

DreamHost Powers Always-On Hosting with Proactive Visibility



INDUSTRY

Hosting & Cloud Infrastructure

PRODUCTS

Internet Performance Monitoring

SOLUTIONS

- + Internet Performance Monitoring
- + Public node visibility
- + Enterprise node-to-enterprise node testing
- + Provider escalation evidence

SUCCESS BY THE METRICS

- + Latency spikes validated at roughly 2x baseline
- + Provider issue isolated to Hurricane Electric
- + Oregon-to-Singapore issue traced to IPsec/IKE timer behavior
- + Tunnel flapping eliminated after timer changes
- + DreamHost moved from reactive customer-reported issues to proactive network issue detection

KEY OUTCOMES



Proved provider accountability



Accelerated root cause analysis



Improved escalation confidence



Supported more proactive always-on hosting



Protected customer experience

DreamHost is a leading web hosting and cloud services provider helping people own their digital presence.

In business since 1997, the company supports more than 400,000 customers and 1.5 million+ websites, WordPress blogs, and applications with open-source technology and 24/7/365 support. For a business that hosts and supports so much of its customers' online presence, reliable internet performance is closely tied to the experience those customers receive. Keeping websites and applications responsive and available requires visibility that extends beyond DreamHost's own infrastructure.

That broader visibility becomes especially important when performance issues appear outside DreamHost's environment. A degradation can originate with a network provider, somewhere along an internet path, or within DreamHost's own infrastructure, but the customer still experiences the result. DreamHost needs to identify the source quickly so it can respond appropriately, protect service continuity, and work with providers when the issue falls outside its control. Before fixing a problem, the team must first understand where it began and what is happening across the path.

As Brett Dunst, VP of Corporate Communications at DreamHost, explains:



The ideal outcome is that customers never notice an issue at all.

Seamless continuity is the goal. For DreamHost, that meant finding a better way to see what was happening across its network before customers ever felt an impact.

DREAMHOST NEEDED A COMPLETE PICTURE

Before implementing LogicMonitor's internet performance monitoring (IPM), DreamHost relied on a mix of vendor-specific tools and open-source monitoring solutions. Each solution gave the team visibility into specific components, but none provided a complete view of the environment. Monitoring was also concentrated on on-premises infrastructure, making it harder to track performance consistently as cloud services became more central to operations.

That fragmentation created several operational problems:

- Delays in issue identification, especially outside working hours
- Limits on correlation across infrastructure layers and related services
- Harder to hold providers accountable when a problem lived outside DreamHost's own environment

Before IPM, the team sometimes struggled to get timely visibility across their global infrastructure. They needed to get ahead of the sources of network degradation rather than learn about them only after they became a problem.

DREAMHOST NEEDED EVIDENCE IT COULD USE

DreamHost evaluated several options because it needed more than data alone. It needed a way to connect that data into something operationally useful in a complex hybrid environment. IPM gave the team broader context through public node coverage and more specific views of performance data, making it easier to understand what was happening across different regions and paths.

As Jiordan Villareal, Network Engineer at DreamHost, explains, "One of the biggest differences internet performance monitoring has made for us is that it provides us a bevy of data that we can bring forth to our providers." Villareal also said, "I like being able to see the dispersed public nodes globally that we have set up for our endpoint testing." Those views gave the team more than visibility. They gave the team evidence that could be used to investigate issues, prove where they started, and move conversations forward faster.

DreamHost Moved Faster From Signal to Root Cause

After implementation, DreamHost immediately saw value. The platform simplified alert triage and improved correlation across servers, networks, and logs, strengthening team confidence that it was seeing the full picture rather than isolated pieces. The monitoring data helped DreamHost move from a component-level view to a broader operational view, making escalation paths more effective and root cause analysis faster.

Jiordan also pointed out that the team does not need to guess whether an issue is within DreamHost or elsewhere along the path. That matters because the company needs to know whether the problem is in its own environment, in a provider network, or somewhere farther out on the internet. IPM helps the team answer that question with evidence rather than assumption.

DreamHost operates in an environment where even brief periods of poor performance can affect trust and service continuity. With IPM, the team can identify problems earlier, work with providers using objective evidence, and minimize customer-facing disruption. Brett captured that point well when he said, "In the best possible scenario, a customer wouldn't have any idea that we had this implementation at all." That is the continuity DreamHost is aiming for.



DREAMHOST MAKES MORE INFORMED MITIGATION DECISIONS

DreamHost also uses IPM during severe distributed denial-of-service (DDoS) activity to determine when traffic needs to be blackholed or null-routed upstream. The monitoring data helps the team decide whether an attack is severe enough to threaten not just the targeted customer, but the broader customer experience as well.

That additional visibility matters because upstream traffic mitigation is never a decision the team wants to make lightly. It can protect the broader environment, but it can also affect the targeted customer. IPM's alerting and metrics give DreamHost the context it needs to make that call more quickly and with greater confidence.

Instead of spending time reconciling conflicting datasets, engineers focused on identifying root causes and improving application performance.

“ Since picking up LogicMonitor's internet performance monitoring, we've been able to be a lot more proactive versus reactive to network issues.”

Ian Clark, *Director of Infrastructure Engineering at DreamHost*

That is the shift DreamHost wanted, because it allows the team to focus on problems before customers feel them.

DREAMHOST PROVED A PROVIDER ISSUE

One of the clearest examples involved the PDX-to-IAD route. DreamHost observed significant latency and packet loss while traffic was transiting Hurricane Electric, and the latency spiked to roughly twice the baseline. The traceroute and hop-by-hop visuals showed RTT increasing after traffic entered Hurricane Electric's network, making it clear that the problem was not limited to DreamHost's own infrastructure.

DreamHost is responsible for the customer experience, even when the root cause sits outside its own environment. If a provider issue causes degradation, DreamHost still needs to explain the issue, protect its customers, and make the strongest possible case to the provider. IPM helped DreamHost do exactly that by showing where latency began and providing objective evidence for escalation.

The provider later confirmed that a faulty patch on a circuit between Chicago and Ashburn had caused flapping and congestion until it was replaced. DreamHost said that the monitoring data helped push the case forward, and the team has since received faster responses when it brings provider issues to the table with reliable evidence.

The main value here was straightforward:



Prove where the issue began with objective network evidence



Escalate to providers with data they could act on quickly



Move investigations forward with more confidence

DREAMHOST ISOLATES PRIVATE NETWORK PROBLEMS

A second incident involved connectivity between Oregon and Singapore. At first, the path looked like a provider or transit issue because the route was long, complex, and easy to misread. Public tests and manual traceroutes did not show the kind of loss that would have made the answer obvious, which is why the team needed a deeper view into the path.

Enterprise Node-to-Enterprise Node testing ruled out the public internet and shifted the investigation to the private datacenter path instead. That view revealed recurring drops and tunnel flapping, ultimately traced to Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) timer behavior. Once the timers were offset so that one side became the sole rekey initiator, the tunnel stabilized, the flaps stopped, and the environment returned to a healthier state.

DreamHost Is Extending Proactive Visibility

With IPM embedded in its daily operations, DreamHost continues to expand its use of the platform.

Future priorities include:

- Broader monitoring across more cloud services and platforms
- More automation to reduce manual intervention
- Better service visibility through a connected service catalog

DreamHost is also looking at how monitoring data can support a broader service catalog, which would make it even easier to show what is green, what is online, and what needs attention. That is a natural next step for a team that already knows the value of seeing the full picture in one place.

For DreamHost, the value of IPM lies not only in helping the team explain incidents after the fact. It helps the team operate more proactively, identify the right fault domain more quickly, and prevent customers from feeling the impact in the first place.

That is what always-on hosting requires, and it is why proactive visibility matters so much to the DreamHost team.

ABOUT DREAMHOST

DreamHost is a leading web hosting and cloud services provider helping people own their digital presence. Since 1997, DreamHost has supported more than 400,000 customers and 1.5 million+ websites, WordPress blogs, and applications with open-source technology and 24/7/365 support.

ABOUT LOGICMONITOR

LogicMonitor® is the AI-first platform for Autonomous IT, enabling enterprises to operate complex digital systems with greater resilience, efficiency, and confidence. By unifying visibility from user to code across infrastructure, cloud, Internet, and digital experience, LogicMonitor delivers the intelligence required to anticipate issues, eliminate blind spots, and take action automatically. Powered by Edwin AI, LogicMonitor helps IT and business leaders reduce operational toil, protect revenue, and accelerate innovation in an increasingly complex digital world. For more information, visit www.logicmonitor.com and our blog, or follow us on LinkedIn, X, Facebook, and Youtube.



Learn how LogicMonitor's internet performance monitoring helps you keep customers online.

REQUEST A DEMO