




# Threat Compass

Look Beyond Your Perimeter  
Manage Your Digital Risk





Today's threat landscape is becoming more and more volatile. Malicious actors use ever-more sophisticated techniques to attack organizations. **Any organization operating online holds data valuable to cybercriminals**, from financial transaction records to customer PII, confidential company assets to industrial IP. A hit on any of these can lead to catastrophic business impact, reputational damage and compliance penalties.

Your enterprise is at risk, and static or reactive cyberdefense is no longer enough. Outpost24 takes a proactive approach to cyberdefense, delivering targeted, actionable cyberthreat intelligence to mitigate cyber-risk. **Targeted threat intelligence saves time and maximizes security resource while accelerating threat detection, incident response performance and investigation.**

Our modular-based cyber threat intelligence solution Threat Compass uses sophisticated algorithms to deliver actionable, automated cyberthreat intelligence from open, closed and private sources, including malware botnets. This makes it easier to identify and manage real threats targeting your organization – **for faster decision-making and accelerated performance.**

Threat Compass covers the broadest range of threats on the market, and a pay-as-you-need modular architecture means you choose only the intelligence most relevant to your business.

Each individual targeted intelligence module is backed up by our world-class in-house analyst team. Enrich and contextualize threats so you can detect attacks, defend your assets and understand your adversaries' plans before they strike. **The pay-as-you-need architecture means our intelligence is streamlined, cost-effective and scalable.**

Fully automated delivery enables us to minimize analyst time and cost, with information that provides value to all levels: analysts want to know how a breach happened, while the C-suite wants to know it won't happen again. Threat Compass provides for both.

Integration is frictionless, with full API and flexible plugins so Threat Compass' targeted intelligence is immediately available to your security systems and teams. **The cloud platform's easy setup means you gain and maintain valuable situational awareness instantly.**



Delivering value in minutes, rather than months, Threat Compass has extremely low operational costs and needs very few people to manage. Better still, you don't need an expert to understand the intelligence delivered. Threat Compass hunts threats outside your corporate network, detecting and monitoring malicious activity, incidents and actors before they can cause harm within your infrastructure.

**Threat Compass automatically collects, analyzes, correlates and delivers enriched threat data across a variety of categories that could impact your business.** From identifying botnets and command & control servers to targeted malware variants; from tracking stolen credit cards and compromised credentials to finding rogue mobile apps, hacktivist activities and phishing campaigns targeting your organization



## Guiding you through the threat landscape

- Who is targeting your organization, and from where?
- Do you know what your presence is on the dark web?
- How has your corporate network been compromised?
- Who is impersonating your brand or VIPs?
- Has sensitive information been leaked?
- Have credentials been compromised, are they being used to commit fraud?
- Do you know what your compliance liabilities are if you're breached?

## Comprehensive, Modular Cyberdefense

Each Threat Compass module can be acquired and used individually. You only need to buy modules delivering threat intelligence most relevant to your business.

We offer a customizable module, enabling you to pick the specific sources you'd like to be monitored.



## Threat Context

Threat Context delivers a continuous stream of up-to-the-minute, user-friendly insights into the threat actors, campaigns, IOCs, malware, attack patterns, tools, signatures, and CVEs affecting your organization. Our expansive database of historical threat data provides the broadest collection of context-rich insights for focused red teaming and effective cybersecurity.



## Threat Explorer

Threat Explorer delivers global Threat Context information, that helps to determine the level of exposure your business faces.

Threat Explorer detects vulnerabilities in your technology and analyzes this with our Threat Intel Driven Sandbox ensuring you are kept informed of malware targeting your business.



## Dark Web

Boost your awareness of what's going on in the underground, observe malicious activities targeting your organization and proactively prevent future attacks. Gain an advantage by putting an eye in the enemy camp: become better informed about criminals targeting your organization; proactively prepare countermeasures; find stolen user credentials and assets in real-time.



## Credentials

Find actionable intelligence around leaked, stolen and sold user credentials. We locate them in real-time on the open, deep and dark web, along with information about relevant malware used to steal the information. Outpost24's sinkholes, honeypots, crawlers and sensors are continuously searching for your stolen credentials from leaks, on forums and in real-time from targeted malware, helping eliminate serious attack vectors and fraudulent actions in minutes rather than in months.

We retrieve two types of stolen credential information. Botnet/BotIP credentials stolen by crime servers and Hacktivism credentials from cybercrime forums, paste sites, P2P, dark web sites and more.



## Data Leakage

Discover if your organization's sensitive documents and source code has been leaked on the internet, deep web or P2P networks, intentionally or not, such as with shared internal documents with poorly-secured file sharing providers.



## Credit Cards

Dig deep enough and you can find all sorts of credit card data online. This module can dramatically reduce losses from theft and fraud of credit cards. We retrieve stolen credit card data and provide relevant information to help organizations mitigate the damage.



## Hacktivism

The Hacktivism module monitors hacktivism activity on social networks, paste sites, IRC chats and more. Ensuring you are made aware of hacktivism groups looking to attack your critical assets. The Hacktivism module allows you to identify and detect zero-day vulnerabilities affecting your software and hardware and strengthen your defenses against potential attack vectors.



## Mobile Apps

Protect your organization against counterfeit apps or apps impersonating your corporate identity. These apps often outdated or maliciously altered can facilitate activities like phishing and pose a significant threat to your brand and customer data. With our mobile app monitoring, you can ensure your information is secure and your brand reputation is maintained.



## Social Media

Monitor and check your organization's digital footprint across Web 2.0 repositories, including blogs, forums, websites, and social networks. Find websites not authorized to use your brands, logos, assets claiming partnership affiliation assets and more, so you can take proactive steps to shut them down.



## Domain Protection

Fraudulent domains are a risk to your organization and your end customers, with the goal of stealing critical information or damaging your brand. Combat phishing and typo-squatting by proactively detecting attacks and take countermeasures to protect your organization.

[Get a Demo](#)[Become a MSSP](#)

# Customized to your needs

*Threat Compass provides a central point of control for automated operational, tactical and strategic threat intelligence*

## Collection

Outpost24 automates threat data collection from multiple sources and in multiple formats.

## Correlation & enrichment

Threat Compass provides powerful information categorization, honey client direct side validation, and sandbox analysis and scoring.

We also investigate data collected from across third-party feeds to identify common attack vectors and actors.

## Actionable intelligence

Outpost24's powerful visualization tools represent targeted, actionable threat intelligence intuitively. Use the information to create your own YARA rules, gain a tactical advantage, and create strategic cyberthreat response capabilities.

## Threat data integration

Plugins are available for the most common SIEMs, SOAR platforms and TIPs. Outpost24 supports STIX/TAXII for easy information sharing between different data formats.

## Collaboration is key

Share relevant information across your internal groups and with trusted third parties.

Enable a single user to collect threat data of specific interest and easily share relevant, timely, accurate Indicators of Compromise about emerging or ongoing cyberattacks to avoid breaches or minimize damage from an important attack.

## Accelerated, adaptive response

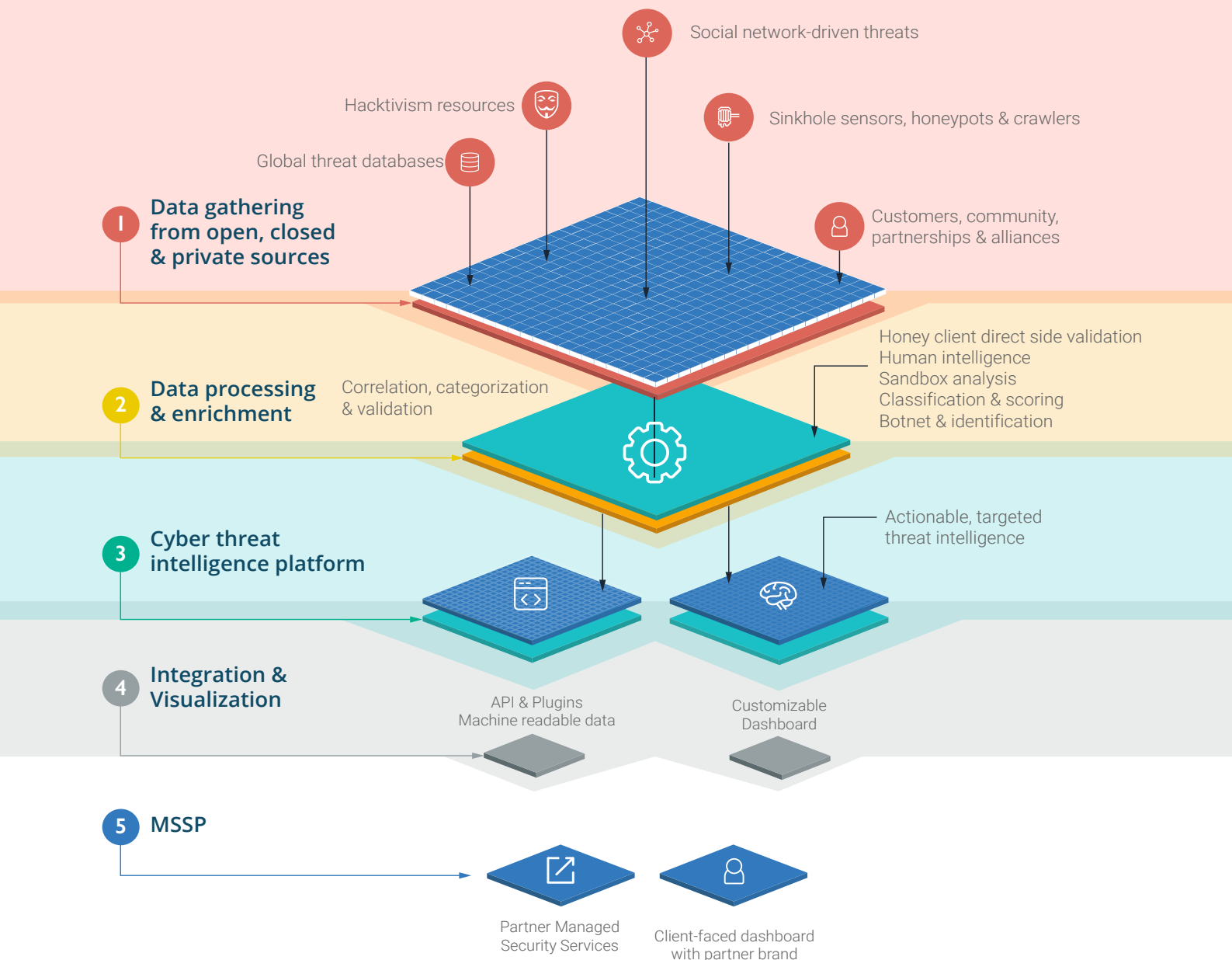
By automating targeted threat intelligence collection and presentation, you gain greater visibility into threats and reduce incident response times.

Big data analytics capabilities quickly deliver actionable information with minimal false positives in a single dashboard view - with context and underlying detail – for faster decision-making.

## Maximize limited resource

Eliminate the need to sort through thousands and thousands of alerts, and let your team focus on targeted threat intelligence with sophisticated analysis capabilities.





## Build strategic responses

Threat Compass enables you to build a list of malicious IP addresses, which can be added into internal and perimeter security control devices. It identifies compromised accounts being used to access corporate resources and ensures greater scrutiny and control over mobile applications and claimed associations. Using Threat Compass users can understand the kill chain and maximize internal security efficiency.

## Easy to deploy

Threat Compass' modular architecture is easy to deploy and provides high-impact results immediately. The cloud-based solution eliminates the need to install hardware or software. Flexible licensing options make it easy to provide adaptive protection across the enterprise to operations located anywhere. Deploy compliant controls exactly where they're needed, and see results in minutes, not months.






## About Outpost24

The Outpost24 group is pioneering cyber risk management with vulnerability management, application security testing, threat intelligence and access management – in a single solution. Over 2,500 customers in more than 65 countries trust Outpost24's unified solution to identify vulnerabilities, monitor external threats and reduce the attack surface with speed and confidence.

Delivered through our cloud platform with powerful automation supported by our cyber security experts, Outpost24 enables organizations to improve business outcomes by focusing on the cyber risk that matters.

 [outpost24.com](https://outpost24.com)

 [info@outpost24.com](mailto:info@outpost24.com)

 [twitter.com/outpost24](https://twitter.com/outpost24)

 [linkedin.com/outpost24](https://linkedin.com/outpost24)

Blueliv® is part of the Outpost24 Group. is a registered trademark of Leap inValue S.L. in the United States and other countries. All brand names, product names or trademarks belong to their respective owners.  
© LEAP INVALUE S.L. ALL RIGHTS RESERVED