

MAKE MORE INTELLIGENT DECISIONS

Business Risk Intelligence (BRI) from the Deep & Dark Web

What is Business Risk Intelligence (BRI)?

Business Risk Intelligence (BRI) broadens the scope of cyber intelligence beyond threat detection to provide relevant context to business units not traditionally afforded the benefits of intelligence derived from the Deep & Dark Web. By informing decision-making and improving preparation, BRI mitigates risk across the enterprise resulting in better decisions that protect a company's ability to operate.

The Story Behind BRI

We've spent years helping companies monitor threats emerging from the Deep & Dark Web. Once customers began using our insights to better understand how these threats influence widespread risk, we recognized that our Deep & Dark Web intelligence could be relevant to far more than just security teams. From fraud to physical protection and beyond, all business functions can leverage our intelligence to alleviate the broad spectrum of challenges and uncertainties contributing to a company's overall risk. Our intelligence can be utilized across the enterprise, so we call it Business Risk Intelligence.

BRI APPLICATIONS



Cyber Threats



Incident Response



Data Loss Prevention



Physical Security



Brand Protection



Third-Party Risk



Fraud



Insider Threat

Why BRI?

Suffuses an entire organization with relevant intelligence



Addresses a full spectrum of threats to mitigate risk, no matter the business function






Helps leaders and stakeholders make better, more informed decisions



The BRI Equation

This BRI equation helps decision-makers across industry verticals and business functions identify and assess the variables impacting their company's overall risk. Below, we've illustrated how our customers have used this equation to apply BRI and mitigate risk in three different scenarios.

$$\text{Asset} + \text{Threat} + \text{Vulnerability} - \text{BRI-Informed Countermeasure} = \text{Risk Outcome}$$

Use Case	 Insider Threat	 Fraud	 Physical Security
Asset	Source code from an unreleased, enterprise-level software	The upcoming USA rollout of Europay Mastercard Visa (EMV)	A Fortune 100 CEO planning to attend a popular public event
Threat	Rogue employee offering to sell the source code on an underground marketplace	Cybercriminals seeking to bypass EMV anti-fraud measures and make fraudulent transactions	Unknown politically-motivated threat actors located in the vicinity of the upcoming event
Vulnerability	Lack of visibility into "extra-curricular" employee browsing activity	Insufficient anti-fraud measures and lack of visibility into the cyber threat landscape	Lack of visibility into the physical threat landscape around the event
BRI-Informed Countermeasure	The company started cross-checking Deep & Dark Web activity with their own internal activity	Financial institutions began monitoring cybercriminal forums to better understand EMV's cyber threat landscape	Prior to the event, security teams collaborated with Flashpoint to identify relevant physical & cyber threats
Risk Outcome	BRI enabled the company to discover and prevent the sale and work with law enforcement to take action against the rogue employee	BRI revealed tactics for exploiting EMV and bypassing anti-fraud measures, so financial institutions could adjust EMV rollout plans to reduce the likelihood of fraud	BRI enabled physical security teams to protect both the executive and the brand's integrity from nearby threat actors during the public event

About Flashpoint

Whether you're an intel expert or new to BRI, we strive to deliver relevant intelligence that can help our customers make informed decisions and mitigate risk.



People

We're a diverse group of white hat hackers, multilingual maestros, and intel geeks who've built programs for the Fortune 500, caught bad guys for the government, and helped leaders make tough decisions.



Data

Intelligence relies on data, and we've spent years honing the cultural, lingual, and technical savvy required to get our hands on the richest Deep & Dark Web data available.



Technology

We've built technology informed by our analysts and customers to drive targeted data acquisition at scale and serve up the most critical data from the Deep & Dark Web.