamAV antivirus/anti-malware for all of its portals. It provides a high performance multi-threaded scanning daemon, and an intelligent tool for automatic signature updates. This utility's databases are updated on a regular basis.

SSL is also enforces for all administrator interactions and user interactions with the portal and dev/test sites.

Intrusion Detection Systems

In cooperation with Google Cloud Platform, Impetus implements a state of the art intrusion detection system to prevent unauthorized access to the server through root privileges and to prevent any DOS or DDOS attacks. Any intrusions will be brought to Impetus' attention via Alert Logic.



In addition to Google Cloud Platform's IDS, we employ centralized IPS to detect failed logins via multiple ingress points and prevent dictionary and brute-force attacks for logging into our server as a root user, administrator or programmer. Security logs from the servers for these failed attempts are centrally collected, processed, secured and stored for 60 days. Access to servers via ssh include use of RSA key pairs in place of passwords, x.509 certificates for API and web-based administration tools, and centralized tamper-evident security log collection.

Network Redundancy

Our networking infrastructure boasts over 9 network providers with a network configuration developed in collaboration with Google Cloud Platform, Cisco and Arbor Networks. We exclusively use fully redundant, enterprise-class routing equipment under managed networks. In addition to this, our fiber carriers enter at disparate points to guard against service failure.

Load Balancing

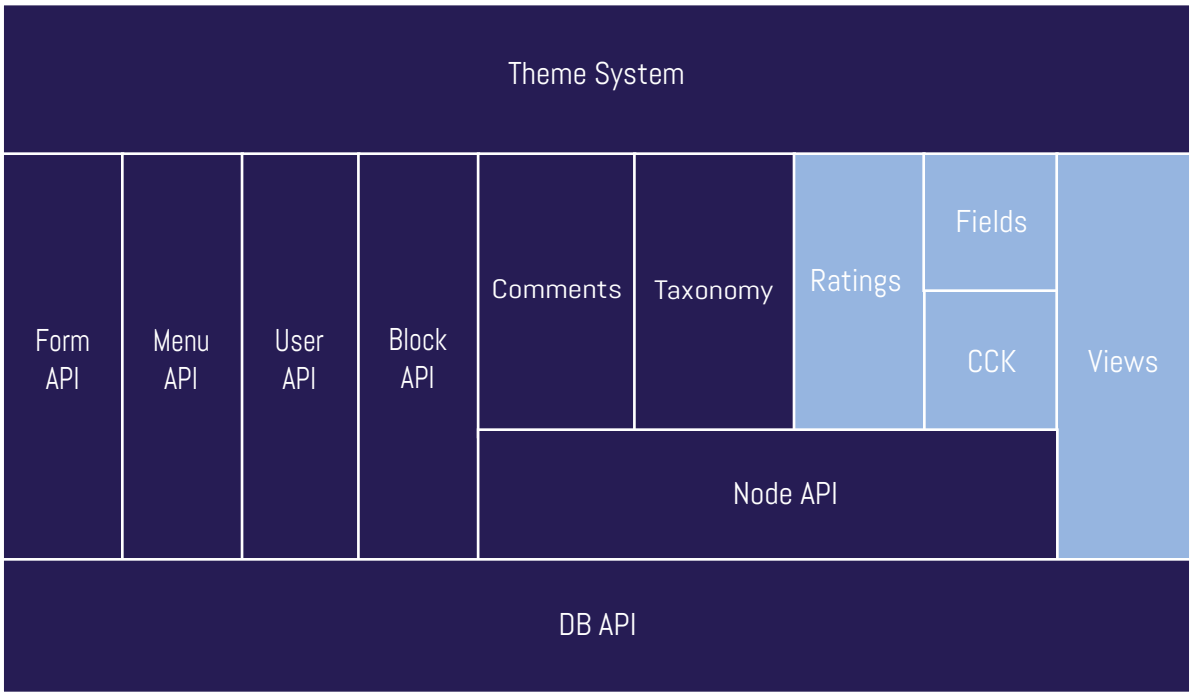
All portal requests through HTTP or HTTPS go through a load balancing server before being distributed to other servers and php workers deeper within our network infrastructure. This will ensure that your portal will stay up and running through peak traffic times.

Section 4: How We Secure Our Software

Our software is based on the popular, open source CMS Drupal, a system that is widely regarded as one of the most secure platforms in the world. Thousands of developers and a dedicated security team work to resolve reported security issues, review security concerns and provide security expertise and assistance. Furthermore, Pantheon provides an easy way to pull in the latest security fixes and core upgrades once they are released, allowing us to stay on top of addressed security bugs.

With the rich set of APIs Drupal provides us, security flaws such as Cross Site Scripting, Insecure Direct Object References and Cross Site Request Forgeries are easily mitigated, ensuring that your platform's information stays in the right hands.

Our software is programmed using an MVC framework that separates front-end logic from back-end, ensuring easy maintainability and increased security.



Secure Database API

This is a robust way of accessing your data when you need it. With this API, all database calls are sanitized and enforce an interface. In addition to this, our file system interaction layer limits where files can be written and alters dangerous file extensions that the server could potentially execute.

Secure Password Storage

Like all good web-based password storage methods, we use one way hash functions to encrypt your passwords, specifically SHA512 via the Portably PHP Password Hashing Framework. Passwords are additionally salted before being hashed for added security.

Account Security

In addition to password protection, we use honeypots in order to protect against bots that want to automatically log in. Administrator accounts have an extra layer of security that disable them if there are too many failed login attempts.

Session Management

All things relating to a user's session are managed by our server in order to prevent a user from escalating authorization up to the admin level. All session data is destroyed upon logging out and completely new session data is created when logging in to avoid session fixation.

Input Filtering

Anything that users can store on our database and show to others are filtered for malicious code such as malicious JavaScript, malicious flash embeds, and malicious PHP code.

Permissions System and Access Controls

Our platform has a very sophisticated permissions system that allows administrators to configure permissions for our users on the fly, whether they need more or less permissions for a particular task.

New roles can also be created on the fly if permissions need to be separated.

Code Versioning Systems

Impetus uses git for all of its platform software releases to ensure that code changes are logged and tracked with their associated programmer. This also ensures that per-platform customizations are done correctly and only for their intended customer. All code pushes, releases and updates require password authentication through an HTTPS connection.

Section 5: Our Policies

We have a number of policies in place that allow us to ensure that your portal and the data contained within that portal are as secure as possible.

Disaster Recovery

In the event that data does need to be recovered after a disaster, rest assured that your portal will be back up and running in a very short timespan. We've implemented the following to ensure the continuity of your business.

- Scheduled daily backups of all customer data are initiated within 2 hours of the scheduled time
- Backups are stored in multiple geographically distinct data centers using Amazon S3
- Backups are encrypted for both transfer and storage
- Backups include the all files and database tables required to get a portal back up and running.
- In the event of a disaster, we will restore customer portals.

Incidence Reporting

Impetus and its hosting services will consistently report and resolve any known or suspected security or privacy problems, incidents or breaches. These procedures will identify, contain and notify affected parties within 24 hours.

Disaster Recovery Testing and Auditing

Our network and hosting infrastructure is subject to quarterly internal risk assessments, and leverages external risk-assessments as necessary. Known risks are catalogued by severity and added to a prioritized backlog. Impetus keeps a close relationship with external hosting partners to ensure that backlogged issues found in testing are resolved.

Compliance

Impetus conducts all of its business in compliance with all US and Canadian laws, regulations, industry guidelines and codes including, but not limited to:

- DDMAC
- Health Canada
- ASC
- Rx&D
- PAAB
- PIPEDA
- GDPR
- all anti-corruption policies

Privacy

It is Impetus' policy to the use the personally identifiable information Impetus acquires in Impetus communities for internal business purposes only in order to provide the services that you have requested. Impetus maintains security measures to keep this information private and agrees not to re-distribute, market, share or sell this information to others.

We use a variety of security technologies and procedures to help protect Personal Information from unauthorized access, use or disclosure. We store Personal Information on computer systems with limited access, which are located in controlled facilities. When highly confidential information is transmitted over the internet, Impetus protects it through the use of encryption technologies such as the Secure Socket Layer (SSL) protocol. See our Privacy Policy for more details.

Impetus Digital
WaterPark Place | 20 Bay Street, 11th Floor
Toronto, Ontario, Canada M5J 2N8

connect@impetusdigital.com

+1 416-992-8557