FireCompass

Continuous Attack Surface Management & Red Teaming

Shadow IT Monitoring, Ransomware Risk Assessment,
SOC Effectiveness Testing & more

SaaS Platform To Run Continuous Real Life Attacks To Safely Discover Blind Spots Before Attackers Do

Every company needs to be aware of security blind spots that are created by increasing cloud adaptation, unknown applications used by agile teams, shadow IT assets, misconfigured assets, etc. Even the best organisations with good teams and tools are in the danger of getting breached.

To eliminate security breaches, you need to be aware of your Digital Attack Surface. FireCompass provides a Saas tool to help organizations discover their Attack Surface.No additional software and no additional configuration is required. Our automated internet wide monitoring capability helps to map your entire digital attack surface and find out the breach risks associated with it.

Simulating real attack through red teaming is the best way to find security gaps and to measure security controls effectiveness. FireCompass provides the ability to continuously conduct recon along with advanced simulation of hacking attempts on your digital attack surface to find out the attack paths before hackers exploit them.

Key Use Cases

- Attack Surface Management (ASM)
- Continuous Automated Red Teaming (CART)
- SOC & Security Control Effectiveness Testing
- Digital Footprint & Shadow IT Discovery
- Ransomware Risk Assessment
- Supply Chain Risk Assessment
- M&A Risk Assessment

Key Advantages

- **Continuous:** Automated Internet wide monitoring capability
- **Comprehensive:** Real attacks (Ransomware, Expert Red Teaming)
- **On Demand Predictive:** Historical Data & Artificial Intelligence
- **Zero Setup time:** No Hardware or Software Installation
- **Speed Cost Saving:** 90% of more cost savings compared to traditional methods

How Does It Work?

1. Index: Continuous Indexing of Deep, Dark & Surface
Our Headless browser crawls across 3+ billion IP's around the globe and collects intel from 3rd party sources like Shodan, Honeypot, Threat intel, etc and indexes it using our big data platform.

2. Discover: Zero Knowledge Attack Surface Discovery
Using AI and ML algorithms, we attribute all your digital assets and provide a near real time view of your Digital Attack Surface. Discover all IPs, Applications, exposed database/cloud buckets, code leaks, leaked credentials, vulnerabilities, exposed test/pre-production systems and risks associated with it.

3. Attack: Multi Stage Attacks
We conduct multi-stage attacks just like real attackers to find vulnerabilities before other attackers do. FireCompass provides ability to continuously conduct recon along with advanced simulation of hacking attempts on your digital surface to find out the attack paths before hackers can exploit them.

4. Prioritize: Risk Based Prioritization
FireCompass SaaS tool identifies, analyses and prioritizes digital risks in the order of increasing level of threats.

5. Continuous Monitoring & Alerts
You will get Continuous Monitoring & Alerts on any changes detected in your attack surface and identification of new risks.

> "To our surprise, the Tool has exceeded our expectation in identifying numerous domains and subdomains that are shown as public, but should be private."
>
> **Risk Manager, Top 5 Telecom Company**

Technical Capabilities

Reconnaissance & Attack Surface Discovery Capabilities

- Fast internet based recon on 3 billion+ IPs using headless browser
- Deep, dark and surface web OSINT data collection
- Intel collection from 3rd party sources like Shodan, Threat Intel, Honeypot feeds, etc.
- Misconfigured DB servers/ S3 cloud buckets
- Code leaks, leaked credentials
- Vulnerabilities - Internet infrastructure, web apps, mobile apps
- Exposed pre-prod systems
- Exposed services like APIs, Open Ports

Multi-stage Attack Capabilities

- Conduct Port Scanning & Network VA
- Conduct DAST and OWASP Top 10 attacks on web based applications
- Conduct DAST, SAST and IAST attacks on mobile applications
- Active social engineering attacks
- Multi-Stage attacks to find out possible attack paths

Risk Based Prioritization

- Vulnerabilities prioritized as critical, high, medium or low
- Prioritizing risks based on each asset to identify how critical it is for business and how vulnerable it is
- Risk-based prioritization helps to focus efforts on the vulnerabilities that are most likely to be exploited

Monitoring & Alert

- Continuous Monitoring & Alerts to detect changes in your attack surface and new risks

How Is FireCompass Different?

	DRP	VA/PT Tools	Consultants	Firecompass
Digital Footprint/ Recon	✓	✗	✓	✓
Dark web	✓	✗	✓	✓
Port Scan/ VA	✗	✓	✓	✓
Application Attacks	✗	✓	✓	✓
Multi Stage Attacks	✗	✗	✓	✓
Social Engineering	✗	✗	✓	✓
Continuous Recon	✓	✗	✗	✓
Continuous Attack	✗	✗	✗	✓
Real Time Alerts	✓	✓	✗	✓

About FireCompass

FireCompass™ is a SaaS platform for Continuous Automated Red Teaming (CART) and Attack Surface Management (ASM). The platform continuously indexes data from the deep, dark and surface web.

Using this proprietary data, FireCompass automatically discovers an organization's digital attack surface. After discovery, it continuously monitors and launches simulated attacks just like a real attacker to discover and patch holes in your defense.

Founded by serial cyber security entrepreneurs, FireCompass is used by the world's foremost organizations to conduct continuous red teaming attacks, which was previously not possible with traditional manual approaches.

To learn more, visit www.firecompass.com.