Web Monitoring Software for Security: A Buyer's Guide

Millions of new social media posts, deep and dark web posts, news articles, and blogs are published every day. Within this sea of content are data critical for a variety of public and private sector functions, from marketing to cybersecurity.

Web monitoring has become popular for gathering insights like marketing campaign analytics—but it's also now essential for security risk detection and response across almost every sector. This includes locating data leaks, disinformation, damaging pre-viral content, and conversations revealing physical security threats.

Without easy access to this information, organizations are unequipped to find and respond to threats quickly enough to protect their people, assets, and data from harm. This is why web monitoring software is now crucial for progressive security strategies—it enables users to sift through the noise and find relevant data fast.

Organizations can then make more timely and informed decisions in response to risk, and ultimately prevent or minimize associated financial costs, physical harm, and reputation damage.

Once organizations understand the value of web monitoring software, it becomes a question of which software to use. This buyer's guide walks you through what web monitoring software is, why you may need it, and how to choose a solution that's right for you.

WHAT IS WEB MONITORING SOFTWARE?

Web monitoring software enables users to quickly and easily search for public information from online sources. The overarching goal for security teams is to find risk indicators and make fast, informed responses to potential security issues. Web monitoring software can also be called open-source intelligence (OSINT) software, social media monitoring (SMM) software, or threat intelligence software, depending on the end user's focus area.

Given the vast amount of public information online, web monitoring software helps users:

- Find content that isn't easily accessible through free search engines like Google.
- Aggregate content across multiple online sources in one place.
- Find relevant data more efficiently than searching manually within websites or applications.
- Extract analytics and other metadata from results.

Web monitoring software varies in data coverage but typically focuses on unindexed content that is hard to find using standard search engines. Some common sources include publicly available news, social media, deep web, and dark web content.

Web monitoring software is commonly associated with intelligence analysts, cybersecurity professionals, and physical security teams—but it's also used by non-technical departments like marketing, PR, and business continuity.

What types of risks are discoverable online?

- Cybersecurity threats like phishing, malware, ransomware, and data breaches
- Brand-targeted threats like impersonation, counterfeiting, negative sentiment, and damaging viral content
- Physical security threats, like a bomb threat alert, or leaked data exposing private location information like building layouts
- National security threats like disinformation and terrorist activity
- Criminal activities like human and drug trafficking

DO YOU NEED WEB MONITORING SOFTWARE?

If you're new to web monitoring software, you might wonder why free tools like Google Alerts or manual web searches aren't enough. There are several reasons why this approach is inadequate for most public and private sector security organizations:

- Search engines like Google only cover indexed content—about 10% of available web content. Relying on free search engines overlooks other data sources relevant for security and brand protection, like the deep and dark web. The dark web, in particular, is also extremely clunky and dangerous to navigate without web monitoring software.
- Many organizations require discrete online data collection so an investigator's tracks are undetectable to potential adversaries. This is very challenging without a web monitoring tool designed to manage attribution.
- Searching manually is time-consuming and unlikely to return relevant data fast enough for timely responses to security and brand risks.
- Filtering functionality on typical search engines is not robust enough to reduce noise and streamline relevant data. Beyond searching by keyword, image, date published, etc., web monitoring software incorporates advanced features like geo-searching and natural language processing.

Web monitoring software ensures that data collection is comprehensive, considering a wide range of relevant sources you might not know about. It also helps you find and respond to risk as fast as possible so you can minimize or avoid potential damage to your brand, people, assets, and data.

WHICH WEB MONITORING SOFTWARE IS BEST FOR YOU?

The online risk landscape is evolving rapidly. To keep up, the demand for web monitoring software is increasing across a variety of sectors. With so many web monitoring software vendors on the market, how do you know which one addresses your requirements?

The truth is, mature intelligence, security, and brand protection functions often need multiple web monitoring tools for a holistic solution. But asking yourself the following questions can help streamline the procurement process:

☐ **What goal are you trying to achieve with web monitoring software?**
Using online data to support marketing and PR campaigns will require very different software than that for cybersecurity teams. Getting specific about your goals will also help you determine which data sources and features to look for.

☐ **What is the vendor's stance on data privacy and compliance?**
Web monitoring vendors vary in their stance on data privacy and compliance. Vendors without an ethical and compliant approach to data collection have caused major public scandals and (often permanent) service disruptions. Choose a compliance-focused vendor to respect the public's privacy rights, ensure a reliable service, and protect your own customer data.

❏ **How easy is the software to use?**
Web monitoring software should speed your personnel up, not slow them down. Some web monitoring tools, especially those catering to cybersecurity users, are often complex and could frustrate rather than support less technical teams.

❏ **What's the vendor's customer support and development approach?**
Online risks evolve quickly, and web monitoring services must adapt accordingly. Reputable customer support improves your team's usage, and feedback integration ensures that the software adapts to end-user requirements over time.

DELIVERY TYPES

You should also consider which software delivery type is best suited for your organization's goals and budget. We've separated web monitoring software vendors into three categories, though some combine at least two in their offerings:

Pre-Built Platform

In this model, the vendor provides web monitoring software that is used directly by your organization's personnel. It's the most common and cost-effective option for online data discovery. This type of software delivery is ideal for organizations that:

- Have the staffing and resources required to investigate online sources internally.
- Want direct tool access rather than using a third-party service provider that is less familiar with the organization's specific needs.
- Want to locate and respond to risks as soon as possible.

API

Some organizations already have commercial or proprietary software for online data gathering and analysis. In this case, they may not require a pre-built SaaS tool—they just need new data inputs. This is why some web monitoring software vendors offer an API, which funnels data from hard-to-access sources directly into the customer's existing software.

Managed Service

Managed web monitoring services do all the customer's legwork, using web monitoring software and domain experts to find, analyze, triage, and in some cases, respond to online risks. This model tends to be more expensive, takes longer to fine-tune to a customer's requirements, and, being managed by a third party, can result in delayed risk response. However, it can be the best option for organizations without the internal resources or expertise to manage web monitoring.

SOFTWARE CATEGORIES: WHAT'S YOUR USE CASE?

We've talked about why web monitoring software is valuable for your organization and how software subscriptions are delivered. Now we'll cover which software and features are best suited for five of the most common web monitoring niches:

1.0 Cybersecurity Software

2.0 Security & Threat Intelligence Software

3.0 Crisis Alerting Software

4.0 Marketing & PR Software

As you read through each category, consider which use case aligns most with your requirements. Each category includes descriptions for:

Data Sources	Depth of Data	Data Fidelity	Common Features
Describes the online sources most common for this web monitoring software category.	Describes the data typically accessible to users using this type of web monitoring software.	Describes the completeness of data from the original source for this web monitoring software category.	Describes software features common to this web monitoring software category.

1.0 Cybersecurity Software

As it might be obvious from the title, this software is used to find, triage, and respond to cybersecurity risks—like data leaks, malware, and phishing—from online sources. Cybersecurity software may also incorporate proprietary feeds from a customer's own network to detect risks.

This software is ideal for customers who need a tool primarily to support their cybersecurity or digital risk protection (DRP) strategy. It's also suited to customers with more technical or advanced teams, as it often has a more complex interface than other web monitoring software types.

Some example software vendors in this category include Recorded Future, Digital Shadows, and Sixgill.

Data Sources	Depth of Data	Data Fidelity	Common Features
• Some social media • Deep web (e.g. paste sites) • Dark web • Internal feeds (e.g. network traffic)	Includes text from the original post and may parse out other relevant metadata, like URLs, authors, and date published.	Raw data—users have direct access to content in its original form without having to navigate to the original source. Some vendors (e.g. Recorded Future) may alternatively provide finished intelligence reports.	• 24/7 alerts • Threat scoring/AI • Data analytics • Integrations

2.0 Security & Threat Intelligence Software

Security/threat intelligence software addresses a variety of security use cases—including physical security, digital risk protection, and their convergence. This software provides access to public online chatter rather than technical cyber feeds, making it useful for applications like early breach detection, but not endpoint or network security. This software tends to be more user-friendly than commercial cybersecurity tools, and provides the data coverage and features to address a broad scope of security threats in the public and private sectors.

This software is valuable for security and intelligence teams who require raw data access spanning a range of surface, deep, and dark web sources in one platform. It's also ideal for customers who aren't hyper-focused on one use case but need a solution that's optimized for a variety of functions—from breach detection to crisis management and marketing support.

The Echosec Systems Platform is one example of this software type. The Platform supports several security functions, including crisis detection and response, some cybersecurity, brand protection, and public sector use cases like counter-terrorism.

Data Sources	Depth of Data	Data Fidelity	Common Features
• Mainstream social media • Fringe social media/ alt-tech • News and blogs • Deep web • Dark web • Breaches data	Includes text and image-based content from the original post, and parses out metadata (e.g. URLs, authors, personally identifiable information, date published, etc.).	Raw data: users have direct access to content in its original form without having to navigate to the original source.	• 24/7 alerts • Geo data/search • Threat scoring/AI • Translation • Data analytics • Broad data coverage

3.0 Crisis Alerting Software

Crisis alerting software is designed to help users identify security threats or other events of interest quickly. This type of software is primarily used to detect physical crises, like natural disasters or bomb threats. As such, crisis alerting software tends to focus on widely-used sources, like mainstream social media and news, where on-the-ground alerts are likely to surface the earliest.

This software type is ideal for users who prioritize timeliness for broad event detection, such as law enforcement or media outlets. They need software to interpret online data and alert them as soon as an event occurs. Interaction with raw data to inform a response or follow-up investigation isn't a primary focus for crisis alerting software users.

Some examples of crisis alerting software include Dataminr and NC4.

Data Sources	Depth of Data	Data Fidelity	Common Features
• News • Blogs • Mainstream social media	Alerts include the original post from which the alert was extracted, and may include other metadata like sentiment analysis or the time and source of the alert.	While raw data may be accessible on some platforms, they are more alert-focused.	• 24/7 alerts • Sentiment analysis • Geo data/search • Translation • Analytics

4.0 Marketing & PR Software

Marketing and PR software gathers online data to detect brand-targeted risks and inform marketing and PR campaigns. These platforms provide end-users with analytics and visualizations based on data gathered from news, blogs, and social media. This software type is designed to help users understand public sentiment towards their brand, but it can also identify risks like brand impersonation, PR risks, or product counterfeiting.

Customers who need web monitoring software specifically to support marketing and PR teams will benefit from this type of tool. Marketing and PR software is also ideal for users who don't have time to assess sentiment or risk from raw data—they just need analytics and alerts for urgent risks like damaging viral content.

Some examples of marketing/PR software include Brandwatch, Talkwalker, and Meltwater.

Data Sources	Depth of Data	Data Fidelity	Common Features
• News • Blogs • Mainstream social media	Includes data analytics, trends, and visualizations based on the user's marketing/PR concerns.	Processed data—users only have access to analytics and sentiment, not actual posts or raw data.	• 24/7 alerts • Sentiment analysis • Analytics and marketing metrics • Translation

Buyer's Checklist

Vendor Requirements

Does the vendor:

- ❑ Understand and address your requirements?
- ❑ Address regional privacy legislation?
- ❑ Have a transparent acceptable use policy?
- ❑ Comply with industry privacy requirements like SOC 2?
- ❑ Offer a delivery method that works for your organization (user platform, API, and/or managed services?)
- ❑ Provide adequate training and customer support?
- ❑ Have an agile development approach to incorporate user feedback?

Software Requirements

Does the software:

- ❑ Include data sources necessary for your use case(s)?
- ❑ Have a UI that is easy enough for your personnel to use?
- ❑ Enable users to translate search queries and results?
- ❑ Leverage AI to expedite data collection and analysis?
- ❑ Provide data analytics relevant to your goals?
- ❑ Deliver results in real-time or near-real-time?
- ❑ Provide 24/7 user alerts?
- ❑ Provide adequate historical data access if required?
- ❑ Give you direct access to raw data if required?
- ❑ Allow users to search by geolocation if required?
- ❑ Provide sentiment analysis if required?
- ❑ Provide influencer data if required?
- ❑ Allow users to export data if required?
- ❑ Support report generation if required?

**Still unsure which web monitoring software to pursue?
Book a consultation to define your goals and explore a solution.**

BOOK A DEMO

Learn more about our solutions: 1-844-ECHOSEC | sales@echosec.net | **echosec.net**