CHECK POINT™

Infinity

INFINITY EXTERNAL RISK MANAGEMENT

Brand Protection Module

Infinity ERM continuously monitors the web for illegal use of trademarked brand names and logos, as well as malicious impersonation of executives. This includes detection of lookalike domains, phishing sites, malicious applications on official or unofficial app stores, and more. It also includes fraudulent social media profiles that impersonate brands, products, or members of the executive leadership team.

The Infinity ERM Brand Protection module comprises the following capabilities:

Module	Description	Entitlements
Infinity ERM Application fundamentals	Asset Discovery Engine	Included
	Alerts Center	Included
	Number of regular users	2
	Number of Threat Hunting users	-
	Tenants (a distinct Infinity ERM environment allowing users to visualize intelligence alerts for one company, subsidiary, or brand separately)	1
	Out-of-the-box integrations	1
	Customer Success Manager cadence	Yearly
	Support SLA	Direct Premium
Brand Protection Module	Typosquatting & phishing & brand abuse sites detection	Included
	Social Media and mobile app impersonation for brand and VIPs	Included
	Manual Threat Hunting for impersonation (Cyberint Analyst)	-
Global Threat Intelligence	Global cyber news and ransomware watch	Included
	Cyberint research threat intelligence reports	-
	Global Intelligence Knowledgebase (Threat Actors, Malware, CVE)	-
	IoC searches and browser extension	Included
Remediation & Investigations	Remediation Credit Points ("Coins") for takedowns* and investigations	40

*Subject to signing Check Point's letter of authorization (LOA)

Phishing Detection

Phishing is still one of the top 3 most common attack vectors. The reason for its success is twofold: (i) it is relatively simple for a novice threat actor to set up a phishing attack, and (ii) it's designed to trick ordinary users, which is a guaranteed success given enough attempts.

To maximize protection against phishing attacks, Infinity ERM is designed to cover each step in both of the attack scenarios illustrated above. Infinity ERM's algorithms combine automatic generation of domain permutations with open source and advanced DNS intelligence to predict with high confidence an imminent phishing attack. Together with the phishing beacon, which proactively protects against phishing sites hosted on domains that aren't flagged as suspicious, Infinity ERM is able to provide the broadest protection against phishing attacks.

Lookalike Domain Monitoring

Infinity ERM continuously monitors for similarities between your domains and the newly registered candidates to provide a level of indication of malicious intent, and alerts you to suspicious, newly registered lookalike domains.

Each domain is tracked for A and MX records to assess the risk. Infinity ERM automatically looks for applications or content on the lookalike domains to check for source code or logo similarities. Upon reaching a minimum risk threshold, Infinity ERM will trigger a phishing alert suggesting remediation steps.

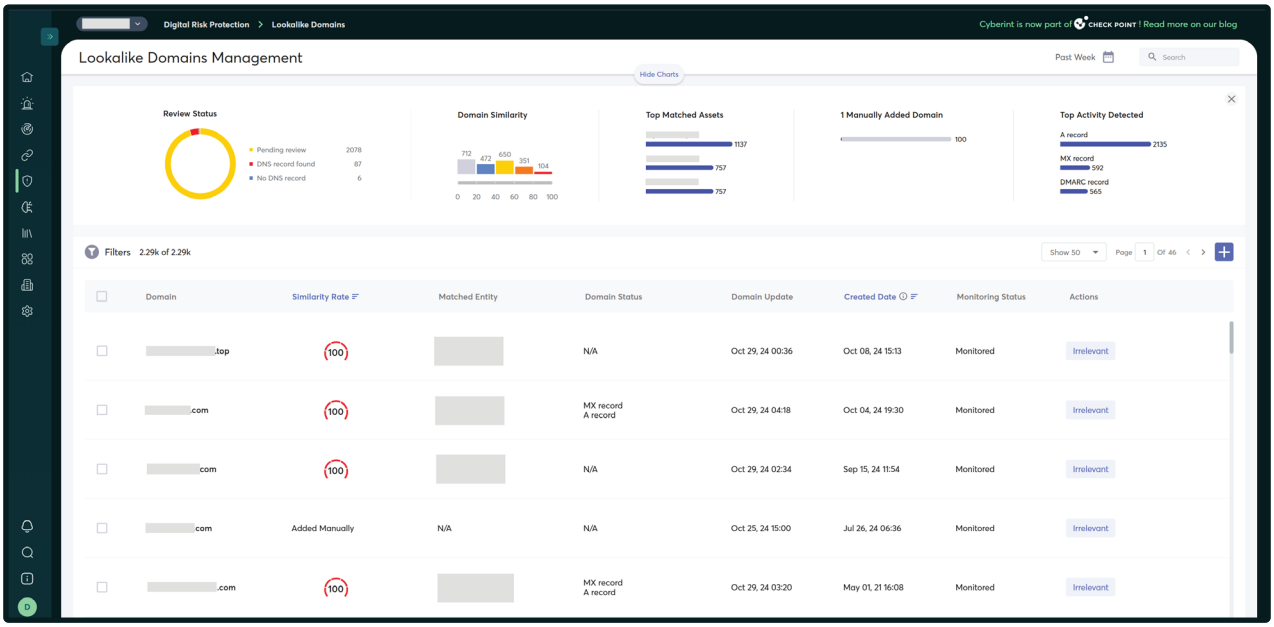

Figure 1 - Argos Lookalike domain tracking module

Social Medial Impersonation

The Social Media Impersonation capability continuously monitors popular social media platforms to identify fraudulent accounts that impersonate brands, organizations, and other registered trademarks, such as product names, as well as executives and important individuals.

The following social media platforms are covered:

- Instagram
- Facebook
- Twitter
- LinkedIn

The Social Media Impersonation Module operates on the customer-configured brand and person keywords which have impersonation enabled. Upon identification of impersonation, an alert is triggered to support remediation.

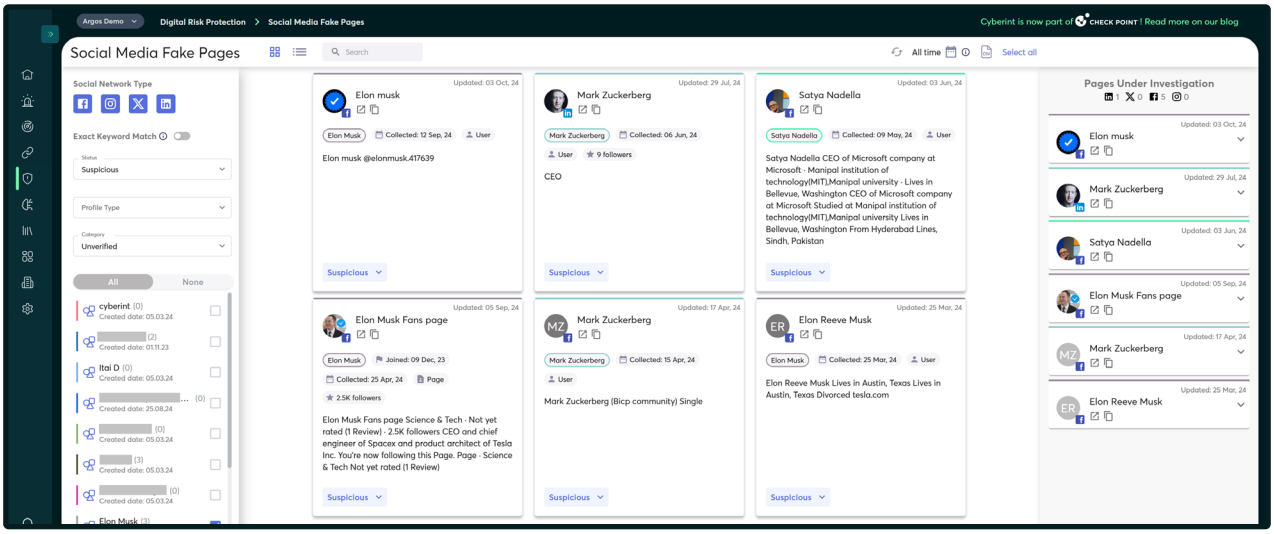

Figure 2 - Social Medial impersonation detection module

Brand Impersonation

Threat actors impersonate trusted brands on social media for a variety of reasons. The purpose may be to drive traffic to a phishing site, where unsuspecting users are subsequently fooled into giving up credentials and other sensitive data. The goal may be to pass off trojanized applications or counterfeit goods as legitimate. Or, in some cases, the objective may simply be brand abuse, impersonating an established brand in order to degrade its value.

The Infinity ERM solution's Social Media Impersonation Module monitors for impersonation of organizations, brands, products, and other registered trademarks. Customers can manually set all of the keywords they would like to monitor upon deploying this module.

Executive Impersonation

In addition to impersonating brands, attackers often impersonate executives within major organizations, such as the CEO, CFO, CISO, or other senior management personnel. In some cases, the attackers impersonate executives in order to have fraudulent invoices paid, effectively stealing money directly from the organization. In other cases, threat actors impersonate executives to recruit legitimate candidates for fake jobs, eventually sharing malware-infected files with the victims to compromise their machines and environments.

Infinity ERM's Social Media Impersonation Module monitors for impersonation of executives across major social media platforms, simply using the first and last names of the executives whom the customer would like to safeguard against impersonation.

Alerting and Remediation

When a suspicious profile is detected, it is added to the Social Media Impersonation Module dashboard for review. If the account is, in fact, authentic, it can be marked as such from the dashboard. Similarly, innocuous profiles can be marked as irrelevant. The profiles that represent real threats are marked as Suspicious and/or converted into an Alert.

Once a social media profile has been converted into an Alert, it will then appear under the Alerts screen and additional actions can be taken. This includes submitting a takedown request, which can be done within the Infinity ERM solution with a few clicks. A dedicated takedown team handles takedowns across all social media platforms in scope for monitoring.

Licensing Details

These licensing instructions are related to the Infinity ERM packages: Essentials, Advanced, Complete, Elite.

	Licensing Instructions
Brand Protection Module	This licensing instructions are related to Brand Protection module.
	The main licensing dimension is Brand Assets, also known as Threat Intelligence Asset. Assets are: Brand, Domain, Social Medial Account, Keyword, VIP name, and more. Generally, in order to fully protect a brand, 2 assets are required: Domain (Example: www.checkpoint.com) & Brand (example: Check Point). These are configured in phishing protection, lookalike domains, social media impersonation and other related modules.
	Select the amount of asset needed based on the customer needs. Additional assets can be acquired as ad-on.
	The stand alone Brand Protection module doesn't include managed services. If required, the Complete and Elite packages include managed services.
	The Brand Protection module includes remediation credit points ("Coins") which can be used for takedowns, darkweb credential purchases and analyst investigations on demand (4-8 coins per takedown, 8 coins per investigation hour, 6 coins for darkweb credential removal).
	Monthly licensing is not available.

The following table displays the number of External Assets and Threat Intelligence Assets that come at eachpricinginterval. Additional External Assets and/or Threat Intelligence Assets can be procured as an add-on, if needed.

ASM assets	200	500	1,000	2,000	5,000	10,000	25,000	50,000	100,000	200,000	350,000
TI assets	30	50	100	150	200	300	400	500	600	800	1,000

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com