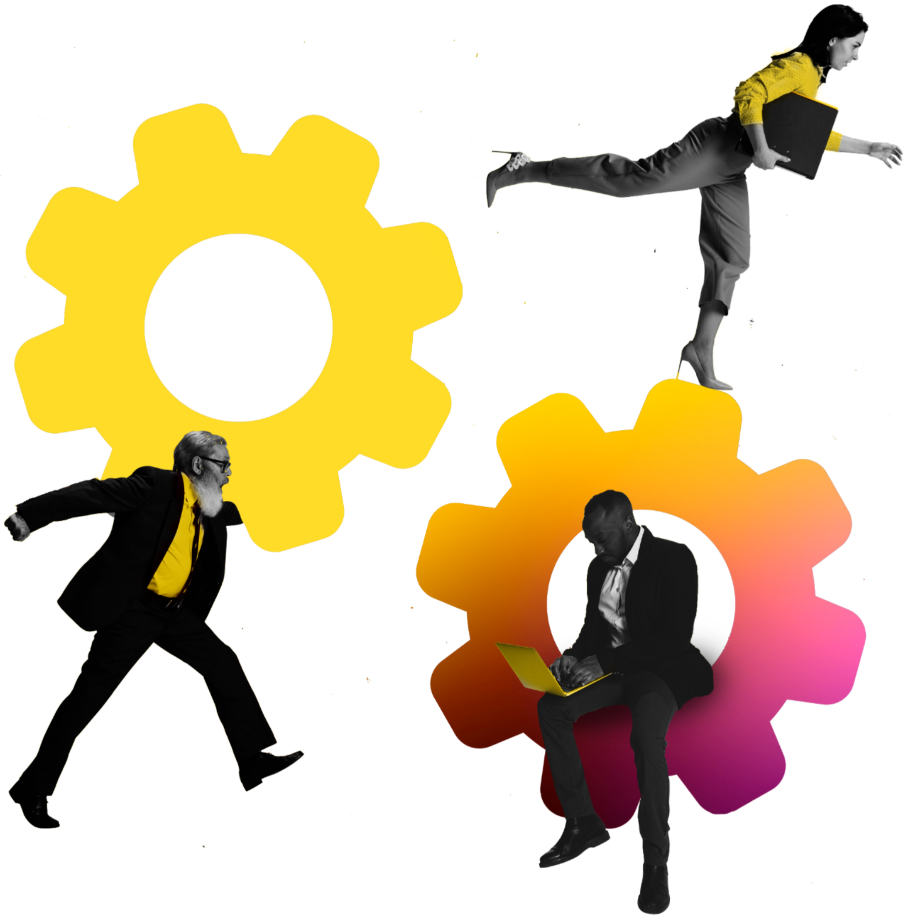
PANTHEON®

# WebOps Security: Automating Site Updates



## Importance of Site Security

One of the best ways to ensure that a website is secure is to regularly update the core CMS and all related plugins/modules/themes. Sites with out-of-date code do not have the most recent security updates and performance optimizations, and as a result are less stable, less secure, and at greater risk of experiencing downtime.

> **“60% of small companies close within 6 months of being hacked.”**

### User Data and Business at Risk

Organizations, large and small, often store sensitive information online — email addresses, usernames and passwords, data entered into online forms, and much more. If this information were to be lost or leveraged in an attack, it could mean the difference between a successful quarterly report and, in some cases, going out of business. In fact, 60% of small companies close within 6 months of being hacked. With both the financial security and future of the business on the line, it’s crucial for organizations of all sizes to have safety measures in place to secure their websites.

Further, about 35% of data breaches start with websites. Your website is on a server somewhere. That server is next to other computers on a network. In shared environments, it is likely that some of those computers have sensitive information and/or access to the next system in the chain that does. Once a hacker finds a crack in the door, they often have enough to move in.

> **“About 35% of data breaches start with websites.”**

© 2022 Pantheon Systems, Inc.

## Developers Need to Think About Security— Even if the Client Isn't

It may be true that your clients aren't asking specifically for website security, but they are paying you for it. Your clients expect site security, just as they expect you to anticipate and address their needs in other areas of site development. Further, by not implementing appropriate security controls, if there is a breach, you can be liable.

One example: In an effort to shift financial responsibility for a data breach at a community bank, Travelers Casualty and Surety Co. of America (insurer) filed suit against the bank's web designer, claiming its negligence and "substandard" maintenance of a website set the stage for a breach. As an agency, you can and should reduce your risk by implementing proper security for your clients, even if it means taking money out of your bottom line.

As many agencies that we interact with can attest, adding security as a line-item when responding to RFPs helped them win bids. It not only ensured their prospective clients that security was top of mind, but also instilled confidence in the competency of their agency.

## Small Sites = Big Target

Businesses large and small—public and private—have security needs. In fact, it is often a surprise to small and medium sized businesses that they are actually considered a greater target than large enterprises. Why? Because hackers know that SMBs are an easy target. According to a recent Forbes article, small businesses are three times more likely to be targeted by cybercriminals than larger companies. SMBs typically have weaker security controls and are not taking a defense in depth approach to data security—often because they are just not aware of security best practices.

## Personally Identifiable Information (PII)

Many websites collect Personally Identifiable Information (PII) and may not realize it. When there is a data breach, authorities ask whether or not PII was lost. If it was, fines are imposed, which can be detrimental to customer trust and a business's financial stability. Generally speaking, PII is any information that alone, or when combined with other information, can identify a unique, individual person - the stuff hackers are after. PII goes beyond just a credit card or social security number.  For example, the following can be considered PII:

- First name
- Last name
- Email
- Social media info
- Phone number

Pause for a moment and consider how many websites you have built that collect this type of information. As you will quickly realize, even the most basic marketing websites collect PII and are of value to a hacker.

## Out-of-Date Site are Like an Unlocked Door

Drupal and WordPress websites running outdated core versions, as well as older plugins, modules, and themes (for WordPress users), present a significant security risk. A WordPress security report by KeyCDN estimated that for those sites running WordPress, 52% of vulnerabilities targeted plugins, 37% were centered around WordPress core, and the remaining 11% were associated with themes.

Fortunately, with WebOps tools like Pantheon's Autopilot, developers can focus on innovation, rather than site maintenance. Autopilot automatically updates a site's CMS, plugins or modules, and theme.

## Pantheon’s Autopilot

Autopilot always keeps sites up to date and allows machines to automatically detect, perform, test, and deploy updates for WordPress and Drupal CMS solutions. Additionally, with Visual Regression Testing (VRT), users can intelligently detect visual and content changes through visual regression testing tools to compare and ensure optimal website functionality and excellent user experience.

> *“Autopilot saves time by effectively automating the upgrading process that ensures that our websites are up-to-date and can comply with international standards.”*
>
> - Ford Motor Company

If you’re not comfortable with Autopilot deploying all the way to the Live environment, you can have Autopilot only deploy updates to Dev or Test and stop. You can proceed with other manual or automated QA processes, and deploy from the Test to Live environment when ready.

You can specify the environments to which Autopilot deploys. When all tests pass, it can deploy to the:

- Dev environment only: A good choice for a site under continual active development
- Test environment (after Dev): A good choice for a high traffic site that needs an extra level of manual quality assurance (QA) or automated CI
- Live environment (after Dev and Test)

Autopilot can run on user-defined schedules. And since Autopilot is extremely customizable, developers can easily direct robots to exclude site theme code or customized plugins for specific clients.

© 2022 Pantheon Systems, Inc.

While there are update tools available in both Drupal and WordPress CMSs, Autopilot can leverage Pantheon's WebOps tools such as Dev/Test/Live, Visual Regression Testing, and automated backups.

## Conclusion

Maintenance risk and toil is probably the single biggest impediment to the open source CMS, the opportunity to apply machine learning capabilities and AI-driven testing to updating your core CMS, plugins, and themes allow for an improved level of scaled web performance.

By regularly updating the Core CMS and all related plugins/modules/themes, organizations can ensure that their websites are secure. When not routinely updated, websites are not optimized for performance and are less secure and at greater risk of experiencing downtime.

The Pantheon WebOps Platform increases the efficiency and effectiveness for delivering WordPress and Drupal websites that drive results. Handling uptime, performance, scale, and security, Pantheon delivers the fastest and most reliable and enterprise web content management solution. Autopilot is a built-in tool that automatically finds available updates, applies the updates to both WordPress and Drupal sites, and tests for errors to ensure updates are safe to deploy.