everbridge signal
powered by NC4

THE FUTURE OF THREAT INTELLIGENCE

In situations where seconds make all the difference, you need actionable real-time data. Be the first to know, not the last.

Product Solutions

Open Source Intelligence (OSINT) tools for advanced security solutions and increased protection.

The very same technology that has helped provide companies and organizations with incredible growth and new opportunities have simultaneously opened up more surfaces for cyber and physical attacks.

When it comes to navigating the evolving cyber intelligence landscape businesses more than ever need accurate real-time data to combat increasingly complex attacks like ransomware or other malware designed to steal intellectual or personal data and property.

In regards to mitigating physical risks, it's often the case that threats emerge in forums or social media first. By monitoring these platforms using an OSINT tool can spot threats before they develop into tangible risk.

"43% of businesses were a victim of a cyber security breach in 2018."

The deep, dark, and surface web hold a myriad of potentially vital information. However, monitoring the web and finding that information when it surfaces is a huge undertaking for any security team.

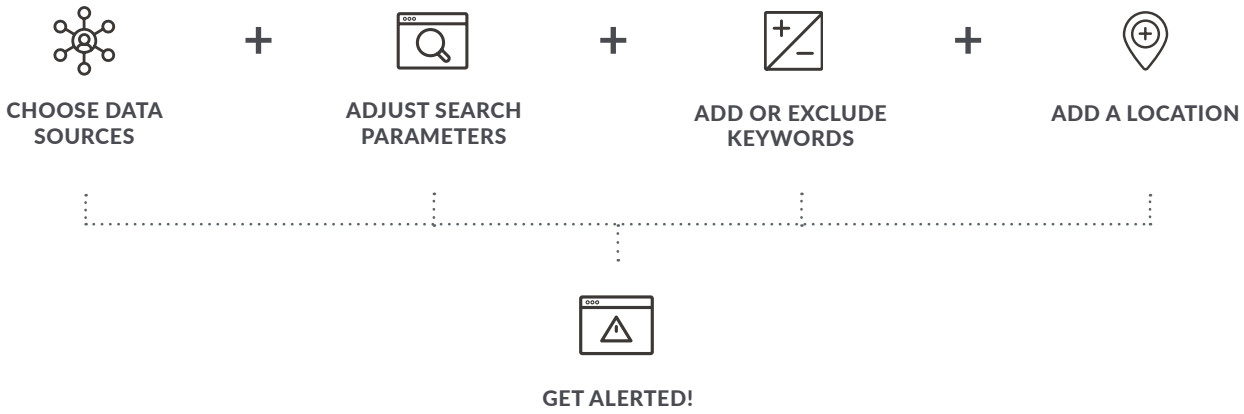
No company can protect themselves from what they don't know.

*Source: Symantec Internet Security Threat Report

Advanced Filters

With Boolean Logic

Create custom filters and apply Boolean logic to create refined search parameters and quickly and efficiently locate hyper-relevant online information from any one of our connected data sources.



With Signal you can get real-time data on potential physical threats as well as emerging cyber-security threats to help protect both your people and assets.

Actionable Data Insights

The first step to putting together an effective incident response plan is gathering, filtering and analysing as much data as possible.

With Signal, as potential threats are spotted you will be alerted in real-time so that you can take action immediately.

Additionally, our sentiment analysis tool Spotlight allows users to further reduce the amount of noise and focus on the threats. Sentiment analys is, in short, analysing the language in online posts and comments to determine the underlying emotion behind what has or is being posted by an individual or group.

More than 77% of organizations do not have a Cyber Security Incident Response plan. An estimated 54% of companies say they have experienced one or more attacks in the last 12 months.*

*Source: Information Management

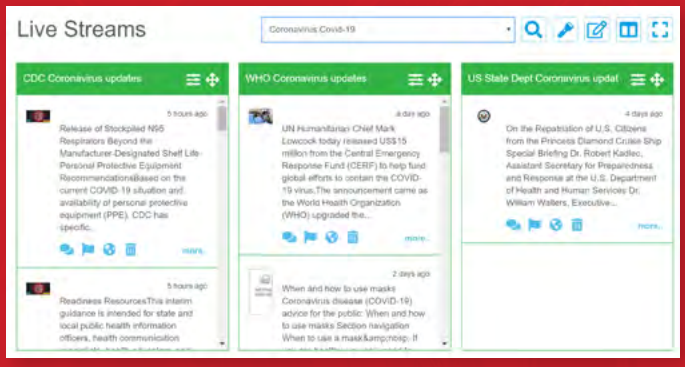
3 Key Ways People are Already Using Signal

Cyber Security

Cyber security encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems from theft and damage attempted by criminals and adversaries.

Hackers are relentless in their attempts to benefit from potential company breaches. Signal alerts our customers to a myriad of potential breaches such as:

- Mentions of an organization as a hacking target are found
- Customer data is detected for sale online highlighting a previously undetected data breach.
- Confidential organisation information is exposed online.
- Attempts to solicit employees in a hacking attack are spotted.



3 Key Ways People are Already Using Signal

Fraud Prevention

Fraud can do more than just financial damage to an organisation – the damage can be reputational too. This risk can come from both external and internal factors.

- Counterfeit goods are found for sale online.
- Mentions of an employee are found as a potential target of fraudulent activity.
- A medical professional has their identity stolen. Their impersonator is found online.
- Phishing and online scams are frequent and effective tactics to steal personal information.

"In 2018 hackers stole half a billion personal records.*"

Physical Security

By paying attention to social media and online data, your organisation can spot potential threats and take action before they become a real problem.

- Threats against facilities or staff often appear online first.
- Threats against executives.
- Natural disasters can impact supplies, logistics and the travel safety of staff.

*Source: Cybersecurity Ventures

Product Solutions

everbridge signal
powered by NC4

An all-in-one OSINT tool. Monitor the Surface, deep, and dark web and stay one step ahead of potential threats.

Full Open Source Intelligence including:

- Deep and Dark Web
- Pro-active alerting
- Emotional analysis
- Multi-language and Translation
- API integration capabilities
- Unlimited People

FEATURES	PLATINUM	GOLD	SILVER
Single Sign-on	✓	----------	----------
Concurrent users	✓	----------	----------
Auto translate streams	✓	----------	----------
Deep web sources	✓	----------	----------
Pastebin	✓	----------	----------
Data Breach Detection	✓	----------	----------
Users	Unlimited	10	5
Active searches	300	100	50
Text alerting	✓	✓	----------
Dark Web	✓	✓	----------
Emotional Analysis	✓	✓	----------
Social media	✓	✓	✓
Open web	✓	✓	✓
Flag items	✓	✓	✓
Email alerting	✓	✓	✓

Analyst Services

The optional Sapphire subscription bolt on provides dedicated specialist analyst capability to manage your Signal account on your behalf.

This includes additional set-up as part of your Signal subscription onboarding, followed by creation and management of your searches including personalised notifications, and detailed reporting.

The analyst leverages your Signal subscription and their expertise to actively monitor for open source intelligence threats relevant to your organization, locations and industry, helping you stay abreast of critical events and emerging threats.

If you want to know how Signal can help your security team contact us

Info@everbridgesignal.com