Active Risk Monitoring

At-Bay's solution to the dynamic nature of cyber risk

Cyber risk is dynamic, and numerous new risks emerge over the course of an insurance year. To meet this threat, At-Bay employs **active risk monitoring** to continuously watch over insured businesses and help them stay secure year-round.

What is active risk monitoring?

Active risk monitoring (ARM) is a combination of frequent security scans to detect vulnerabilities and an in-house security team to help insureds and their brokers resolve issues before they are exploited. ARM allows us to address changing conditions in the cyber market and serves as a feedback loop that provides immediate security insights to make better underwriting decisions.

At-Bay customers experience 5x fewer ransomware incidents than the industry average through active risk monitoring.

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form. ©2022 At-Bay. All Rights Reserved.

How active risk monitoring helps insureds avoid loss

We scan the digital assets of our insureds to look for security issues that are commonly exploited by attackers, both at the time of quoting and throughout the policy year. One-time security scans don't always capture the dynamic nature of cyber threats or IT changes, so we actively scan and notify insureds if new issues appear, such as vulnerable software, unprotected email services, exposed system entry points, and missing password protections

ARM allows us not only to identify more of the vulnerabilities that emerge mid-policy, but also to help insureds quickly mitigate their risks:

At-Bay uncovers 80% of the RDP risk one-time scans miss

At-Bay helps insureds patch vulnerable software 5x faster

Real-time security alerts

Our security team is constantly working to stay up to date with new vulnerabilities and exploits, and creating new detection methods to help keep businesses secure. When a new vulnerability is detected, our security team immediately issues a security alert to the insured and their broker and provides recommendations on how to resolve the issue.

We only send security alerts for critical and time-sensitive vulnerabilities that are highly linked to potential loss, such as:

- Unpatched business critical systems, including **email servers**
- **Software exploits** targeting core infrastructure, such as firewalls and VPN applications
- Targeted protocols and services, such as **Remote Desktop Protocol** (RDP)

Even small businesses rely on dozens of different softwares, and it can be difficult to keep track of all vulnerabilities and patch all systems before they are exploited. We include brokers in all security alerts to ensure swift response and help insureds avoid loss. If an insured does not have a dedicated security contact on file, we will request it from the broker.

Learn more about active risk monitoring

Scan the QR code to download our new report:
Overcoming Ransomware: A Blueprint for Thriving in a Digital World

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form.