CISOs:

This is the #1 Threat to Your Digital Properties

Over the last six years, malware attacks and other security issues related to third-party code have increased by 600%.

So how much website / application code required to render the user experience is not controlled by you?

More than you think.

THE MEDIA TRUST

We know digital security.

Executive Summary

- Security issues related to third-party code are the biggest blind spot and #1 security threat for companies that rely on digital revenue.
- Malware attacks and other security issues related to third-party code have increased by 600% in the last six years.
- The Media Trust detects a new third-party code malware attack every 30 seconds.
- Digital Shadow IT is third-party code that adds functionality or content to your website that was not created or directly operated by your in-house team.
- Examples of third-party code include ads, analytics, customer relationship management (CRM), data management platform, online chat, shopping carts, software plugins, video platforms, etc. Third-party code can become Trojan Horses if not regularly monitored. Further, third-party code can drop cookies on your site to collect data on your valuable customers without your knowledge.
- Scans of over 1 billion web pages over the last year by The Media Trust revealed that 65-95% of a typical consumer-facing website relies on third-party code.
- Third-party code executes dynamically on consumer devices and varies by geography, browser type, user profile, browser history, business rules, and device type. Because of this, CISOs who only scan code developed by their internal teams (e.g., AppSec or DevSecOps) miss the majority of today's attack vectors.

- Comprehensive, client-side scanning is the best method for protecting websites and customers from third-party malware attacks regardless of geography, user profile, device type, or operating system.

- Without comprehensive scanning, CISOs face these daunting questions:

  > *Do you know all the companies in your digital ecosystem?*
  >
  > *Do you have contracts with them? Are they following your security and data compliance policies?*
  >
  > *Do you known how many domains are called through third-party code, and how often new domains are called?*
  >
  > *Do you know what JavaScript is rendering on your users, and where it's coming from?*
  >
  > *Do you know what cookies are being dropped on your users and the data they're collecting?*
  >
  > *How do you know if you're in violation of privacy regulations that could cost millions in fines?*

- The Media Trust maintains the largest and most comprehensive scanning network in the world. Last year, The Media Trust scanned over 1 billion web pages across 10 million of the most heavily trafficked websites from more than 550 cities across more than 95 countries.

- The Media Trust offers a free digital risk scan so companies can discover what third-party code and third-party cookies are executing on customers around the world.

- CISOs who work with The Media Trust can better protect their company revenue, reputation and customer relationships.

Security for digital assets has changed. The attack surfaces for websites and mobile apps have multiplied exponentially.

In the early days of the Web and e-commerce, CISOs could secure the web application code developed by their internal teams. But now, the majority of a website's code relies on third parties. In fact, based on The Media Trust's scans of over 1 billion web pages over the last year, 65-95% of a typical consumer-facing website relies on third-party code—meaning code written by someone outside of the enterprise developer, website operations or technology teams.

Instead of managing a secure, fixed digital asset, CISOs find that third-party code exposes them to risks they can't detect, let alone manage, on their own.

The Media Trust detects a new third-party code malware attack every 30 seconds.

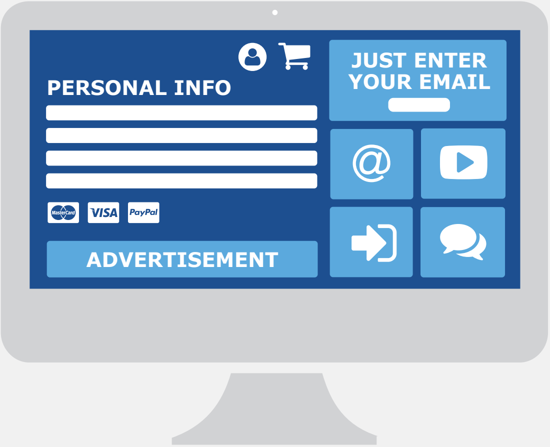
Ads, analytics, videos, software plugins, online chat, CRM management, and shopping cart technology that make calls to external domains can all become Trojan Horses if not regularly monitored. Further, third-party code can drop cookies on your site to collect data on your valuable customers without your knowledge. In fact, some e-commerce sites unknowingly use advertising technology owned by their competitors.

It's only a matter of time before third-party code on your site gets hijacked by bad actors to deliver malware. If any of your customers' data privacy is breached, your company will take a reputational hit. With web-based malware incidents doubling since 2017, it's clear the next frontier in Shadow IT is securing third-party code executing in the digital environment.

What CISOs need to know in order to protect themselves and their digital properties from malicious third-party code:

Securing Third-Party Code: The Next Frontier in Shadow IT

- Third-party code is code that adds functionality or content to your website that was not created or directly operated by your in-house team.
- Analytics, templates, ads, videos, online chat, plugins, CRM management, and shopping cart tech are all examples of third-party code.



Third-party code comprises anywhere from **50-95% executing code** to render the user experience.

B2B sites **50-70%**

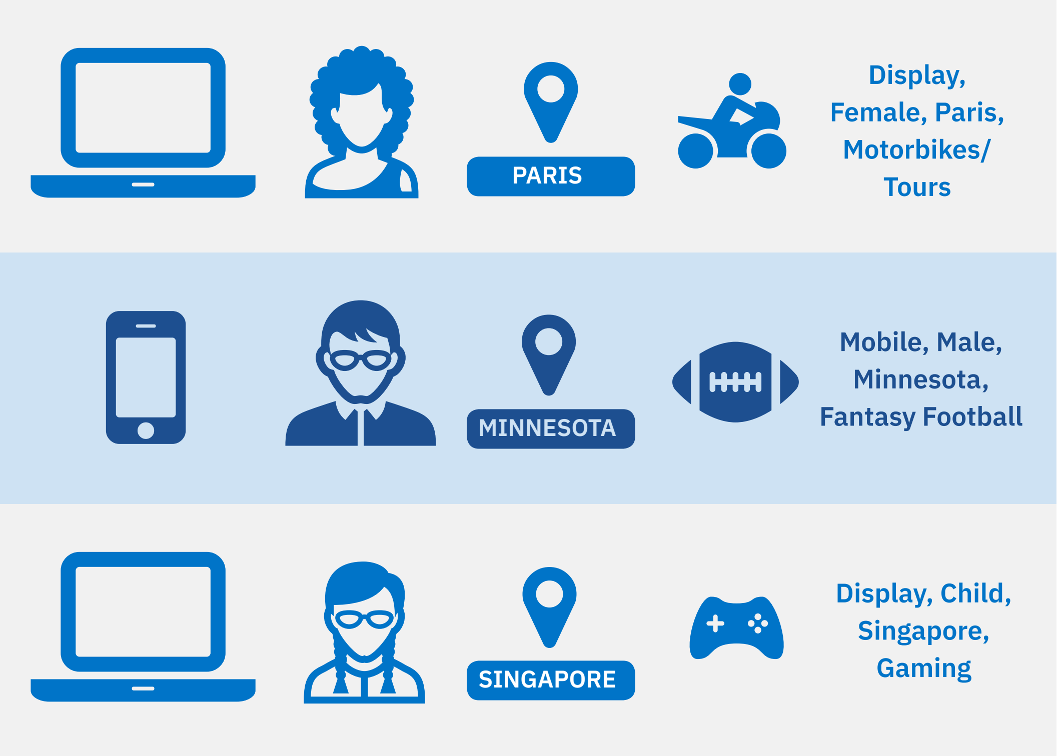
Retail sites **65-85%**

Media & ad-supported **75-95%**

Scans From Behind the Firewall Aren't Enough

In the early days of the web, application security pros could scan source code and have a good idea of what is executing on digital assets. This is no longer true, since modern website and mobile app code is incredibly dynamic. The code that executes on a device varies by geography, browser type, user profile, browser history and business rules. A 30-year-old French woman who lives in Paris and is interested in motorbike tours will have a very different experience of the same website than a 20-year-old man living in Minnesota who plays fantasy football.

Why? The web is built to sell an idea, a service, or a good. To do that, a tailored customer experience is needed to present the right message to the right person at the right time. Over the past 20 years, the digital ecosystem exploded with the ability to provide a custom experience.


PARIS
Display, Female, Paris, Motorbikes/ Tours
MINNESOTA
Mobile, Male, Minnesota, Fantasy Football
SINGAPORE
Display, Child, Singapore, Gaming

Today, any website or mobile app with user profile generated content/services (i.e., weather, news), dynamically targeted ads (i.e., sales), or customer-specific identifiers (i.e., login) has code that executes on each customer device differently. Further, when you factor in geography, browser and device type, the code execution varies dramatically.

Each new instance of dynamically-generated code for a single visitor's session is a new attack surface. In the eyes of the consumer, if a poor user experience occurs on one of your digital properties—even if it was caused by an unknown third-party partner—your brand is perceived as responsible. Recent large-scale attacks are frequently referred to by the brand name impacted, not the third-party code that was compromised. Consumers, especially the ones you want to be your customer, rarely differentiate. The result? Slower sites and hijacked browsing experiences can cost millions in lost revenue.

Online shoppers expect an e-commerce site to load in three seconds or less.

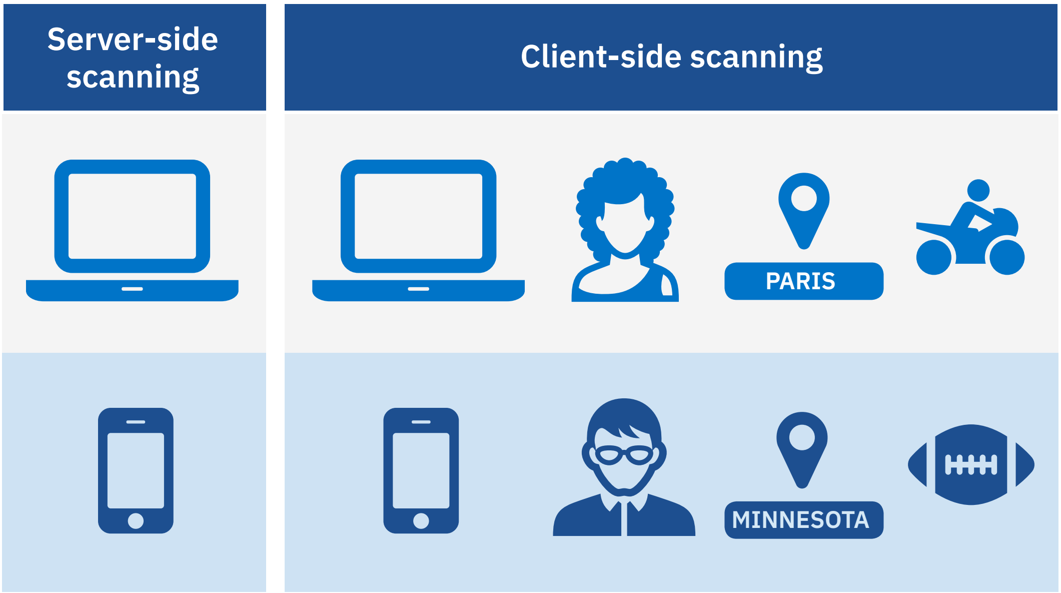
In the eyes of the law, both brands and third-party vendors that collect personal data from consumers are held responsible for data breaches. Under Europe's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), and Texas' Privacy Protection Act (TPPA), even if a data breach occurred due to a third-party vendor—either via poorly written or hijacked code—the owner of the digital asset where that code appeared can be held liable and fined. In the case of GDPR, the fine can be substantial—up to 4% of annual worldwide revenue for the previous year.

Third-party code isn't necessarily bad. In fact, it provides efficiency in developing today's consumer-oriented websites. Third-party code generally enhances your website's functionality, makes site creation easier, and enables new or streamlined revenue possibilities. But any unmonitored code can become a problem. It’s like locking the front door to your house while leaving the garage and back windows wide-open.

When the stakes are high to revenue and your reputation, comprehensive, consumer-side scanning is your best tool to protect your digital properties. Just as there is no substitute for security guards and security cameras for physical properties, there is no substitute for increased vigilance on digital properties.

Casting a Light on Your Shadow IT

Comprehensive scanning is about client-side emulation. Scanning is comprehensive when you capture a representative sample of all the various ways that your website’s code executes on customer devices. Client-side emulation means you capture variations in how your website’s code downloads and/or performs based on country, device type, browser type, user profiles, browser history, cookie history, and business logic.



The main purpose of comprehensive scanning is to:

- **Detect what third-party code executes on your customers' devices regardless of version, OS, or geography.**
- **Analyze for suspicious or unauthorized code.**
- **Identify data tracking activity collecting data on your valuable customers.**
- **Gain insights into how third-party code impacts performance.**

The greater the number of scans you perform and the more customer variables you emulate, the more comprehensive your scan becomes. Frequency is also an important factor in comprehensive scanning because website code, particularly third-party code, changes constantly.

While it's possible to scan on your own, the cost of setting up infrastructure and technology is tremendous. You would have to set up actual scanning resources inside each country so that your scans truly reflect what code executes for users in that specific country. You would also have to view your code from many different devices, browsers, and with many different user profiles. And you would have to keep all these scanning IP addresses and users from being "made" or detected by cyber criminals—who could keep their malicious intentions secret.

The Media Trust maintains the largest and most comprehensive scanning network in the world. Last year, The Media Trust scanned over 1 billion web pages across 10 million of the most heavily trafficked websites from more than 550 cities across more than 95 countries. To mimic actual site users, our clients historically provided us with the profiles they use to target customers with content. In turn, we've used this information to create tens of thousands of real-world customer profile emulations. As new devices, geographic requirements or other campaign parameters emerge, we add to these emulations. This grows our emulation and scanning capability by at least 20% every year.

Due to The Media Trust's extensive client-side scanning for 15 years, many of our customer profiles and email addresses are so developed that they are indecipherable from real customers with rich Internet use histories. The Media Trust detects, on average, a malware attack every 30 seconds or less and takes action to protect over 600 clients and more than 2,000 vendors in our digital network.

In 2018, The Media Trust:

SCANNED

- over 1 billion web pages
- over 10 million websites
- from 95+ countries and 550+ cities

EMULATED tens of thousands of customer profiles

DETECTED one malware attack every 30 seconds or less

PROTECTED over 600 enterprise clients, online publishers and their digital partners

Client-side scanning yields interesting results. When The Media Trust scans, we first look to identify all third-party domains that are active on your site and who these third parties are. Ideally, these third-party lookups efficiently add functionality or content to your site, and you have contracts that define what these third-party vendors can do on your site. Unfortunately, this is rarely the case.

Clients are often shocked to find the number of third-party vendors that are on their site, dropping cookies and collecting valuable information about their customers. Even worse, competitors are found executing, with some placing cookies on your site and collecting data.

The first time a comprehensive scan runs is often a jaw-dropping experience. CISOs are surprised to learn that the amount of third-party code is two to three times more than expected. A CISO who thinks only a handful of cookies collect data on their customers may discover that a third party may have brought in a fourth, fifth, and sixth vendor who collects customer data that could be resold to the highest bidder. This of course raises red flags on compliance issues.

For a CISO, comprehensive scanning reveals a more complete landscape of all the third-party vendors and third-party cookies executing code on their customers. Comprehensive scanning reveals the attack surfaces that need to be investigated to secure your digital properties.

GET YOUR FREE DIGITAL RISK SCAN

Discover What Third-Party Code Executes on Your Customers

# of Third-Party Domains	# of Active Third-Party Cookies	Risk Exposure

GET FREE SCAN NOW

Five Questions to Ask Once You’ve Reviewed Your Health Check

1 Do you know all the vendors in your digital ecosystem?

Once you review your health check with our team, you’ll see that your site makes numerous calls to external domains. These external domain calls typically pull third-party code into your customers’ digital experience, and add more time to every page load.

The list of third-party vendors may be extensive. Prioritize identifying the ones that drop cookies to collect information about your digital customers and expose your business to regulatory violations. Review the cookie summary report to easily identify these domains.

As you review the summary of active domains, ask yourself: “Are they a contracted vendor? Did my company authorize them to be on our site?”

2 How did they get there? Who brought them to your site?

If a digital vendor is not someone you have a contract with or authorized to execute within your digital ecosystem, you need to determine who brought them to your site. Often, a digital vendor is an essential part of another vendor’s offering, itself a third party to your contracted vendor.

But sometimes domains and even competitors sneak inside your digital ecosystem using another vendor as a Trojan Horse. Because The Media Trust has conducted client-side scanning of the consumer web for more than 15 years, we know how to identify and separate the good, legitimate activity and actors from the bad, unauthorized activity and actors.

3 What are they doing? What is the impact on your customers?

Now that you understand what domains are active on your site, next review the functionality each digital vendor actually delivers. In many instances, the third party executes more than one domain: the intended functionality and also something extra like a cookie drop or compromised code. As you delve into specific third-party domain activity, focus on the impact these third-party domains have on your customer. Each domain and url should enhance your customers' experience or deliver valuable content. Check to see if third-party domains have dropped cookies that aren't necessary to deliver their core functionality. Check to see if third-party domains increase site latency and damage your users' experiences with code and files that are too heavy.

4 What is their impact on your business?

When you review your health check, divide the impact on your business into two simple areas: reputational risk and site speed.

Ask yourself: "Are there any domains on my site that shouldn't be there? Is there any cookie activity or JavaScript activity that shouldn't be happening?"

The presence of any third-party vendor collecting cookies presents a risk of data leakage that could impact your company's reputation. Data leaks on your valuable customers can also be used to steal your customers. As a CISO, it's up to you to determine with other executive leadership which business risks are manageable and which risks are unnecessary.

You should also investigate if excessive file sizes or too frequent network calls are slowing your site. Reputational risks and site latency impact revenue, so any deficiencies in both of these areas should be addressed.

5 What action should you take?

It's best to have a contractual relationship with the third-party vendors that appear on your site and to be sure that each digital vendor complies with your policies or "rules of the road."

If a third-party vendor is not adding functionality or content that you want to your site, it's best to remove them—either by removing any embedded code, cookies, or JavaScripts or by taking steps to block them.

If a third-party vendor adds functionality or content that you want but is not complying with your rules of the road—for example, unauthorized dropping of cookies or delivering heavy code that's slowing your site—it's best to proactively communicate your service expectations or digital policy. Communication is better than blocking because it allows you to resolve issues that may be harmful to your site and your customers while preserving valuable relationships. Communication protects revenue, whereas blocking can sever relationships.

Contact Digital Vendors to Fix Issues

Once you identify the digital vendors on your site, you should build a contact list for each vendor. It's particularly important to include the contact details for the technical people you need to work with to resolve any issues that appear on your site.

When you have a contract with a digital vendor, it's relatively easy to get in touch with a technical person at that digital vendor to immediately resolve issues when they arise, and they will. But when you don't have a contract, it's much harder.

The Media Trust maintains an extensive **digital vendor network** with more than 2,000 listings for the most commonly-used digital vendors. Each vendor profile contains not only technical contact information for a variety of vendors—from demand-side platforms and data management platforms to ad exchanges and supply-side platforms—but also their industry memberships, data trackers and more. These represent the bulk of third-party domains

We know all the third-party vendors on your site.

Our system makes it easy to:

GAIN a 360 degree view of your digital ecosystem

DETECT authorized cookie drops and other user data collection activity

SHARE your rules with third-party vendors

VERIFY they agree to follow them

BUILD an audit trail of vendor activity likely to appear on your site. This **digital vendor network** saves you significant time by helping you to easily reach out to third-party digital vendors, communicate your digital policies and evaluate for compliance.

Through The Media Trust's digital vendor network, you can easily share your rules of the road, have your vendor verify that they have seen the rules for compliance purposes, and communicate to repair specific issues.

In support of our clients, The Media Trust audits our clients' digital environments to verify we know their digital vendors and then works to fill in the gaps. As a result, The Media Trust maintains the largest technical contact database for digital vendors in the digital security space.

Through The Media Trust's **digital vendor network,** you can easily share your rules of the road, have your vendor verify that they have seen the rules for compliance purposes, and communicate to repair specific issues.

This network has evolved into a digital neighborhood watch, which works to shut down bad actors and clean up the digital ecosystem.

Shut Down Bad Actors

When The Media Trust identifies malware and bad actors intruding on your site, you don't want to just block them. You want to shut them down.

It's important not to let bad actors recycle in the digital ecosystem for one main reason: you don't want bad actors to get stronger and profit off their malware on other sites while they figure out a way to get around your block.

Instead, you want to identify the source where the bad actor entered the digital ecosystem (DSP, SSP, or Ad Network, for example) and alert that gateway to lock them out.

You should also notify federal and global law enforcement so they can investigate and prosecute cybercriminals. Don't worry, we have the connections to do it for you.

The Media Trust detects a malware attack every 30 seconds or less. Our 15-year history scanning the digital ecosystem means we know when bad code and bad domains appear. The Media Trust immediately alerts clients when there is an issue on their site 24/7, 365 days a year—not only during the week or during business hours.

For advertising-supported websites, The Media Trust takes an additional step to directly block the malware from executing. The Media Trust also does further research to identify where the attack came from.

Malware Takedown in Action

Malware attacks are growing in sophistication. Here's just one example of why comprehensive scanning is your best defense.

By coding a polymorphic feature in the AfterShock-3PC attack—frequent code-switching and jumps from more than 30 domains—this malware

We know how to stop sophisticated malware attacks.

- Continuous, global scanning through emulated user profiles
- Automated and live behavioral analysis to find obfuscated malware
- Smart blockers that use machine learning to stop complex attacks
- Collaboration with 2,000 global vendors in the digital ecosystem
- Trusted by Federal authorities to provide extensive information that can help shut down bad actors

outsmarted signature-based defenses. 200+ premium ad-supported websites experienced over 50,000 related incidents that resulted in hundreds of thousands of users having their devices ransomed and their personal information captured by keystroke loggers. Even worse, this attack bypassed a malware blocking solution used by these publishers.

Through continuous client-side scanning, The Media Trust detected and quickly blocked the code from infecting client sites. Our team then worked with the two buy-side platforms (where the bad actors entered the digital ecosystem) to identify the bad actor and shut down the attack at the source.

The Media Trust also notified Federal authorities of the attack and provided extensive information to assist their investigation.

How Often You Need To Scan

The user experience on your digital properties constantly changes, particularly as the browser histories of your customers change. Further, the hijacking of third-party code or Trojan Horse malware attacks can occur at any time.

Scan at least
50 - 100
times per day

Each business case is different, but in general, for large consumer-oriented sites with hundreds of thousands of visitors per hour, The Media Trust recommends that businesses scan their digital properties across different geographies and different user profiles at least 50-100 times a day at random intervals.

There is further benefit to being part of a large scanning network. With everyone in your network on the lookout, bad actors will often be spotted by someone before they reach many sites in the network.

Contact The Media Trust

For 15 years, The Media Trust has maintained the largest scanning network dedicated to detecting malware attacks. We know digital security.

The Media Trust leverages a physical presence in 65 countries and 500 cities to detect and remediate security, privacy, ad quality and performance violations executing on websites and mobile apps. More than 600 media publishers, ad tech providers, agencies, retailers and enterprises—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to protect their digital environment, their revenue and, most importantly, their brand.

Contact The Media Trust if you have any questions about comprehensive scanning.

703.893.0325 | info@mediatrust.com

GET YOUR FREE DIGITAL RISK SCAN

Discover What Third-Party Code Executes on Your Customers

# of Third-Party Domains

# of Active Third-Party Cookies

Risk Exposure

GET FREE SCAN NOW

THE MEDIA TRUST
We know digital security.

THE MEDIA TRUST
We know digital security.