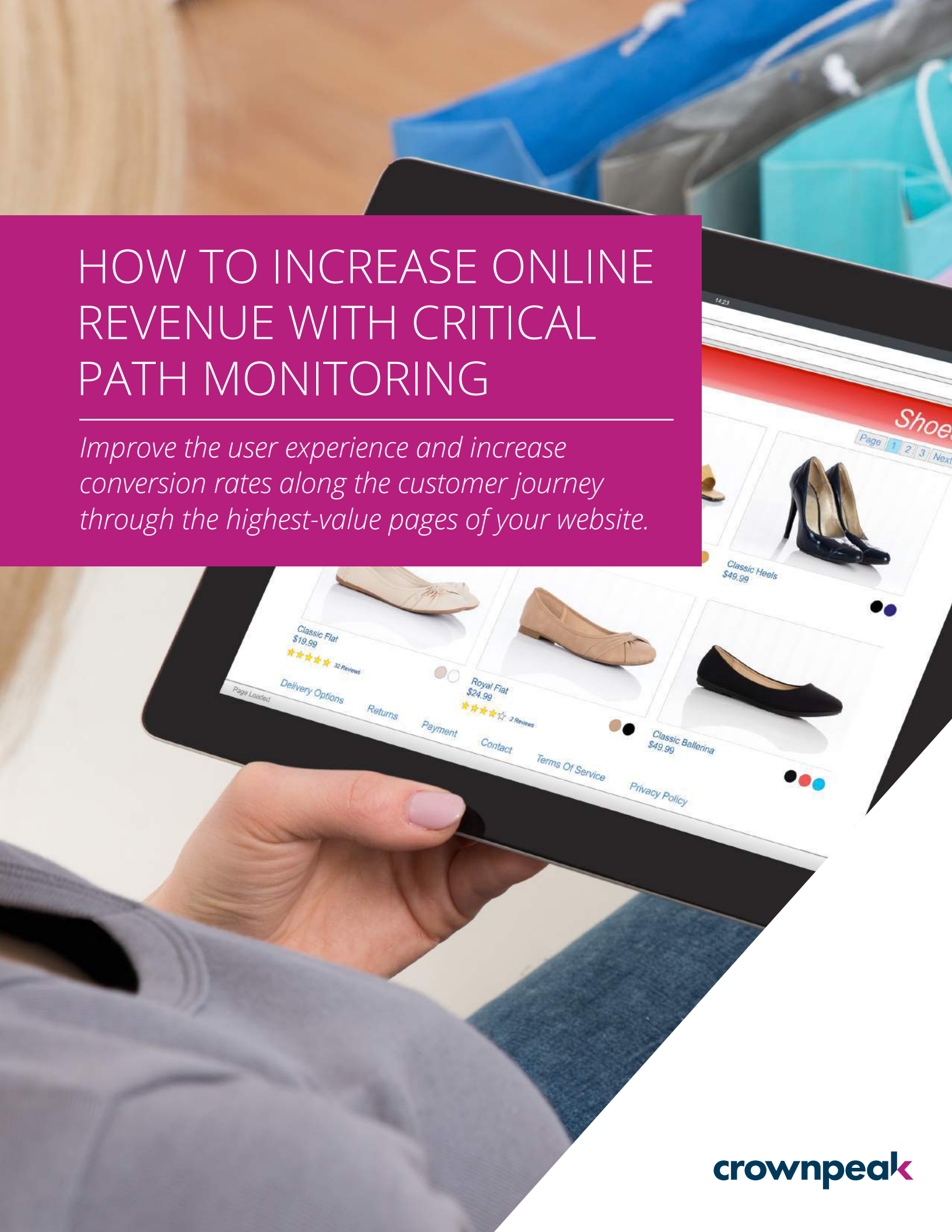


HOW TO INCREASE ONLINE REVENUE WITH CRITICAL PATH MONITORING

Improve the user experience and increase conversion rates along the customer journey through the highest-value pages of your website.

crownpeak

Year after year, optimizing your e-commerce experience to cope with peak selling periods becomes more important, as consumers do more of their shopping online:

According to eMarketer, e-commerce accounted for 10.6% of total retail sales during the 2016 holiday season; in 2017, it was expected to make up 15.8% of sales.[1]

During these high-demand periods, it's crucial to minimize downtime, avoid latency, safeguard customer data, and maximize functionality, especially on the paths critical to delivering revenue. These may include a common sequence of pages leading up to the check-out process, pages visited during the check-out process, or a route that leads to an email subscription form submission page.

While there are many well-documented best practices for increasing conversions, there's one that is commonly overlooked: **the optimization of third-party implementations**, also referred to as the digital supply chain.

The digital supply chain is an online ecosystem comprised of a myriad of technologies that facilitate e-commerce functionality and marketing campaigns, providing a wealth of benefits to organizations, like analytics, data management, retargeting, and conversion tracking, among others.

Although many of these technologies are mission-critical for both maximizing and measuring today's marketing campaigns, they can cause a litany of issues behind the scenes. In this paper, we'll explain how ensuring they behave properly can improve user experience and increase revenue.

UNDERSTANDING HOW TAGS WORK

Today, the average website depends on over **75** third-party technologies!

These technologies are powered by tags - a piece of code you add to your website that helps integrate them with your website or mobile app.

To understand the issues tags can introduce, we first need to understand how they work.

In practice, tags function like this: a user launches a web page, the browser reads and initiates the page's source code, and executes the scripts found on the web page.

Some specific examples of what a script in a tag might do:

- Set cookies to remember a user's preferences, behavior, or the items they've added to their shopping cart
- Place third-party content (from YouTube, for example) into a website page
- Track conversions from ad campaigns you run on third-party sites like Facebook, LinkedIn, Twitter, etc.
- Provide metrics on user engagement with your website via Google Analytics

If you're already familiar with how tags work, this seems straightforward, right? Well, not always. Often, the third-party vendors you've contracted with, **partner with *other* vendors** (often unbeknownst to you) to help them better qualify and reach specific user segments, for example. So the tag you add to your website gives your vendor's partner the ability to process and analyze ***your*** website data too.

In this case, when a script executes, it delivers another tag to the page. That tag then fires, and can return scripts itself. With each "hop," new tags can be deployed on the site – meaning this other vendor (that you have no direct relationship with) gets access to a wealth of data about the user visiting the page.

When you multiply that by ten or twenty tags on your website, it's easy to see how the user's privacy and their interaction with your site can be threatened.

HOW TAGS CAN DAMAGE THE USER EXPERIENCE

Although tags provide an invaluable source of visitor intel and undeniably more effective (and trackable) marketing campaigns, they contribute to an ever-increasing digital supply chain that can imperil a safe and seamless user experience.

Some common negative implications tags can cause:

- **Site Performance**
  Too many tags or improperly implemented tags can increase latency and compromise the end user experience leading to cart abandonment or higher bounce rates.

- **Failure to Execute**
  As critical as a tag may be for an aspect of your business, sometimes tags fail to fire. When a tag misfires or doesn't fire at all, data can't be collected and revenue opportunities are often lost.

- **Loss of Control**
  When you add a tag to your site, you relinquish some control of your visitor data and give it to a third-party provider and their partners. As you add more tags to your site, more third-parties gain access to your customer data.

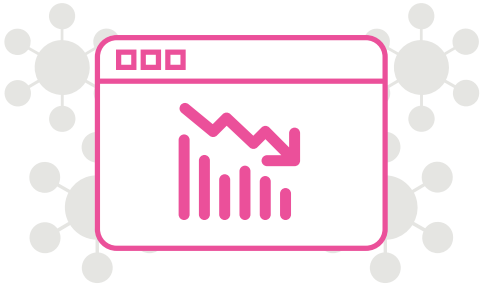
- **Access by Unknown Parties and Data Leakage**
  Redirects, or daisy-chains, are partnerships established between technology vendors to better qualify and reach a user base. While beneficial, these vendors gain indirect access to valuable audience and page data through partner networks, which, if not monitored closely, can be leveraged to compete against known partners, resulting in higher advertising costs. This is often referred to as audience data leakage. There are also security challenges that this can pose.

- **Data Privacy and Security**
  Under the General Data Protection Regulation (GDPR) and other laws that govern data collection, you are responsible for protecting the privacy of your website visitors. When you give third-parties access to your user data, you're accountable for how that data is collected, stored, and used. So, with every

vendor you enable, you increase your risk of facing non-compliance fines or brand reputation damage for someone else's carelessness.

> ***"Marketing is on the front lines of risk when it comes to cyberattacks...because the biggest application marketing uses—the website—is a prime target. 75% of IT leaders surveyed believe vulnerabilities from marketing infrastructure will be the source of a breach."***
>
> ***–RSA Security*** [2]

EXAMPLES OF HOW TAGS CAN RESULT IN LOST REVENUE



Because one can't fix what's not seen, when tags introduce performance challenges, the time it takes to be notified of the issue and to remediate it can increase exponentially. Here are a couple of real-world use case examples of the problems tags can cause:

1. Technology Error

The Scenario:
To test which landing page is most compelling, an e-commerce marketer uses a third-party technology to test whether "Headline A" or "Headline B" garners more conversions. After reviewing the aggregated metrics, the data seems skewed – only metrics from one region are being collected.

What's Happening:
The technology being leveraged for this multivariate test has failed to fire properly.

Business Impact:

- Incomplete datasets
- A/B test is inconclusive
- Lost revenue

67% of site operators think that there are third-party technologies on their site that they are unaware of, and 79% say that they have directly impacted site performance.

-2016 Evidon Survey on the State of Digital Governance[3]

2. Non-Secure Content Warnings

The Scenario:
Ready to book an online cruise, the user navigates through the conversion funnel and is interrupted with a mixed content warning, asking if they are sure they want to proceed. The user no longer feels safe inputting their credit card and exits the site.

What's Happening:
The page contains a tag that is attempting to load a non-secure (http) technology on a secure (https) page, prompting the browser to signal to the user that the page contains mixed secure and non-secure elements.

Business Impact:

- Lost revenue
- Poor user experience
- Diminished brand trust
- Security vulnerability

> ***"Applications leveraging public cloud, APIs, and the Internet are highly dependent on factors beyond IT's control … [related] to a lack of visibility into the details of application execution."***
>
> ***-EnterpriseManagement.com[4]***

These are just a couple examples of how tags can compromise the performance of a website. These issues and countless others can be avoided by using **Critical Path Monitoring,** an automated tool that emulates a user's behavior along a specified high-value online pathway in order to identify any sticking points that may threaten the user experience and negatively impact revenue.

TAG OPTIMIZATION BEST PRACTICES CHECKLIST

To improve governance of your tags, we suggest starting with these best practices:

- [ ] Define and publish a set of tag standards to proactively determine vendor criticality
- [ ] Identify whether the availability of your webpages is dependent on these third-party resources
- [ ] Leverage free browser tools, such as SPOF-o-meter to identify third-party single points of failure (SPOFs)
- [ ] Eliminate expired and unused partners, and update URL protocols where applicable
- [ ] Establish a baseline for performance of your vendor technologies and keep tabs on fluctuations over time – during peak and off-peak periods
- [ ] Finally, leverage a platform like Critical Path Monitoring to automate monitoring third-party services in real-time during key junctures in the customer journey.

HOW CRITICAL PATH MONITORING CAN HELP

The most reliable way to protect and enhance the user experience requires real-time visibility into the tags on your website and their impacts. Without this visibility, intent-rich moments (e.g. the checkout process) can be jeopardized without anyone in your organization knowing.

With **Critical Path Monitoring**, you can choose pre-defined user paths and our proprietary scanning technology will simulate the user experience to identify when and where tags might result in higher bounce rates, increased shopping cart abandonment, or cause an otherwise negative user experience.

Here's how it works:

1. Select the sequence of pages that you'd like to scan (your business-critical paths). This might be your subscription sign-up, a registration page, conversion funnel, or any other revenue-generating pathway.

2. Choose the frequency that you'd like the scan to run (choose hourly, daily or weekly).

3. Choose the specific issues that you'd like to be alerted to when discovered. These might vary depending on your focus. For example, latency alerts protect against gaps in analytics data and missed ad revenue, while unapproved alerts protect against exposure to data leakage and compliance concerns.

4. Choose the geography that you'd like to scan from (different geography exposures can lead to different technologies activating) and the experience you'd like to scan from (e.g. desktop, mobile).

5. Where applicable, input the appropriate page interactions that need to be simulated. This might mean including the option to scroll, click, and input text.

6. Set up alerts within each path you'd like to monitor, and you'll receive notifications when issues arise with tags found on these critical pathways.

SOURCES

1. *https://www.emarketer.com/Report/US-Holiday-Shopping-Preview-2017-Recapping-2016-Looking-Ahead-This-Season/2001992*

2. *https://www.forbes.com/sites/kimberlywhitler/2017/11/01/2018-marketing-predictions-from-the-c-suite/#240a5a8d4c91*

3. *https://www.evidon.com/blog/digital-governance/new-research-digital-governance/*

4. *https://www.enterprisemanagement.com (Taming IT Complexity with User Experience Monitoring)*

crownpeak

crownpeak.com

About Crownpeak

Crownpeak provides the leading, enterprise-grade, cloud-first Digital Experience Management (DXM) platform. The Crownpeak DXM platform empowers Fortune 2000 companies to quickly and easily create, deploy and optimize customer experiences across global digital touchpoints at scale.

Besides featuring content management, personalization, search, and hosting, it is the only digital experience platform that includes built-in Digital Quality Management (DQM) to ensure brand integrity, best practices, and web accessibility compliance.

Recently, Crownpeak acquired Evidon, the leading provider of simple technical solutions to complex digital Governance, Risk & Compliance (GRC) challenges, including a Universal Consent Platform, designed to help companies comply with the General Data Protection Regulation (GDPR).