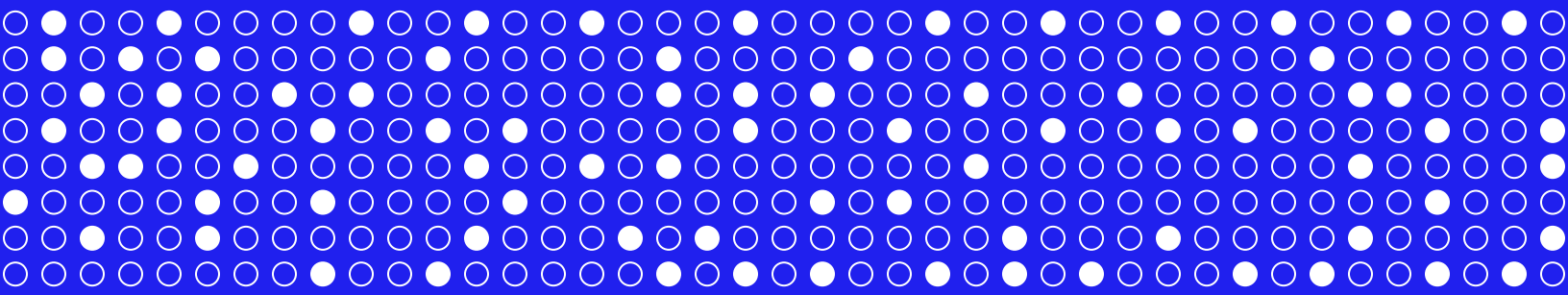
Overcoming Ransomware:

A Blueprint for Thriving in a Digital World

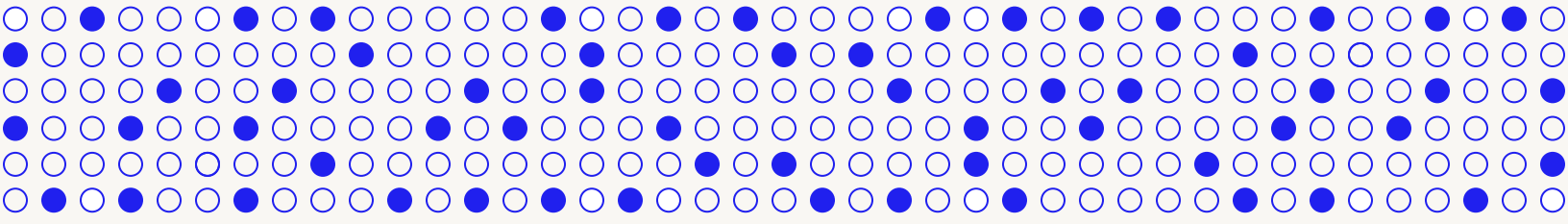


July 2021

at bay

at bay

Table of contents



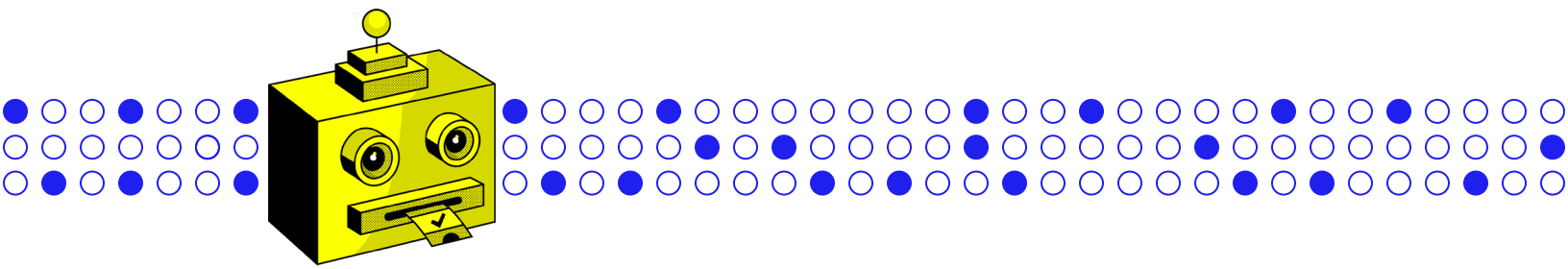
Introduction

Ransomware is the gravest digital threat to American businesses, representing an estimated 60% of all cyber insurance claims in the United States. The average ransom payment has nearly doubled in the past year,[1] and the average total recovery cost for a single ransomware incident is now $1.8 million.[2]

The insurance industry continues to reel from ransomware, as loss ratios have nearly doubled over the past 18 months.[3] Meanwhile, a high-profile attack on Colonial Pipeline in May 2021 disrupted a major supply of fuel to the East Coast, prompting significant action from the FBI and the White House. With no clear solution in sight, the industry's response has been to increase premiums by 80% across the board, with some industries experiencing spikes of up to 200%, while simultaneously reducing coverage.[4]

Cyber risk breaks two fundamental insurance assumptions. First is the notion that the risk of a business can be assessed once a year. Cyber risk is dynamic. Numerous new risks emerge over the course of an insurance year, most of which are impossible to anticipate and out of the control of an insured business. Second is that past cyber breaches are a good indicator of probabilities of future cyber breaches. Technology evolves rapidly, and insurance actuarial models have always lagged a year behind, which was rarely a problem until now.

To meet this dynamic threat, we redesigned the insurance operating system by combining technical underwriting with active risk monitoring to help businesses stay secure year-round. This approach allows us to generate a dramatic reduction in ransomware attacks in At-Bay's portfolio. In this report, we share At-Bay's blueprint for thriving in a digital world.

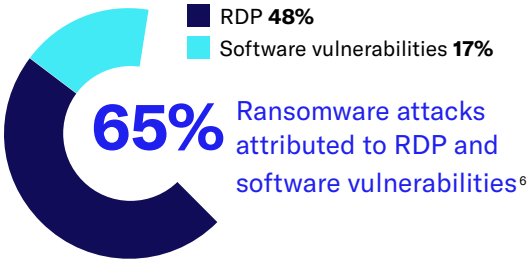


Active risk monitoring reduces ransomware attacks by 7x

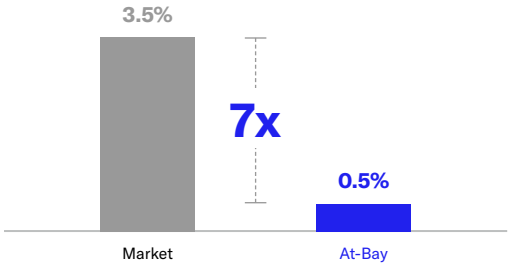
Most ransomware attacks in the middle market are not sophisticated. Attackers are not seeking out specific businesses and trying to find ways to attack them. Rather, they look for predictable and easy-to-identify security issues and attack whatever they find. Thus, the key to success in preventing ransomware is to identify ahead of time the middle-market businesses that are vulnerable and then proactively mitigate their risks.

Conducting a technical scan of a business' digital assets to find vulnerabilities, similar to how attackers identify targets, is a valuable tool when underwriting a business to offer an initial policy quote. A scan cannot find every security issue, but it can dramatically lower claim frequency by identifying two of the most common attack vectors: Remote Desktop Protocol (RDP) and vulnerable software running on publicly facing devices. Together, exploitation of RDP and software vulnerabilities accounts for 65% of all ransomware attacks.[6]

Performing a one-time scan before providing a business with insurance is a step in the right direction, but it falls drastically short of what an insurer must do to successfully manage cyber risk. New vulnerabilities are constantly emerging, and insured businesses can instantly go from secure to fully exposed.



Ransomware claims frequency



An estimated 3.5% of all cyber insurance policyholders in the U.S. have filed a ransomware claim in the past 12 months.[5] By comparison, At-Bay's ransomware claims frequency for the same period is 0.5%.

Active risk monitoring is the solution to these changing conditions: a combination of frequent scans to detect vulnerable portfolio businesses and an in-house security team to help businesses and their brokers resolve issues before attackers can exploit them. By employing active risk monitoring, the frequency of ransomware attacks in At-Bay's portfolio is seven times lower than the industry average.

Assessing portfolio security once a year misses 80% of RDP vulnerabilities

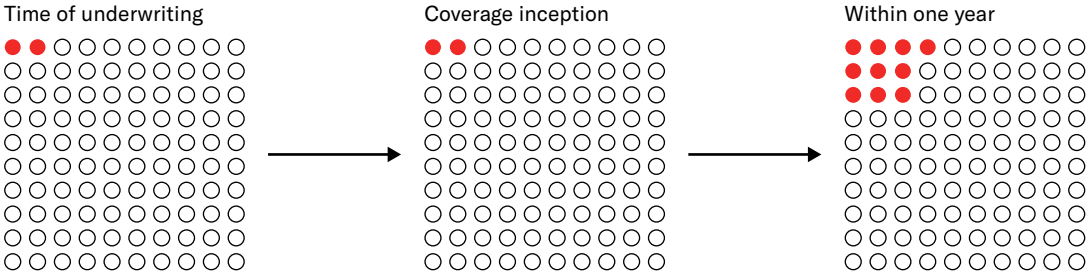
RDP compromise is the leading cause of ransomware incidents, responsible for nearly 50% of all attacks.[7] As a service that enables network access, RDP is widely used by remote users and administrators. Small and medium-sized businesses, in particular, are more often vulnerable to RDP risk due to reliance on third-party vendors who access their networks remotely and fail to close or secure the RDP port. In their basic configuration, RDP services are easy to exploit; when an RDP port is left open, it is like leaving the front door to your business open to anyone on the internet.

On average, we found that 2.0% of businesses have an open RDP port at the time of quoting a policy. Identifying these businesses and helping them remediate the issue as a contingency to providing insurance is an effective strategy that can have a positive effect on loss results, but a one-time perimeter scan addresses only 20% of potential RDP attacks.

2.0%

Businesses with an open RDP port at the time of underwriting

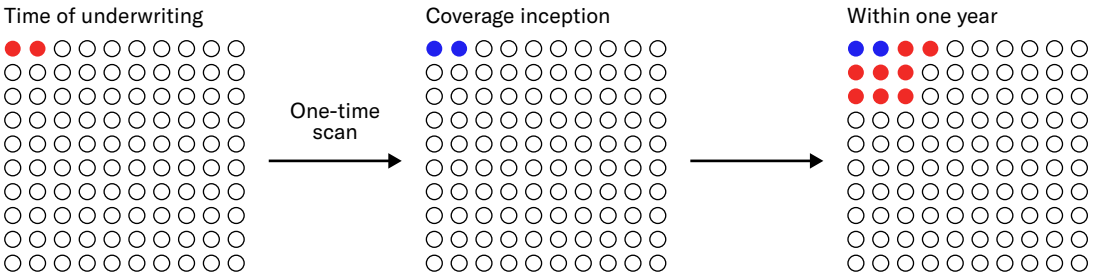
Exposure to RDP risk: Traditional underwriting



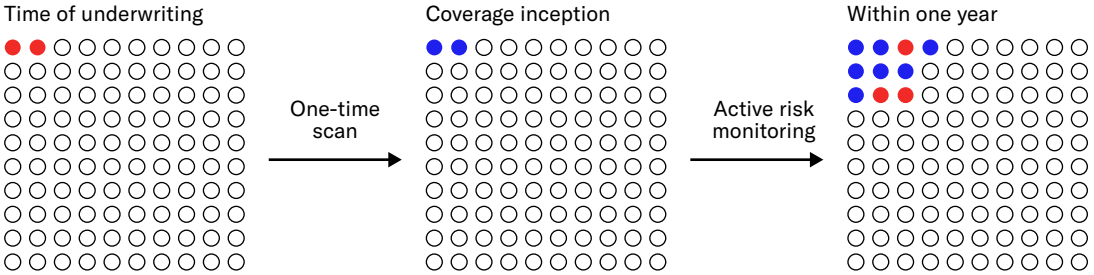
● Open RDP ports

In a portfolio of 100 SMBs, two will have an open RDP port at the time of underwriting. Without a one-time perimeter scan, the two RDP ports will remain open after the policy is bound and, cumulatively, another eight will open throughout the life of a one-year policy.

Exposure to RDP risk: One-time scan



Exposure to RDP risk: Active risk monitoring



● Open RDP ports ● Closed RDP ports

In a portfolio of 100 SMBs, two will have an open RDP port at the time of quoting. With a one-time perimeter scan, the two can be identified and closed before a policy binds. Cumulatively, another eight RDP ports will open throughout the life of a one-year policy, but active risk monitoring helps reduce the number to three.

By frequently scanning the network security of At-Bay's portfolio, we found that a total of 10.1% of businesses have an RDP port open for an extended period of time during the policy year, even if all RDP ports were closed at the time of coverage inception. The true portfolio exposure to RDP risk is thus five times greater than identified by a one-time scan at the time of underwriting. This is why active risk monitoring is the best way to mitigate RDP risk throughout the life of a policy.

This approach removes most, but not all, of the risk from At-Bay's portfolio. While we have been impressed by the cooperation of our insured businesses, some issues persist. Insureds are occasionally required to have an open RDP port due to technical issues associated with legacy systems. A very small number of insureds do not heed our recommendations, and we take this into consideration in future underwriting.

10.1%

Businesses with an open RDP port during the policy year

Active risk monitoring expedites software patching by 5x

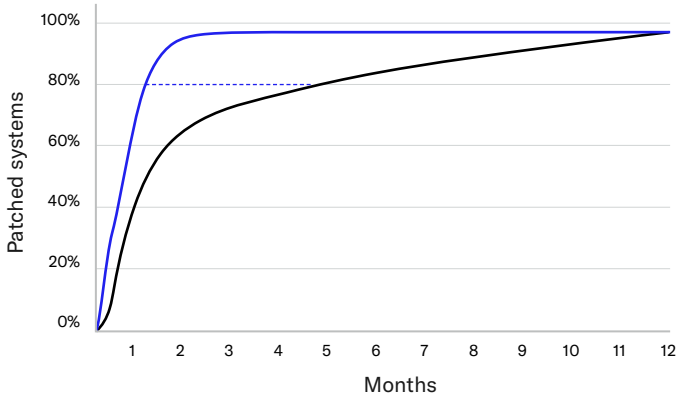
Software vulnerability is another major ransomware attack vector, accounting for nearly 20% of all ransomware incidents.[8] The key to avoiding the exploitation of software vulnerabilities is to quickly identify and patch the vulnerable software. While it may sound trivial, consistent and timely response to all critical patching alerts is often an insurmountable task for under-resourced or legacy-dependent businesses.

A scan can discover vulnerable software if it is running on a publicly facing server. A security team can then help the insured business understand how to fix the issue. However, because new software vulnerabilities emerge constantly, only active risk monitoring can address new issues as they emerge during a policy period.

The window of opportunity for an attacker starts when a new vulnerability is publicly disclosed and an exploit is published. The vulnerability ends when the business patches the software. Attackers work quickly. More than 67% of vulnerabilities have an exploit within one month of a patch being available.[9] Conversely, businesses are slow to react, and more than 20% of systems remain unpatched five months after a patch is available.

Active risk monitoring allows us to scan for new vulnerabilities as soon as they are publicly available and work with At-Bay insureds promptly to install patches. Together, we shrink the window of opportunity for an attacker by more than five times, achieving 80% remediation within one month, which dramatically decreases the exposure of At-Bay's portfolio.

Time to patch vulnerable software



5x faster

At-Bay insureds patching vulnerable software vs. other businesses

At-Bay insureds
Other businesses[9]

On average, businesses with vulnerable software take five months to reach 80% remediation once a patch is available. By comparison, At-Bay portfolio businesses achieve 80% remediation within one month.

Conclusion

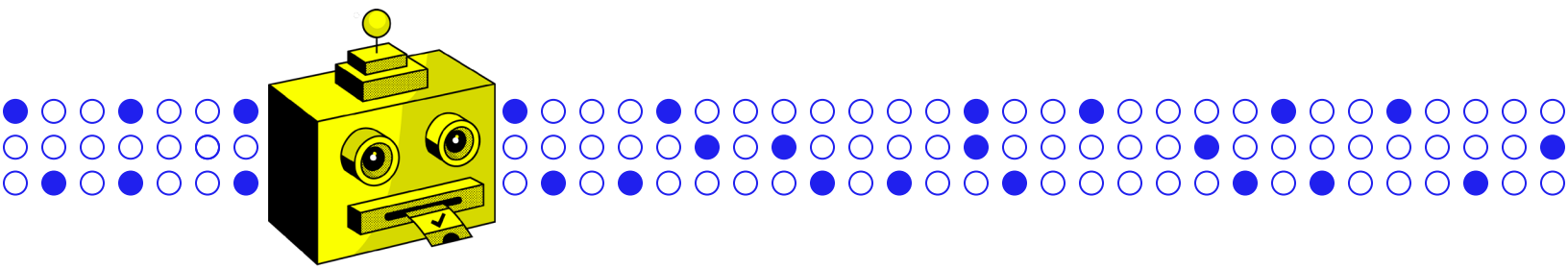
Ransomware is perhaps the most disruptive type of cyber attack today. Not only has it quickly risen to become the highest frequency attack method among insurance claims, but ransomware is also one of the more devastating attacks to a business, targeting both data and operations to extract maximum leverage.

As we have shown in this report, active risk monitoring can successfully curb the impact of ransomware in an insurance portfolio and enable insurers to continue providing broad coverage at affordable prices. At-Bay data shows that active risk monitoring uncovers the 80% of RDP risk in a portfolio that others miss, even with a one-time security scan, and shrinks the attack window of an attacker to exploit vulnerable software by five times. Together with strict technical analysis at the time of underwriting, our use of active risk monitoring reduces ransomware frequency in At-Bay's portfolio by more than seven times, compared to the market.

Active risk monitoring and technical analysis at the time of underwriting are two important features of At-Bay's operating system for digital risks. They are enabled and empowered by a scalable cloud technology stack that creates a single environment that allows for:

- Cyber security research and data acquisition teams to ensure that scans keep up with new and evolving threats
- Eligibility and pricing models that reflect technical insights that can be deployed in real time into underwriting systems
- Consistent classification of technical data at the time of underwriting and claims that can optimize learning
- Systems, processes, talent, and culture to enable rapid cycles, from discovery of new cyber threats to updating technical scans and deployment of new underwriting rules into field operations within days

In the modern economy, every business is a technology business. That means everyone is at risk of ransomware. With the right operating systems, insurance can empower every business, large or small, to manage risk and thrive in a digital world.



Appendix

Best practices for minimizing ransomware risk

Secure Email Gateways: Implement SEG software for all email providers other than Gmail. For businesses using Office365, we recommend Microsoft Defender with Advanced Threat Protection. For all other providers, SEG can be implemented with a security vendor.

Data Backups: Audit all locations to ensure no data is excluded from the backups. When creating data backups, follow the 3-2-1 Rule: Make 3 copies of the data, store the data across 2 different mediums, and keep 1 copy of the data offsite.

Multi-Factor Authentication: Implement MFA at all sensitive access points, including email, internal applications, remote network access, and external-facing systems. The most common and safest verification method is an authenticator application, which is recommended over text messages or phone calls.

Remote Desktop Protocol: If an open RDP port is required for business operations, hide it behind a secure gateway, such as a virtual private network, and enable network-level authentication.

Methodology

We conduct thorough, periodic scans of At-Bay portfolio businesses to track changes in our risk profile, including discovery of new assets, availability and versions of services on open ports, and other vulnerabilities and configuration issues. Our security team tracks the engagement of At-Bay portfolio businesses with our alerts, and ad-hoc technical scans confirm completion of required fixes to critical issues alerted by our team. Our claims team tracks and provides an appropriate technical classification for all types of cyber claims. We have compiled the information collected over the past 18 months to identify patterns in exposure to ransomware risk and measure the impact of our security services on those patterns, compared to established industry benchmarks referenced throughout this report. For more information on our research or methods, please contact us at **info@at-bay.com**.

Citations

[1, 6, 7, 8] Coveware Q1 2021: Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

[2] Sophos: The State of Ransomware 2021

[3] Fitch Ratings: U.S. Cyber Insurance Market Update (Spike in Claims Leads to Decline in 2020 Underwriting Performance)

[4] Marsh Global Insurance Market Index; At-Bay portfolio data

[5] At-Bay portfolio data

[9] Kenna Security: Prioritization to Prediction Volume 6: The Attacker-Defender Divide

at bay

Insurance for the digital age

at-bay.com

@KeepRisk_AtBay
info@at-bay.com