Digital Risk Management in 2021

A Cross-Industry Examination of Residual Risk in Enterprise Websites

THE MEDIA TRUST

We know digital security.

A False Sense of Security

Digital attack surface is larger and more vulnerable than expected

Imagine this: it's the beginning of Spring, and you're excited to begin a long-needed home renovation project. You select Bob, a trusted, well-known contractor. On the first day, Bob shows up with a handful of subcontractors, many of them expected. But as the day wears on, more unknown characters arrive: by the end of the week, your house is littered with trash and several personal items appear to be missing. It's clear that Bob hasn't done a great job vetting his subs and you hesitate to recommend his services to others.

This same scenario occurs in enterprise websites and mobile apps: hundreds of unmonitored third-party domains are present every time a consumer accesses the digital asset. Eventually domain drift sets in, meaning that new and unknown domains appear on a daily basis and change the way your website operates. It's as if unknown subcontractors show up to your home every day. This ever-changing situation contributes significantly to your digital attack surface, and if unmanaged, third-party domains will target your customers for nefarious purposes using cookies, digital fingerprinting and other data collection techniques.

The data is clear: third-party domains are driving a massive rise in fraud, malware and disinformation across the web. At the beginning of the COVID pandemic, online fraud increased more than 400% and Magecart attacks rose 3.5X when malicious third parties took advantage of a disaster by exploiting popular websites across many industries.

Businesses are suffering from a digital pandemic, and it is getting worse every day.

The Web is the World's New Battleground

"In the wrong hands the Web could become a destroyer of Worlds." - Tim Berners-Lee

Today, organizations realize that digital is important: they care about transformation efforts, internal data systems, email, and communication apps. But not enough attention is spent on consumer-facing apps and websites that directly affect the end consumer, and how the consumer digital experience drives digital risk.

Digital risk mediated through the World Wide Web (WWW) affects customers during any stage of their journey—from discovery through checkout. Overwhelmingly, the biggest driver of risk is a lack of ownership and insight that leads to an abundance of unmonitored vendors, malicious cookies, and domains.

If not addressed, these risks harm consumers via:

Delivering a poor user experience (UX)

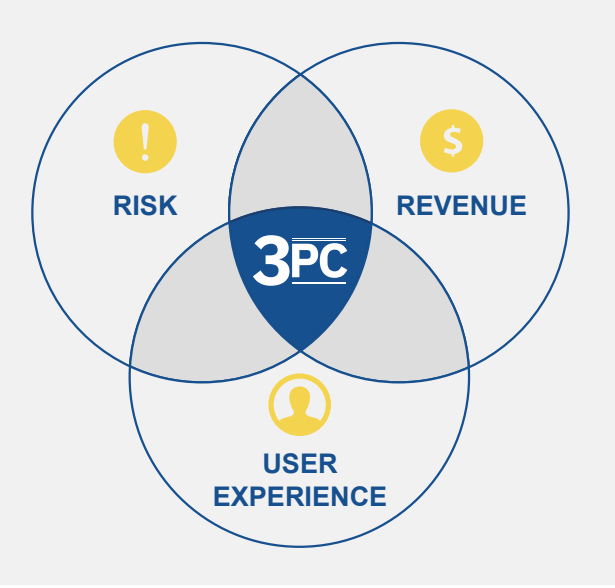
Violating personal data privacy expectations

Enabling credit/payment card theft

First-party vs. Third-party Code is Significant in Digital

The dynamic nature of digital highlights the amount of unmanaged code executing across websites and mobile apps

Enterprise IT teams typically focus on first-party code; it is owned and/or directly operated by their organization. However, today's digital assets are primarily composed of third-party code which is written and managed by someone outside of the enterprise. This third-party code—analytics, virtual appointments, plugins, online chat, libraries, payment systems, and more—only executes client-side on the consumer device.



FALSE PROMISES AND ASSURANCES

Security scorecards only evaluate 10% of your digital asset risk, and do not account for domain drift and other risks brought by third, fourth, fifth and nth parties

Big 6 security consultants consistently fail to accurately report on the third-party code running on digital applications

Data privacy platforms do not provide data to help you *stay* compliant in a highly-dynamic environment like digital

Popular commercial blocking applications rely on outdated information and often "misfire," leading to crippled performance and further UX issues

Third-party risk management providers lack insight into the ever-changing nature of digital domains and their data-collecting activities

In the grand scheme of things, unmonitored third-party code lies at the intersection of **risk**, **revenue**, and **user experience**. The ability to identify and control third-party code leads to improvement in all of these three areas. Unfortunately, companies who have attempted to gain control are often misled by false promises and vendor assurances.

In reality, less than 10% of the code across Alexa 500 websites is owned or operated by the host organization.

2021: Your Digital Assets Are (Still) Not Secure

Lack of control and insight into client-side executing code exposes enterprises to customer hijacking, regulatory fines, and revenue loss

When it comes to the 90% shadow code executing across their digital environments, businesses are completely in the dark. They fail to maintain their security and compliance posture in the face of invisible risks that have real consequences.

The enterprise digital attack surface includes all executing code that renders the user experience—both first-and third-party. Client-side analysis of digital journeys presents a more complete picture of the dynamic user experience and potential vulnerabilities. Not only are the digital risk artifacts different for each industry but it also constantly changes.

Just like how Bob's subcontractors can wreak havoc on your home, third-party domains wreak havoc on your website and customers. It is also a betrayal to consumers, who reasonably assume they are dealing directly with your business and a handful of trusted vendors—not hundreds of unknown third parties that regularly cycle in and out.

Artifacts of Digital Risk

Bob + 50

DOMAINS

More than 90% of the vendors contributing to your website and mobile apps are third parties whom you do not control.

BOB

You hire Bob to do the job but 50 other unvetted contractors show up to your home.

Bob + 50

DOMAIN DRIFT

The domains on your website are constantly cycling and this variability leads to increased risk.

BOB + 50 NEW PEOPLE DAILY

Bob brings new contractors to your house every day. Even if you fire the bad ones, new ones appear.

50 New People

COOKIE VOLUME

The known and unknown vendors in your digital ecosystem are collecting large volumes of data from your customers.

BOB'S SUBS SELLING YOU MORE

These unvetted subcontractors are knocking on your door daily trying to sell you things. Even worse, they've sold your personal information to others.

To make matters worse, digital environments are not static, and variability leads to increased risk in the form of domain drift. On average, websites may experience **digital drift of up to 45% per month.**

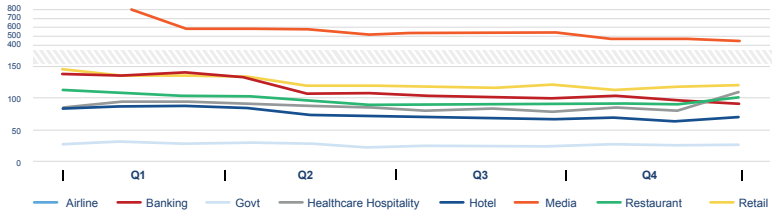
This variability signals a lack of control over your digital environment and increased risk to your customers. Using old and emergent tracking technologies, malicious domains will identify your users and target them with competitive or fraudulent offers. **More than 100 domains can be found on an average website—3X more than most IT teams expect—and many of them remain active for years.** Ultimately, this leads to lost customers, missed revenue, and regulatory violations.

Industry Insights Reveal Risk Posture

Benchmarks establish risk profiles for key consumer-oriented websites

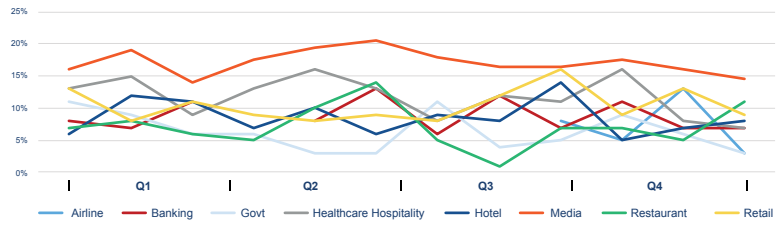
During 2020, uncontrolled digital risks affected businesses across multiple industries in measurable ways. Analysis of more than 100 consumer-oriented websites across 8 key industries reveals:

Executing Domains | Client-side Code



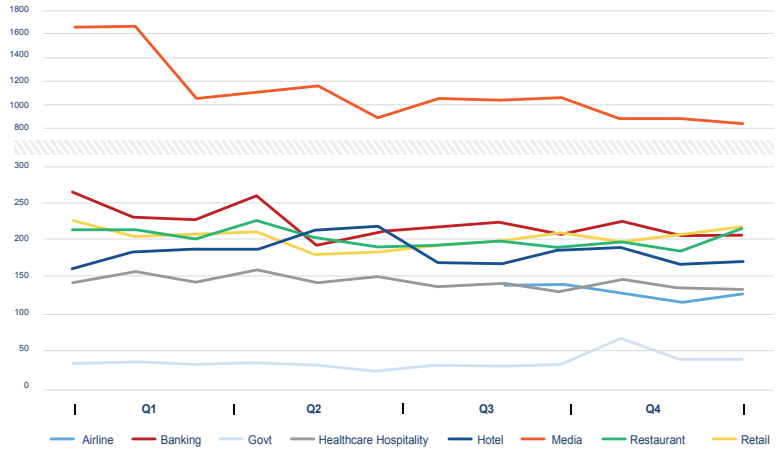
Each time a consumer accesses a website the average amount of executing code ranges from 57 domains (airline) to more than 576 (retail)

Domain Drift | New Domains Introduced Each Month



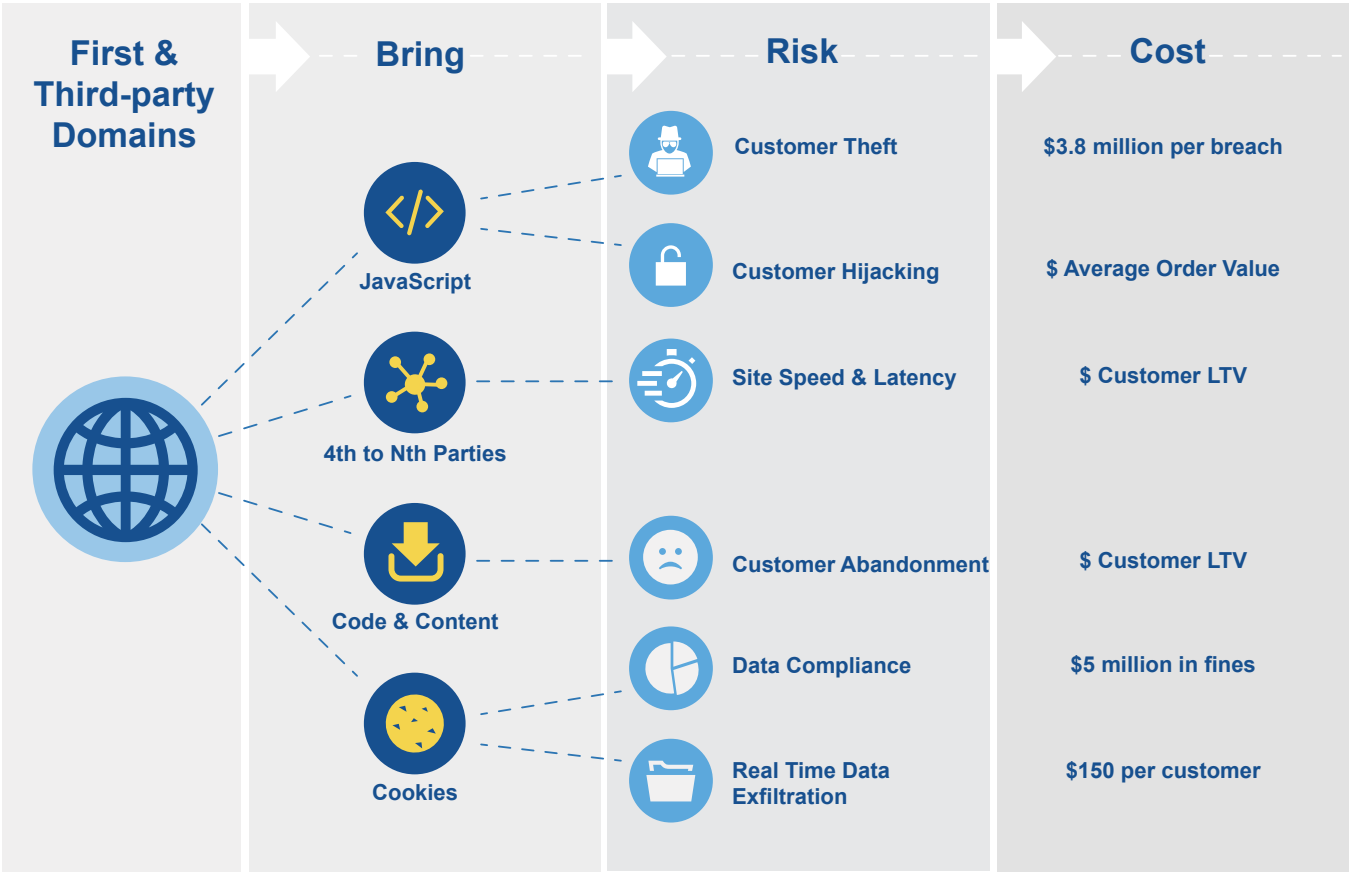
Domain Drift spans from 7% (airline) to 17% (media) on average each month.

Cookies | Average Number of Cookies Per User Access



Minimum number of cookies dropped per consumer access fluctuates from 131 (airline) to 3938 (healthcare)

Highly-publicized incidents in three major industries can be connected to a rise in unmonitored third-party domains, illustrating the serious consequences of complacency. To protect their revenue and customers, businesses must actively monitor the domains executing across consumer-facing apps and websites.



RESTAURANTS

In the middle of COVID lockdowns, restaurants across the world turned to food delivery service to fill orders for customers in quarantine. Analysis of 10 well-known restaurant chains reveals:

- **98 executing domains**
- **90% of domains aren't owned by the restaurant**
- **9% domain drift**
- **2% of domains are high-risk**
- **201 cookies (at least) drop during every visit**

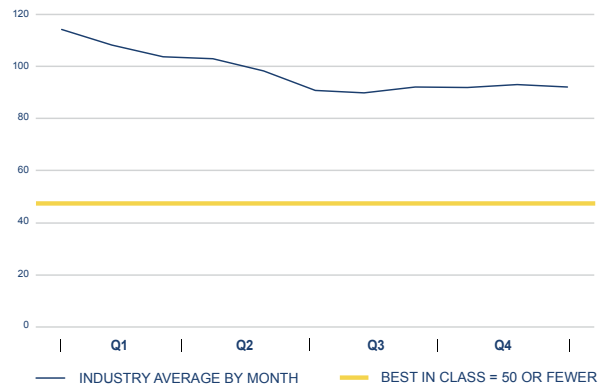
IMAGINE: A customer places an order for family dinner through your website. Dozens of shadowy figures watch over their shoulder as they enter their payment information. They claim their presence is necessary—that they are simply working for your restaurant. One inserts its code on the payment page of your online ordering system, and the customer arrives to pick up a prepaid order that is missing payment information.

REALITY: In April of 2020, New Jersey-based sandwich shop Primo Hoagies alerted customers to a data breach that included stolen names, addresses, payment card numbers, expiration dates and security codes. The attack was caused by unauthorized third parties executing on their digital assets who accessed online purchase data.

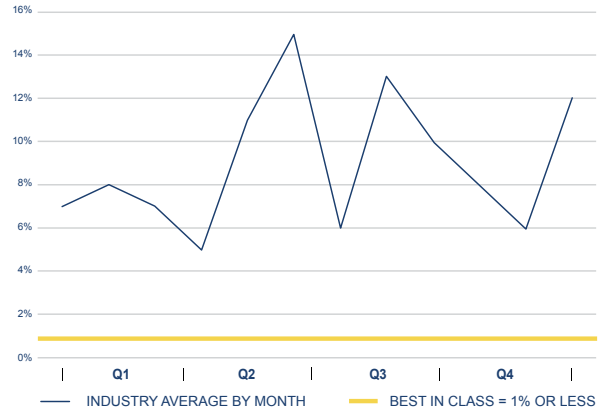
Restaurant Benchmarks

Throughout 2020, when a typical consumer accesses a restaurant website they experience:

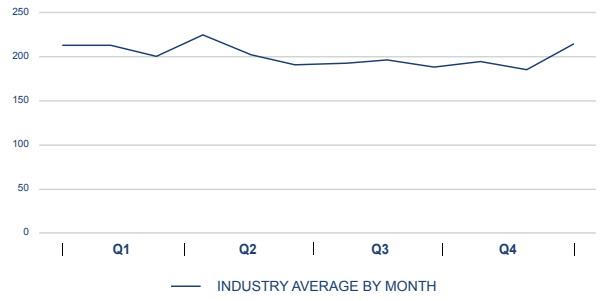
Domains



Domain Drift



Cookies



If third-party code and it's activity is left unmanaged, restaurants are vulnerable to compromise and violating consumer data protection regulations.

RETAIL

eCommerce channels have always been a popular target due to the presence of customer data and credit card information. Last year, many retailers quickly pivoted to online orders and/or experienced a rise in traffic as consumers turned to the Internet for essential items and health products. Consequently, attackers used third-party domains to target and steal sensitive information from visitors. Based on analysis of 19 well-known stores, the retail benchmarks reveal:

- **124 executing domains**
- **91% executing code are not controlled by the retailer**
- **11% domain drift across retail websites**
- **2% of domains are high-risk**
- **203 cookies (at least) drop during every visit**

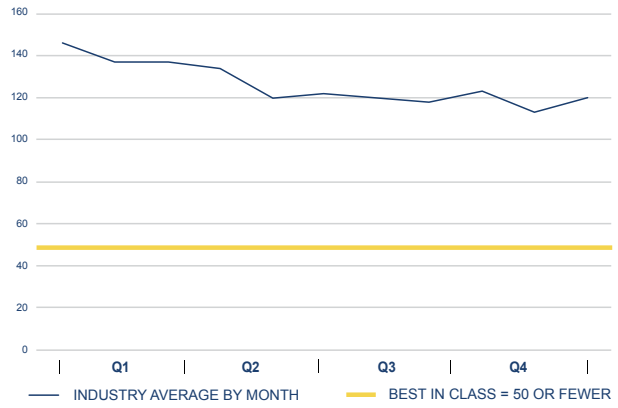
IMAGINE: a customer signs up for your retail loyalty program through a mobile app. Along the way, more than 200 unauthorized third parties are listening in. Some snag consumer information to sell to your competitors; others harvest IP addresses for a future attack. All bog down the load time for your special offer, and the customer eventually gives up in frustration. They know something is wrong even when your organization doesn't.

REALITY: Nutribullet—a popular food blender—became the victim of Magecart, a credit-card skimming attack based on third-party code that watches shopping cart transactions. Starting in February, bad actors were able to inject their credit card-stealing script on at least three occasions.

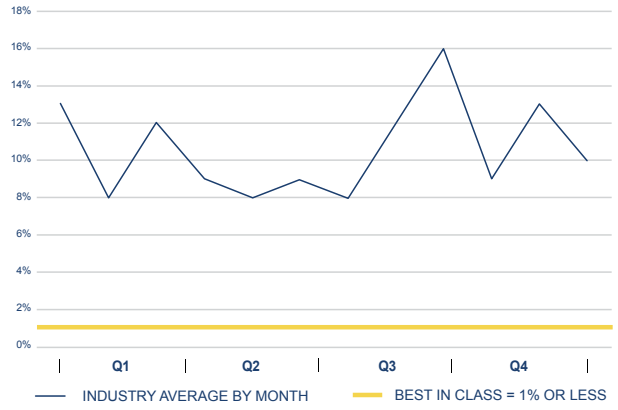
Retail Benchmarks

Throughout 2020, when a typical consumer accesses an ecommerce site website they experience:

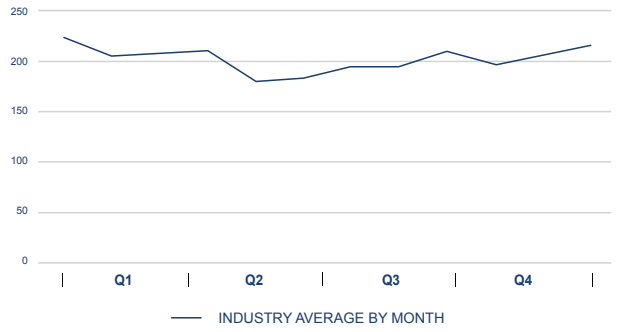
Domains



Domain Drift



Cookies



Inability to identify and control third-party code negatively affects website performance. In addition to potential data privacy violations, increased cookie volume leads to longer load times which correlates with shopping card abandonment and increased bounce rate.

TRAVEL

After months operating at a loss, businesses throughout the travel industry—including hotels and airlines—were eager to open back up towards the end of 2020. When lockdowns were lifted, domain drift spiked as third parties clamored to take advantage of restless travelers eager for a vacation. Based on analysis of 15 hotels and airlines, the travel benchmarks reveal:

AIRLINE:

- **59 Executing domains**
- **90% of executing code not controlled by airline**
- **7% doomain drift**
- **1% of domains are high-risk**
- **131 cookies (at least) drop during every visit**

HOTELS:

- **105 executing domains**
- **9% of domain drift**
- **1% of domains are high-risk**
- **183 cookies (at least) drop during every visit**

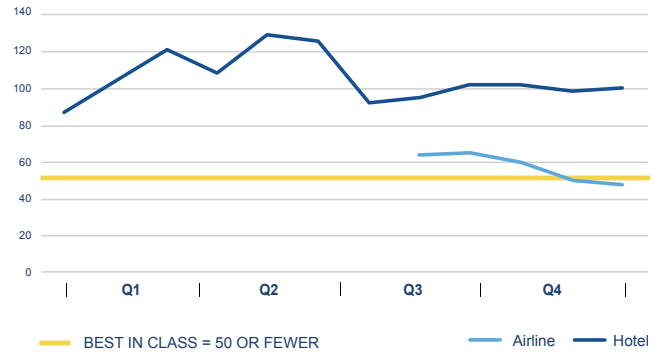
IMAGINE: You arrive at your hotel after booking a trip online. When you reach the counter, you realize that a group of silent onlookers is crowding around you; the clerk smiles and tells you not to worry—"They're with us". To check-in, you provide your credit card information and notice a few in the crowd copy it down. They take your name, phone number and email address, too: anything that could be useful.

REALITY: In November, the Prestige hotel booking platform experienced a data breach that exposed 10 million guest-related files dating back to 2013. Many included full credit card details and personally identifiable information (PII). Under the General Data Protection Regulation (GDPR), Prestige could face massive fines, and its ability to securely process credit-card payments does not meet Payment Card Industry Data Security Standards (PCI DSS).

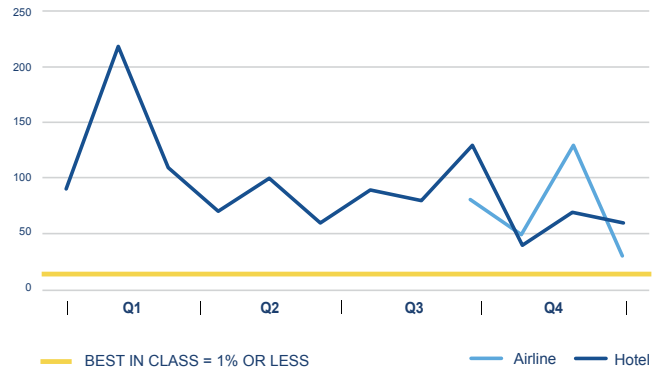
Travel Benchmarks

Throughout 2020, when a typical consumer accesses a travel website they experience:

Domains



Domain Drift



Cookies

With the travel industry showing signs of recovery, airlines and hotels launching campaigns driving consumers to their websites. To safeguard this new traffic, airlines and hotels need to control client-side code to avoid personal data theft and customer journey hijacks.

Mitigating Digital Risk Requires Client-side Insight

Digital third-party risk management demands a distinct approach

In 2021, businesses across every industry should be able to answer a simple question: who is watching your digital properties and influencing your customers? Once answered, they should strive to align their websites and digital applications with the following measurements:

INDUSTRY BENCHMARKS

- Best in Class for Domains: 50 or fewer; ideally, no more than you can actively remember.
- Best in Class for Domain Drift: no more than 1% month-over-month.
- Best in Class for Data Collection (cookies): 95% first party ownership.
    - 100% secure
    - 0% collection on CA residents who have opted out

Understanding your digital attack surface requires analysis of executing domains and their activities. Any domain—including those owned by authorized vendors—found to not be necessary for functionality or enhancing the customer experience should be removed and/or blocked. Pursue strategies to monitor digital properties in the long-term and remediate threats as soon as they surface. Tactics include:

- Scanning: continuous, client-side scanning captures the code from a true user experience
- Digital Attack Surface Map: document your core executing code and relevance to site functionality
- Lockdown reports: alert on new domains and cookies that appear outside your map
- Scorecard: generate thorough reports to inform executive decision-making regarding digital risks

Don't let your consumer-facing digital properties be a vulnerability to your business. You can take control of the vendors and third-party code appearing on your sites and apps, and mitigate your digital risk—for the sake of your customers and your bottom line.

REQUEST YOUR DIGITAL RISK ASSESSMENT TODAY: mediatrust.com

THE MEDIA TRUST

We know digital security.

Learn more: www.MediaTrust.com