

Executive Briefing





"This is the daily dose of cyber news despite all the millions spent"

3.5m MobiKwik users' data up for sale on dark web

[!\[\]\(666e09182d4cd268646ea700ea60dcdf_img.jpg\)](#)
[!\[\]\(1ef1ef0bf9af6c6996401964cf280f2d_img.jpg\)](#)
[!\[\]\(e9a80c8557f9285916925bd4ac40fff5_img.jpg\)](#)
[!\[\]\(88e2edecff3400e68a80dd08c57d2f9c_img.jpg\)](#)

This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers. **It is very possible that your browser isn't affected.**

Exposed ELK Exploited !

[illegible]



The Broken Triage

**Threat Intelligence is
in fact only threat
data**

**Asset visibility beyond
firewall is limited &
without context**



**Risk perspectives are
operational & half
baked**



Troublesome CISO Questions

DATA

Is my data on the Dark Web?



GAPS

What gaps exist or develop on my digital surfaces?



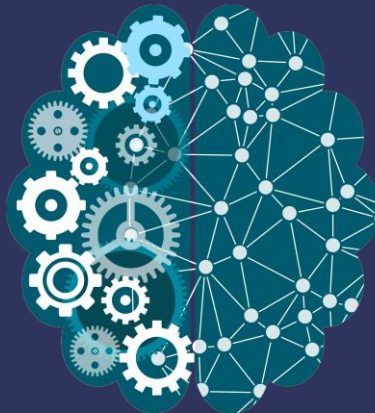
RISK

What is the risk exposure to my organization?



THREAT SOURCES

What threat actors and sources exist out there?





Need of Shift

Prioritization



Risk Perspective



Threat Intelligence



Threat Signals

Enterprise IT network



**Most Response and
Protection Actions are here**

Assets beyond firewall



**Maximum Exposure is
at perimeter**

Internet: phishing domains, stolen cred



**Constantly Evolving threat and
attack infrastructure is here**

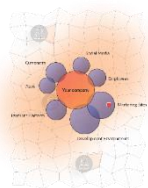
Darkweb and Deepweb



**Real threat signals and
intelligence is here**



The Answer



Continuously discovers
& maps assets beyond
firewall



Stolen Creds



Phishing



Fake Assets



Code Leaks



Hunts for your stolen
data & signals on
darkweb 24x7

Hunts, discovers and analyzes
threat sources, threat data &
threat infrastructures



- **Prioritize & Respond**
- **Know Risk Exposure**
- **Detect External Threats**
- **Manage Attack Surface**



24x7 threat watch platform

Darkweb | Attack Surface | Threat Sources | Cyber Risk


Everyday, 24x7

- Find **Stolen and Sensitive Data** across the dark web, gitHub, paste sites, your web
- Detect new **Phishing Domains** and check **Social Media** for handles and posts
- Catch **malicious chatter** on darkweb and identifies potential adversaries & attacks
- Identify **fake digital assets** such as fake mobile apps, fake sites, fake no listing
- Keeps a watch for **new vuln** due to **misconfigs** and **exploits** on web, net, cloud & API surface
- Locate **hacked password** on dumps and **dark web** commerce sites
- Measure and know your **threat score** as well as how you compare to industry/peers
- Get **proactive alert** you on **urgent** findings, out of our reporting schedule



Threat Watch Coverage



 7.4

Surface Map

Domain/Sub-Domain Enumeration
Domain Threat Analysis



 1.6

Phish Watch

Hunts Phishing Domains
Phishing Suspect Analysis



 2.8

Cred Watch

Employee Credential Loss
Credential Stuffing Risk Analysis



 2.1

Reputation Watch

Blacklists Monitoring
Detection of Malicious Content



 8.5

Fake/Fraud Watch

Monitoring for Fake Sites/Pages
Detecting Misuse of Social Accounts



 4.4

Social Watch

Social Surface Inventory for Company
Social Surface Check for Company



 9.2

Dark Watch

Dark web Monitoring
Breach & Stolen Data Detection



 1.2

git Watch

git Scan for Code Leakages
Threat Analysis of Detected Code



 5.6

Leak Watch

Leakage Detection on Company Web
Threat Analysis of Leaked Info



 4.9

Attack Surface Watch (Web)

Continues map of web attack surface
Gaps & Vulnerabilities



 3.1

Attack Surface Watch (Network)

Continues map of network attack surface. Gaps & Vulnerabilities



 1.2

Attack Surface Watch (DNS/Mail)

Continues map of DNS/Mail surface
Gaps & Vulnerabilities



 6.2

API Watch

Continues map of API surface
Gaps & Vulnerabilities



 6.1

Cloud Watch

Continues map of cloud surface
Gaps & Vulnerabilities



We are exploring more
threat components and
adding them to our platform



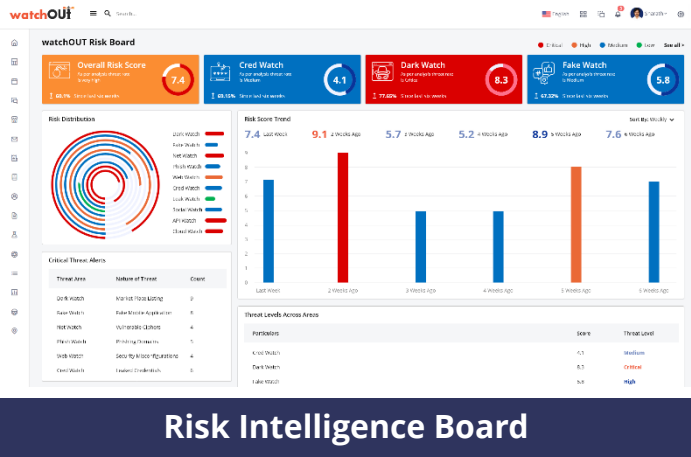
Take Action

Address gaps on
attack surface

Take action on
threat sources

Act on darkweb
data & threats

Manage your
risks exposure





SaaS Platform

SaaS cloud platform for 24x7 monitoring of external threats



No Installation

Not agents, no setup. We take a hacker's view of your enterprise



Subscription

Available as a subscription, just one risk mitigated pays you back



Monitoring

Beyond reporting, you get cyber experts assessment and advice



watchOUT Risk Board

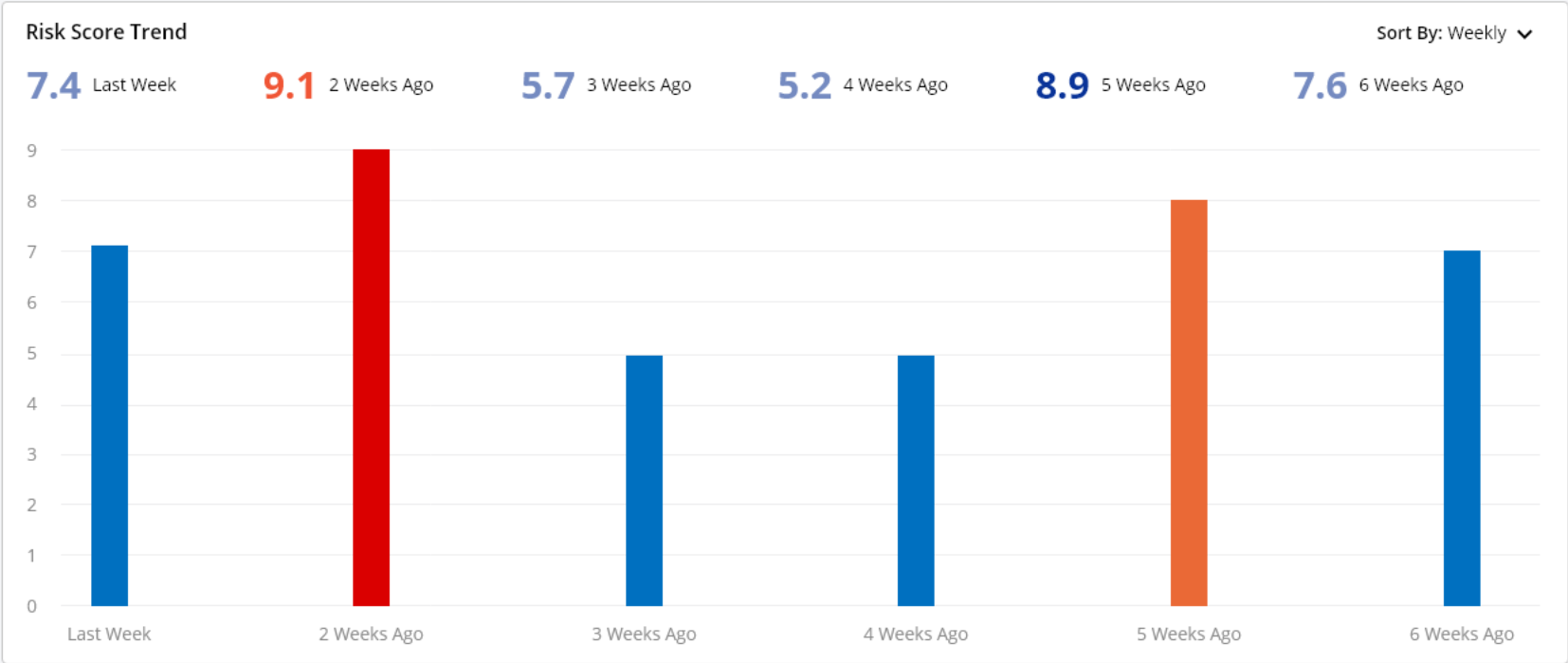
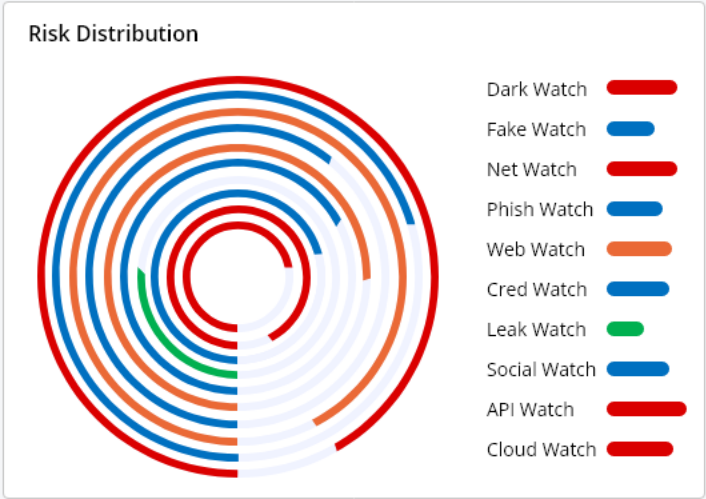
Critical High Medium Low See all >

Overall Risk Score
As per analysis threat rate is very high
7.4
↑ 60.1% Since last six weeks

Cred Watch
As per analysis threat rate is Medium
4.1
↑ 69.15% Since last six weeks

Dark Watch
As per analysis threat rate is Critical
8.3
↑ 77.65% Since last six weeks

Fake Watch
As per analysis threat rate is Medium
5.8
↑ 67.32% Since last six weeks



Critical Threat Alerts

Threat Area	Nature of Threat	Count
Dark Watch	Market Place Listing	9
Fake Watch	Fake Mobile Application	8
Net Watch	Vulnerable Ciphers	4
Phish Watch	Phishing Domains	5
Web Watch	Security Misconfigurations	4
Cred Watch	Leaked Credentials	6

Threat Levels Across Areas

Particulars	Score	Threat Level
Cred Watch	4.1	Medium
Dark Watch	8.3	Critical
Fake Watch	5.8	High



Sample WO Alerting/Reporting/Interface

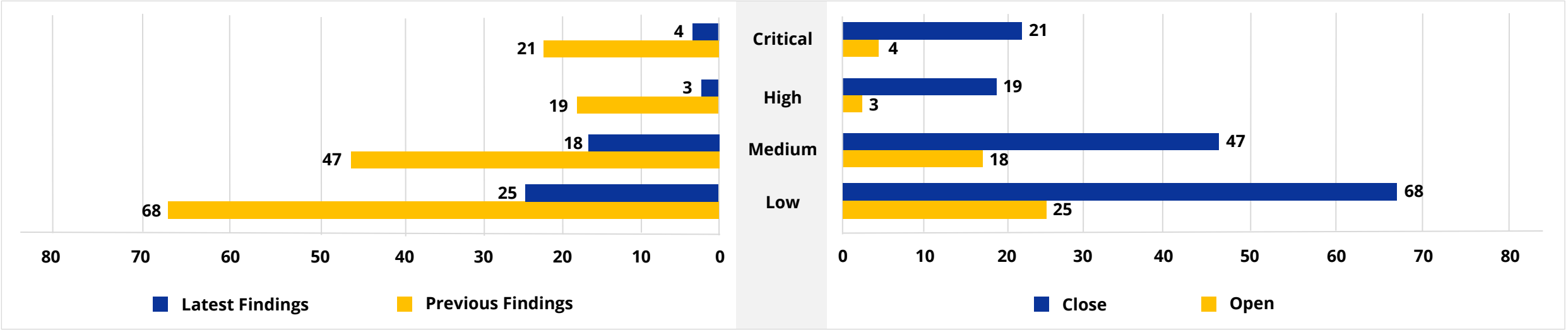
Finding Summary @ Web WATCH	Latest	Previous	Overall
New Insecure S/W Detected on Web Surface	15	43	58
Endpoints with Insecure Config Settings	12	45	57
Attack Vector Susceptibility	23	67	90

Web Watch Threat Index Level

Medium

4.9

Alert Severity Distribution for Web WATCH



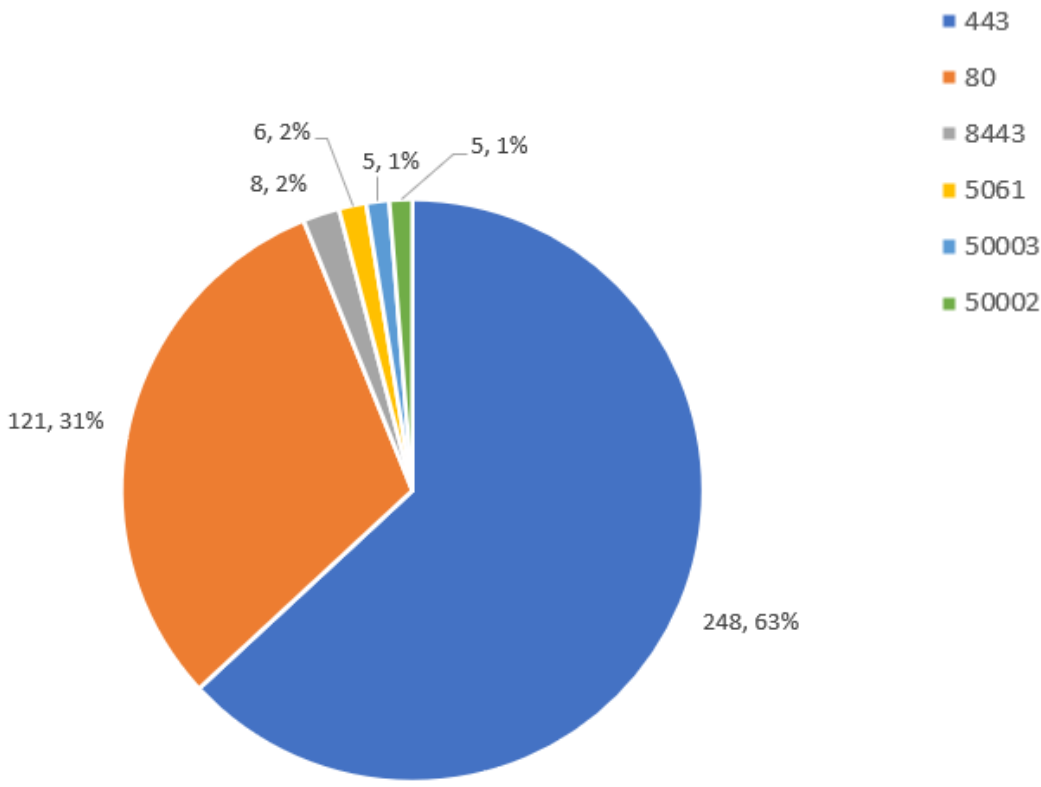


Domain	Vulnerability Name	Info	Location of the Vulnerability	Potential Threat	Alert Severity
http://example.com	Admin Panel Disclosure	Default file access	http://example.com/admin/	Internal Files Disclosure	High
http://example.com	Admin Panel Disclosure	Default file access	http://example.com/admin/	Internal Files Disclosure	High
git://example.com	Directory traversal	Testing for Directory traversal	http://example.com/.git/info/expose	Internal Files Disclosure	Medium
git://example.com	Directory traversal	Testing for Directory traversal	http://example.com/.git/objects	Internal Files Disclosure	Medium
example.com	Host Header Injection	Host header injection is possible	http://example.com	Business Logic Bypass	Medium
http://example.com	Admin Panel Disclosure	Default file access	http://example.com/admin/	Internal Files Disclosure	Critical
git://example.com	Host Header Injection	Host header injection is possible	http://example.com/.git	Business Logic Bypass	Medium
example.com	Insecure error handling	Testing for Insecure error handling	http://example.com/error.php?admin	Sensitive Info Disclosure	Critical
http://example.com	Admin Panel Disclosure	Default file access	http://example.com/admin/	Internal Files Disclosure	Critical
http://example.com	Admin Panel Disclosure	Default file access	http://example.com/admin/	Internal Files Disclosure	Critical
git://example.com	Server Information in Headers	Checking for server information in headers	http://example.com/.git	Attacker might try for known vulnerabilities	Low
example.com	Server Information in Headers	Checking for server information in headers	http://example.com	Attacker might try for known vulnerabilities	Low
example.com	Server Information in Headers	Checking for server information in headers	http://example.com	Attacker might try for known vulnerabilities	Low
example.com	Application Supported HTTP Methods	Insecure HTTP methods allowed	http://example.com/examples/unsafe/protected.html.js	HTTP Verb Tampering	Medium



Sample WO Alerting/Reporting/Interface

Net Watch – Protocol Map – Top 5 Ports



Net Watch – Protocol Map - Public IP Addresses



Net Watch – Protocol Map - Open Services





Summary of Reported Threats for “One Current Customers”

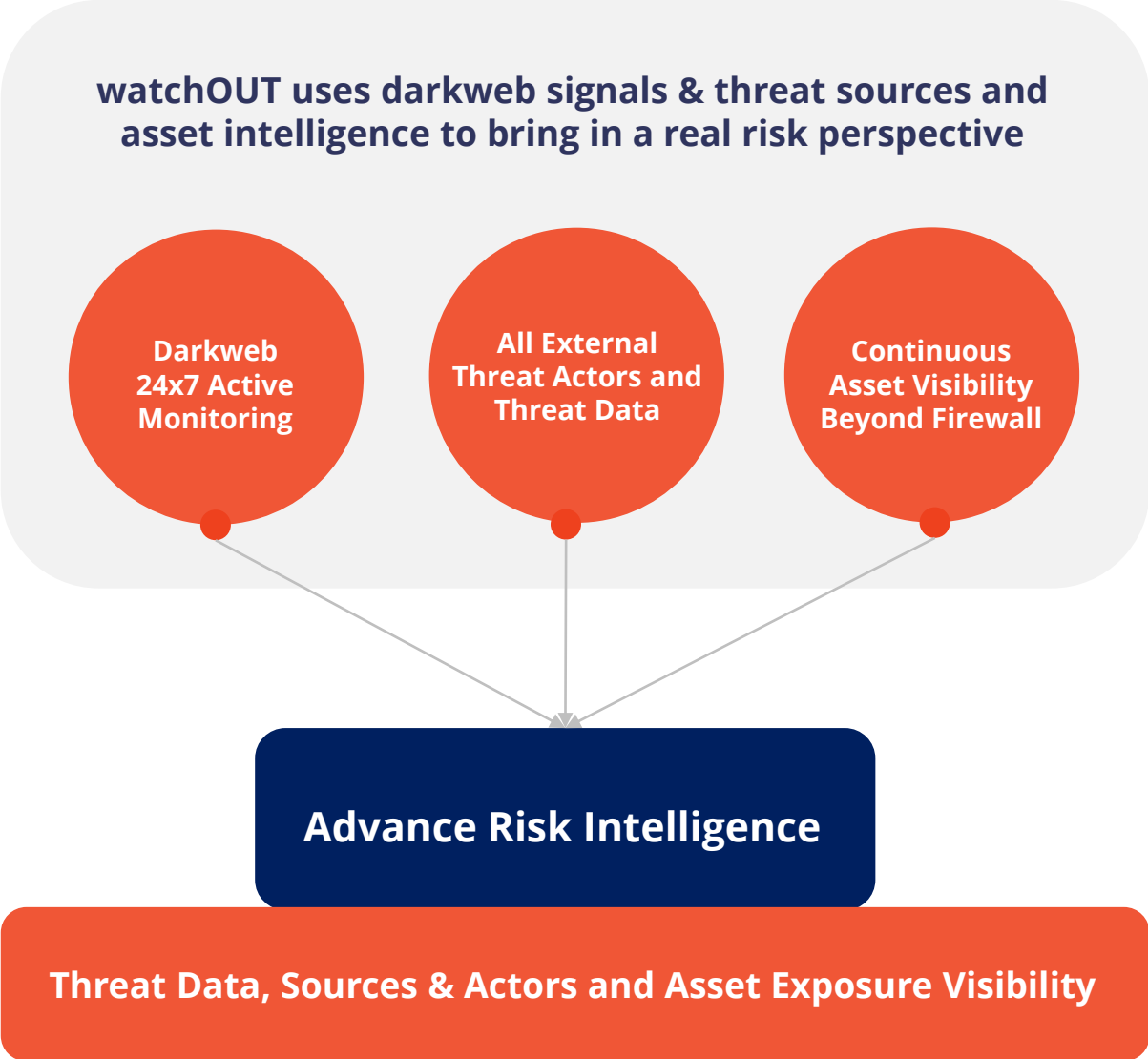
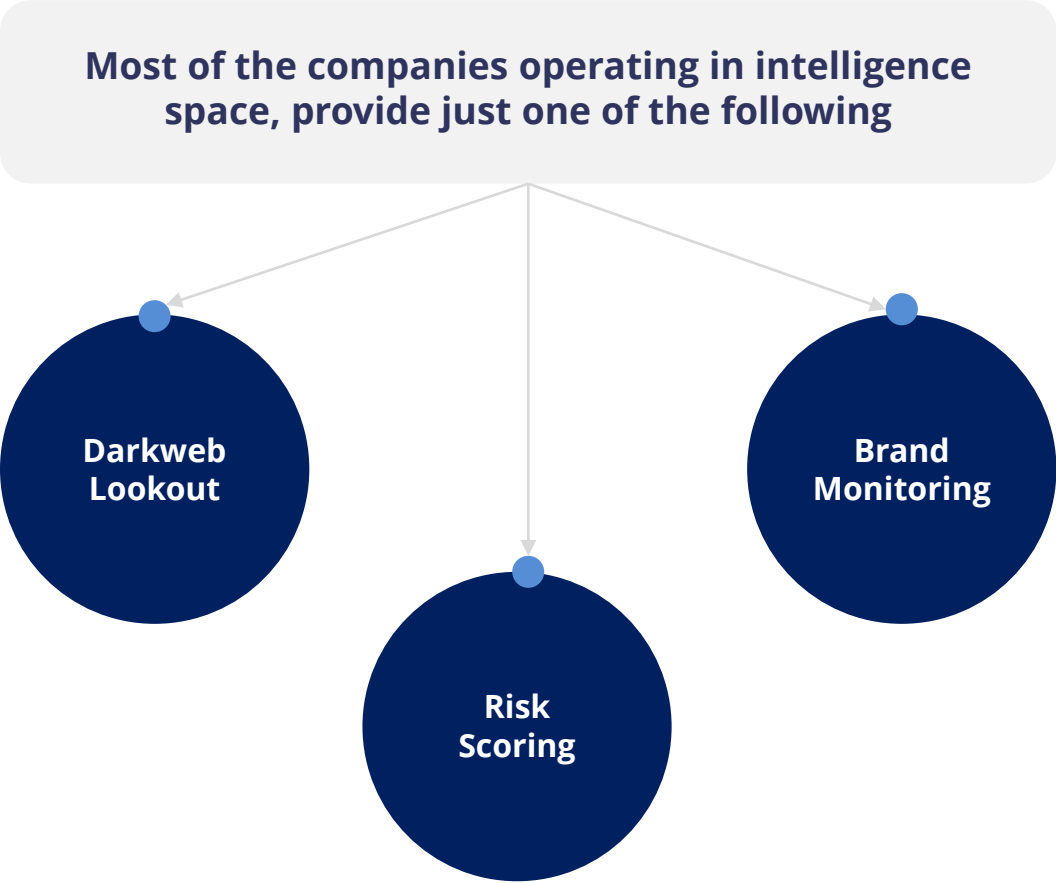
“Summary List of Reported and Closed Critical & High Severity Threats in 11 Months”

Large number of medium and low severity threats also reported. Their count not included here.

Months	Threat Area	Reported Issues	
		Critical	High
20-Oct	CredWATCH	2	
20-Nov	CredWATCH	2	
20-Nov	Attack Surface Watch (Net)		15
20-Dec	CredWATCH	1	
20-Dec	Attack Surface Watch (Net)		15
21-Jan	PhishWATCH		1
21-Jan	Attack Surface Watch (Net)		15
21-Mar	PhishWATCH		1
21-Mar	Attack Surface Watch (Net)		15
21-Apr	CredWATCH	16	
21-Apr	Attack Surface Watch (Net)		15
21-Aug	NetWATCH		22
21-Aug	WebWATCH		14
21-Sep	WebWATCH		20
21-Sep	WebWATCH	1	5



Integrated Comprehensive Platform





Know More @ _____

www.getwatchout.com

info@getwatchout.com

