mySites.guru

Why you're getting downtime alerts (and why they matter)

How uptime monitoring works, what triggers downtime alerts when your site seems fine, and how to monitor hundreds of sites from a single dashboard.

Phil E. Taylor | 25 March 2026

You've probably had this experience: an email lands from mySites.guru telling you a site is down, you open it in your browser, and it loads perfectly. Frustrating.

But think about it from the other direction. Our server tried to reach your site three separate times and couldn't. If we can't get through, there's a decent chance your visitors couldn't either during that window.

How do the monitoring checks work?

Every 5 minutes, our custom-built monitoring engine checks each of your connected sites. We don't fire off an alert on the first failed request. Instead, we run three checks before we tell you anything:

1. We send a HEAD request to your site with a 45-second timeout. If it responds with a success code, we mark it as up and move on.
2. If the first check fails, we wait 10 seconds and send another HEAD request. This catches momentary blips like a slow database query or a brief resource spike.
3. If the second check also fails, we wait another 10 seconds and send a full GET request. Some servers handle HEAD and GET differently, so the final check switches methods to rule that out.

We only send a downtime alert if all three checks fail.

In the worst case, where each request hits the full 45-second timeout, we've spent over two minutes trying to reach your site before alerting you. In practice, failed requests usually fail fast (connection refused, DNS error), so the whole thing takes well under a minute.

When your site comes back, we pick that up on the next check cycle and send you a recovery notification.

Why do you get alerts when your site “seems fine”?

You check from your browser and it loads. So why are we saying it’s down? There are a few common causes.

Your host is blocking our IP address

This is the most common one. Hosting providers run firewalls and intrusion detection systems (ModSecurity, Fail2Ban, Imunify360) that automatically block IP addresses making repeated requests. If your sites are behind a corporate firewall, the same thing can happen. Our monitor hits your site every 5 minutes from the same IP, and some security tools decide that’s suspicious and block us.

The block might be temporary, lasting a few minutes to a few hours, or permanent until someone removes it manually. If you see your site going down and coming back up in a pattern, a temporary block is almost certainly what’s happening.

Your server is briefly overloaded

Servers have finite resources. During traffic spikes, heavy cron jobs, backup processes, or plugin updates, there may not be enough capacity to handle new requests for a few seconds. If our check lands during that window, all three attempts can fail.

This is especially common on shared hosting where your sites compete with other customers for the same resources. A full disk partition can cause the same kind of failure.

DNS resolution failures

If your domain’s DNS servers are slow or temporarily unavailable, we can’t resolve your domain to an IP address, and the check fails before it even reaches your server. Less common, but it happens, particularly with budget DNS providers.

SSL/TLS handshake failures

An expired or misconfigured SSL certificate, or an overloaded TLS stack, will cause the secure connection to fail before any page content gets exchanged. We treat that as a failed check.

What happens when all your sites go down at once?

If you manage dozens or hundreds of sites and they all show as offline at the same time, it's almost never a coincidence.

When all your sites live on the same server, they share a single point of failure. If that server has a problem, every site on it goes unreachable at once. Common causes:

- A runaway process or traffic surge eats all available RAM and the web server stops accepting connections
- Heavy background tasks (backups, malware scans, bulk updates) peg the CPU so hard that nothing else gets served
- The server hits its maximum concurrent connections and starts rejecting new ones
- The server's firewall sees our IP hitting many different domains and decides we're attacking it, blocking us across the board
- A brief network interruption between our server and yours

These events are usually short - 30 seconds to a couple of minutes - but our 5-minute check interval with 3-step verification means even brief outages get caught and reported.

If all your sites are on one server and they all go offline together, the server is the problem. Talk to your hosting provider about the resource limits on your plan, or consider spreading sites across multiple servers so a problem on one only affects part of your portfolio.

What can you do about it?

1. Whitelist our monitoring IP

Start here. Ask your hosting provider to whitelist this IP address:

```
165.227.239.229
```

Have them add it to their firewall's allow list so it never gets blocked or rate-limited. This solves the most common cause of false downtime alerts.

If you manage your own server, you can do it yourself. In CSF (ConfigServer Security & Firewall), add the IP to `/etc/csf/csf.allow`. In Fail2Ban, add it to the `ignoreip` setting.

2. Check your server resources

Frequent brief downtime across multiple sites on the same server usually means the server is underpowered. Look at your memory usage, CPU load during the times alerts arrive, and disk space. Your hosting control panel usually has graphs for this, or ask their support team.

3. Spread sites across multiple servers

If you have 50+ sites on one server, splitting them across two or three servers means a problem on one only takes down part of your site portfolio. It also makes troubleshooting easier because you can see exactly which server is having issues based on which group of sites goes offline.

4. Review your security software

Check that rate-limiting thresholds on your server or security plugins aren't set too aggressively. Monitoring traffic from a known IP every 5 minutes is not an attack.

5. Look at the timing

If your alerts cluster around specific times (say, every night at 2 AM), something scheduled on your server is probably eating all available resources during that window. Backups and bulk updates are the usual suspects - consider staggering your schedules.

Why should you take the alerts seriously?

We built the monitoring engine to avoid false positives. Three checks, pauses between each, a different HTTP method on the final attempt. If we send you an alert, our server genuinely could not reach your site after multiple attempts over at least 20 seconds.

If we can't reach your site, your visitors probably can't either. Each downtime alert represents a window where real visitors may have hit an error page or a timeout instead of your site.

The alerts aren't the problem. They're telling you about it.

Need help?

If you're still getting frequent alerts after whitelisting our IP, get in touch. We can check the response codes and timing from our end to help narrow down what's going on.

For the broader monitoring picture, see our complete monitoring and alerting guide.

Frequently Asked Questions

Why am I getting downtime alerts when my site appears to be online?

Your site may be temporarily unreachable from our monitoring server due to firewall rules, rate limiting, or brief server overloads, even though it loads fine from your own network. Our monitor checks from a fixed IP address, and some hosts block or throttle automated requests.

How many checks does mySites.guru make before sending a downtime alert?

Three separate checks with pauses between each. A HEAD request, then a second HEAD request 10 seconds later, and finally a full GET request 10 seconds after that. An alert only fires if all three fail.

What IP address does the mySites.guru monitor use?

All checks come from 165.227.239.229. Ask your hosting provider to whitelist this IP to prevent false positives.

Why do all my sites go offline at the same time?

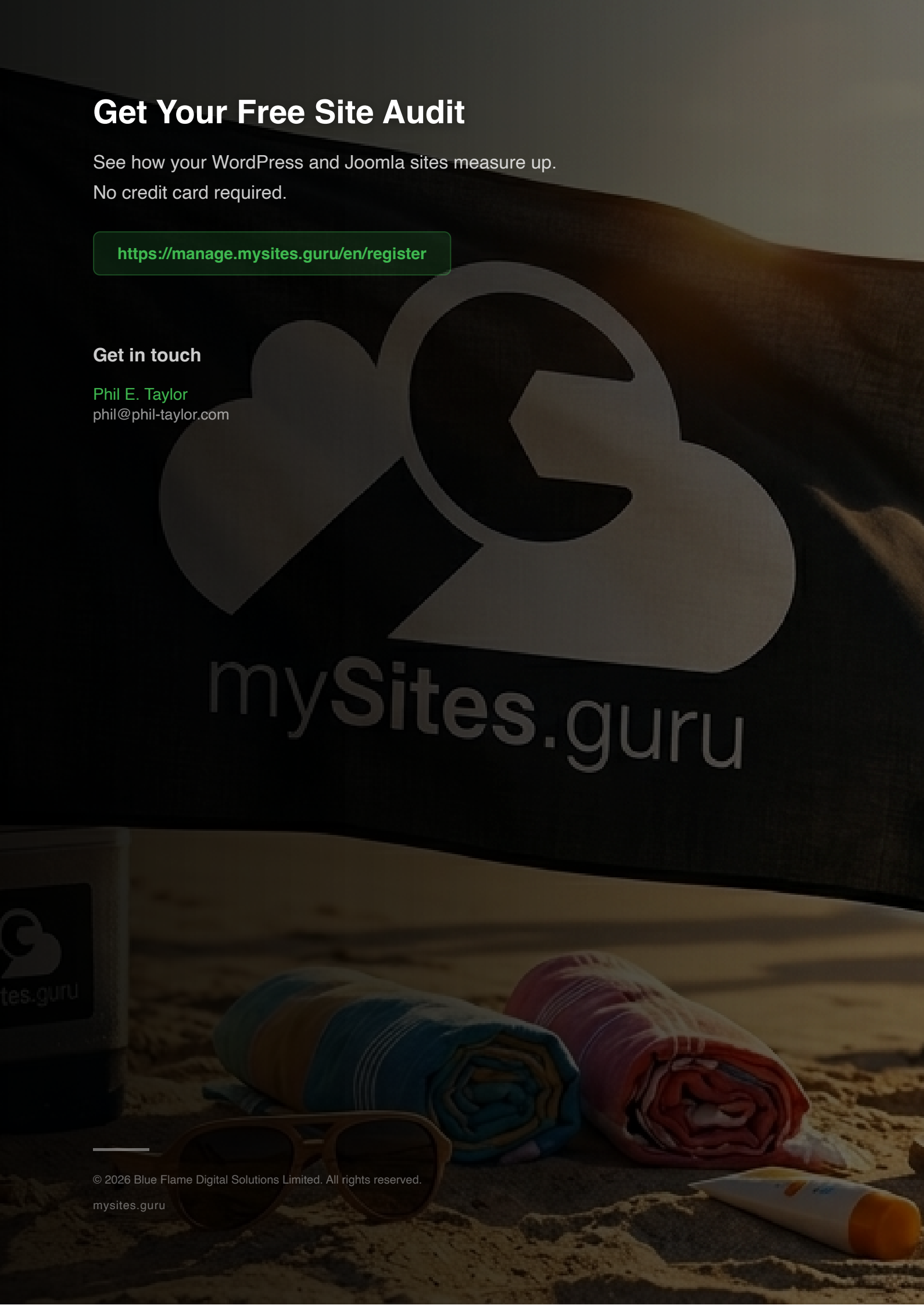
If all your sites share the same server, a brief overload, memory spike, or firewall rate limit will affect every site at once. The server is the single point of failure.

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

https://manage.mysites.guru/en/register



Get in touch

Phil E. Taylor
phil@phil-taylor.com