



# 2022 Cyber Claims Report

An in-depth analysis of cyber claims data from Coalition

2022

# Cyber Claims Report

An in-depth analysis of cyber claims data from Coalition

## Executive Summary

Technology is the most significant driving force of change in today's digital economy. Especially since the pandemic began, businesses have adapted to the changing nature of work and an economy powered by digital technology. Today, employees work from digital home offices, intelligent software is available to assist with everything from exercise to shipping, and business can thrive with nothing but a digital presence. The transformation of our world has allowed organizations and employees to weather the COVID-19 pandemic, but it has also accelerated a new type of risk: **digital risks**.

By the end of 2022, nearly 65% of the global GDP will be digitized — reliant on a digital system of some kind.<sup>1</sup> This shift to digital has made it possible to create, run and scale businesses faster and easier than ever before, but the shift to digital technology has also created a new class of digital risks that are constantly evolving and strike faster and often with more

severity than traditional risks. The events of the past two years have made this shift clear: from ransomware attacks to the challenges of managing distributed workforces during the pandemic, **digital risk is different**.

While traditional insurance has served mainly as a hedge against loss only after an incident, insurance designed for the digital economy needs to be **active** — providing value before, during, and after an incident that could lead to a loss. Coalition is the world's first Active Insurance company, providing a new model for risk management in the digital age.

Coalition, together with the broader cyber insurance industry, is well-positioned to fight cybercrime and help organizations to embrace ongoing technological progress. We have unique insight into the digital risks that result in claims for our policyholders and our incentives are aligned with our customers to actively prevent claims. On any given day Coalition performs billions of security scans, sends hundreds of



critical security alerts, investigates reported cyber incidents, and helps our over 140,000 customers navigate an increasingly fast-paced digital world. In that spirit, we share this report to help all organizations solve digital risk.

The following report provides a detailed look into the incidents that led to claims from our policyholders over the second half of 2021. In addition to the data, we share a thoughtful analysis of the current trends and predictions for 2022.

Analysis of our claims data through the second half of 2021 reveals a number of evolving trends:

**1. Ransom demands continue to increase, though claims severity has started to plateau.**

The ransomware business model has begun to mature, though attackers are showing no signs of slowing down. The average ransom demand made against our policyholders increased 20% in the latter half of 2021 and the claims severity increased 10%.

**2. The frequency of other attack techniques also rose as hackers expanded to new tactics.**

This heralds an era of omnidirectional threat-equality — cyber threats are ever-present from all angles. While ransomware may be the most newsworthy, no attack vector can be trivialized or ignored.

**3. Small businesses are disproportionately impacted.**

As attacks become increasingly automated, it has become easier and more profitable for criminals to target small organizations. Overall claims severity rose 56% for small organizations under \$25M in revenue. We also saw a dramatic increase in claims frequency, with a 40% increase in ransomware attacks and 54% increase in funds transfer fraud attacks.

**4. Active Insurance works.** We've processed more claims across more organizations in the past year than in any other period, and there wasn't a single organization that we weren't able to help successfully recover. **Through our active protection and response capabilities, we were able to solve 46% of reported incidents at no cost to the policyholder.**

We've also helped thousands of companies improve their baseline cybersecurity hygiene, including our own policyholders who continue to experience less than one-third the frequency of claims as the broader cyber insurance market.





While many things have changed since our last report, there was one constant: organizations continue to be targeted by criminals because they have made poor technology choices, often exposed to the public internet, that make them vulnerable. It's more important than ever that companies take the time to understand their cyber risk, and it's never been easier with new tools like [Coalition Control](#).

**Before we dive into the data, a few quick caveats:**

- The sample size of reported incidents and claims is limited in strict statistical terms; we'll continue to regularly update and share our analysis to identify changing trends.
- Our underwriting and risk engineering capabilities are unique among cyber insurance providers, and our claims frequency reflects this. As a result, we may see different types of claims than others.
- Recently reported claims will continue to develop and mature. The report contains our current loss estimates, but these may fluctuate in overall severity in the coming months.
- This report contains predictions from our team of in-house experts. These are our opinions based on current market conditions and proprietary data. In most cases, we hope we are wrong (if only for the sake of our customers).
- This isn't an exhaustive review of the data we collect. If you have any questions, please reach out to us. In the spirit of our mission to solve cyber risk, we'll share what we can.

Organizations continue to be targeted by criminals because they have made poor technology choices.



# table of contents

2 **Executive Summary**

6 **Key Findings**

9 **Ransomware:**  
The cyber epidemic that's made hacking into a lucrative business

14 **Funds Transfer Fraud:**  
The low-tech attack that disproportionately target small businesses

17 **Emerging Attack Techniques:**  
Tactics and techniques threat actors used to execute cyber crime

22 **Predictions for 2022**

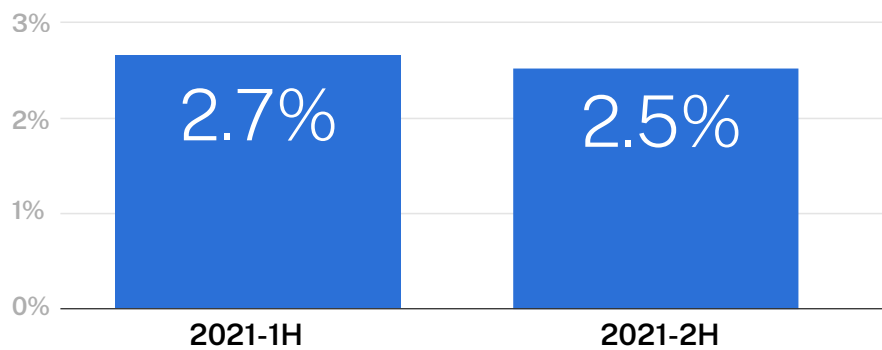
24 **Active Insurance:**  
How Coalition continuously combats digital risk



# 01 Key Findings

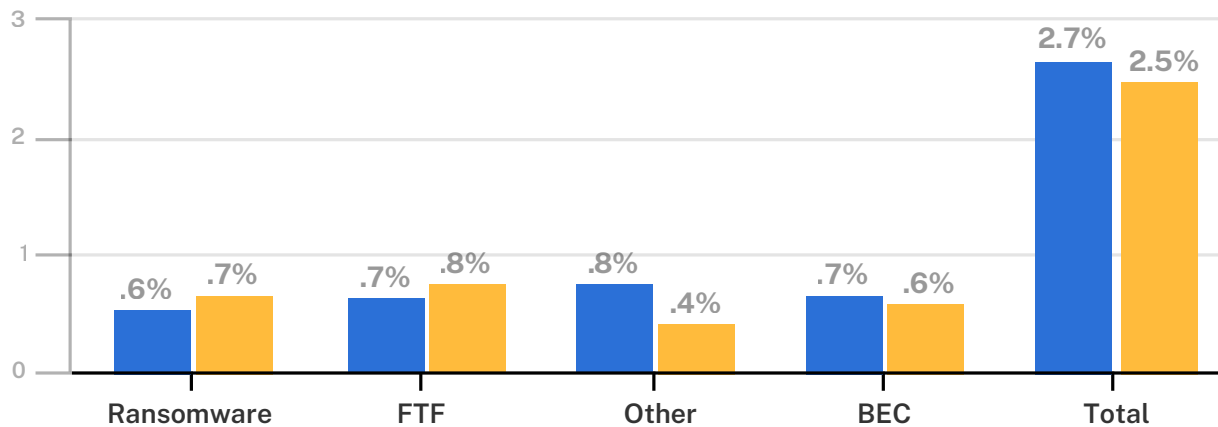
The impacts of the past two years — from the rapid transition to remote work and new technologies to evolving digital threats — continue to transform all facets of life and business. The COVID-19 pandemic continued to disrupt daily routines, companies large and small continued to support hybrid work models, and cybersecurity incidents shook many industries. The scale and frequency of these incidents led 2021 to be the year that cybersecurity issues entered the mainstream discussion, with President Biden convening a session on the importance of protecting America’s business interests in the face of a growing wave of cyber attacks, which Coalition was invited to attend.

Overall claims frequency



Claims frequency includes events that may fall below the policy retention.

2021 claims frequency by event type



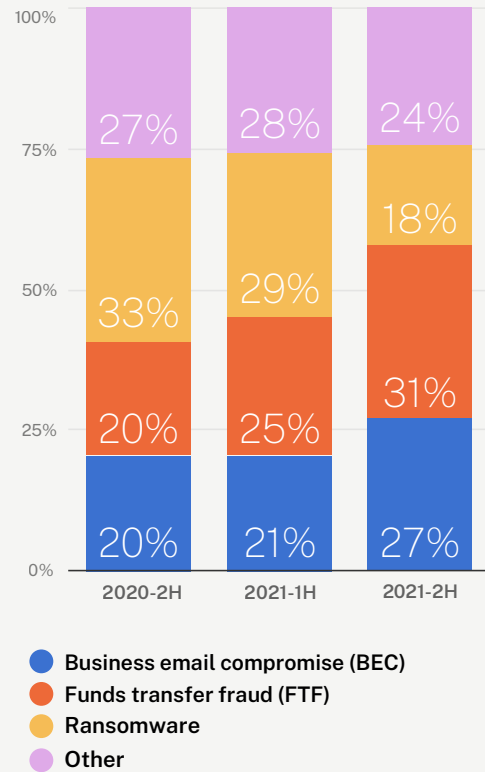


It seemed as though the onslaught would never end – starting with highprofile cyber events such as Colonial Pipeline, Kaseya, and then Log4j in the latter half of the year. As a result, we saw a substantial increase in claims during the first half of 2021, with frequency rising 31% from the second half of 2020. Claims frequency stabilized over the course of 2021, with frequency decreasing 7% from H1 2021 to H2 2021.

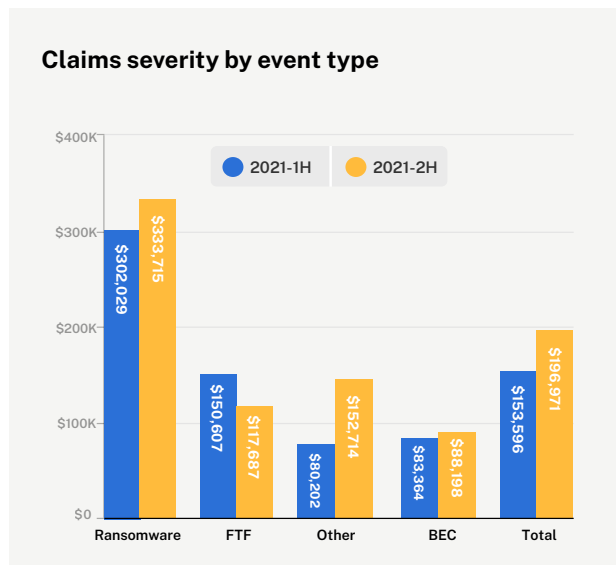
The surge in cyber crime also impacted claims severity, which we define as the average cost of a cyber claim. Overall claims severity increased 28% to an average loss of \$197,000 across all of our policyholders. Claims severity in Canada increased over 4x from 2020 to the first half of 2021, only to decrease 20% during the second half of the year.

Historically, small and midsize businesses seemed to be off the radar of cyber criminals, but that has unquestionably changed in the past few years. While cyber incidents can be equally devastating to businesses of any size, we’ve seen a material uptick in claims targeting small and midsize businesses.

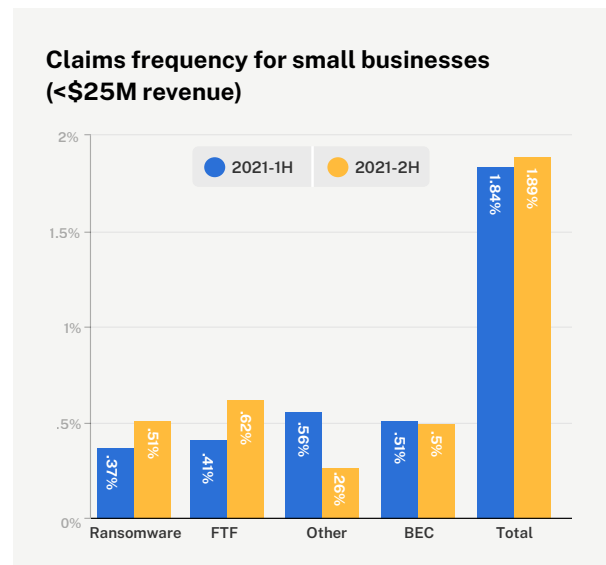
Percentage of reported claims by event type



Claims severity by event type

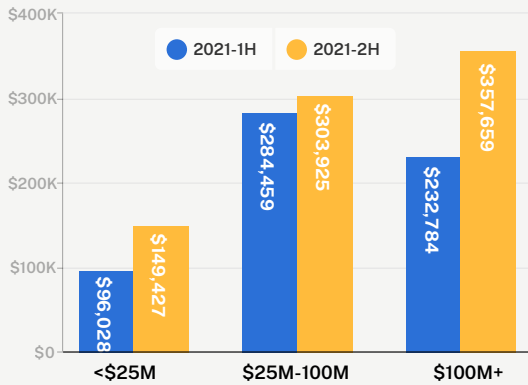


Claims frequency for small businesses (<\$25M revenue)





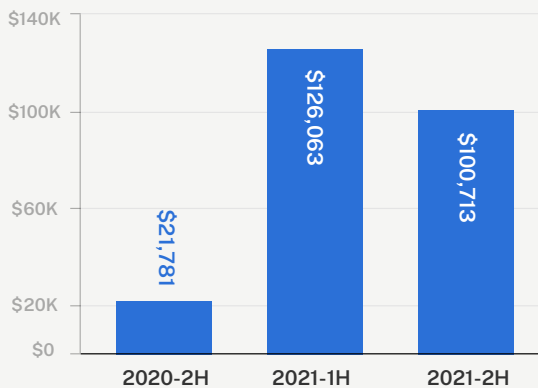
### Claims severity by revenue band - US



Small businesses with under \$25M in revenue were particularly vulnerable in 2021. We saw a 56% increase in the average claim cost, increasing to \$149,000 by the end of 2021. We also observed dramatic increases in the frequency of attacks; small businesses also saw a 40% increase in ransomware attacks and a 54% increase in funds transfer fraud incidents. Small businesses are especially vulnerable to threat actors as they often lack the resources to respond quickly.

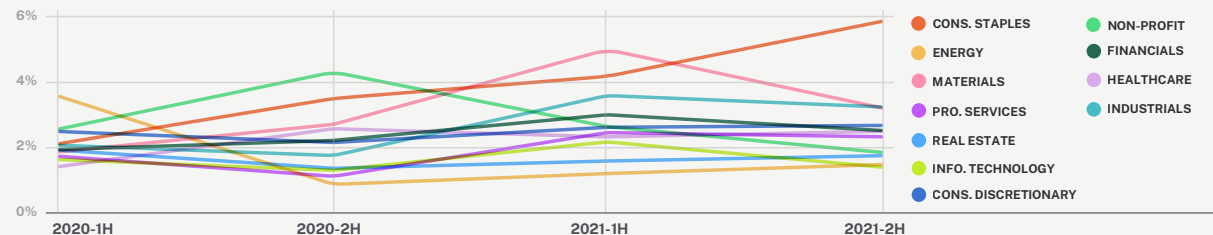
Middle market businesses with \$100M in revenue or more also saw a material increase. Claims severity increased 54% to a whopping \$358,000 from H1 to H2 2021. While claims frequency fluctuated for this segment, it remained consistently 2-3x higher than the claims frequency for small businesses.

### Claims severity - Canada



**Cyber criminals are opportunistic, particularly when it comes to small and midsize organizations, and the technology and processes that organizations use are far more key to their risk than what their industry is.** No company is too small to be an enticing financial opportunity for attackers. Still, some industries did experience notable increases in claims in the past year. From H1 2021 through H2 2021, we saw a 40% increase in claims severity for consumer staples businesses and 23% increase for energy businesses.

### Claims frequency by event type







## 02 Ransomware:

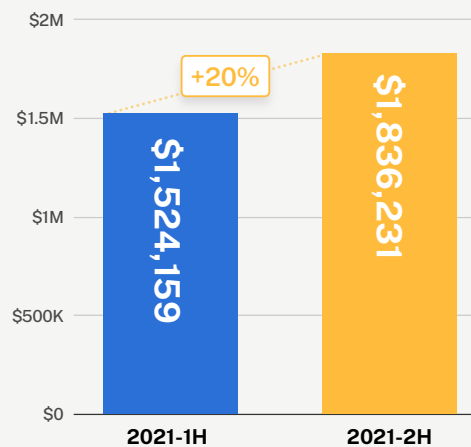
### The cyber epidemic that's made hacking into a lucrative business

Ransomware has reshaped the way we view cyber risk. Over the last two years, ransomware attacks have made headlines frequently, impacting everything from critical infrastructure to healthcare and small businesses. It has become clear that all organizations are vulnerable to this persistent digital risk.

Throughout 2021, ransomware demands and frequency continued to increase, while claims severity has started to plateau. Coalition policyholders experienced a 20% increase in ransomware demands to an average of \$1.8 million — a cost that remains untenable to pay for many organizations. We also observed a 23% percent increase in ransomware claims frequency in the second half of 2021, to 0.67% of all policyholders.

Ransomware claims severity also continued to increase, albeit moderately, rising 10% from the first half of 2021. We anticipate that the severity of ransomware will continue to flatten over time. As we predicted in our previous Claims Report, there is little leverage threat actors can gain beyond what they already have once they have taken an organization's operations and data hostage.

**Average ransom demand made against Coalition policyholders**



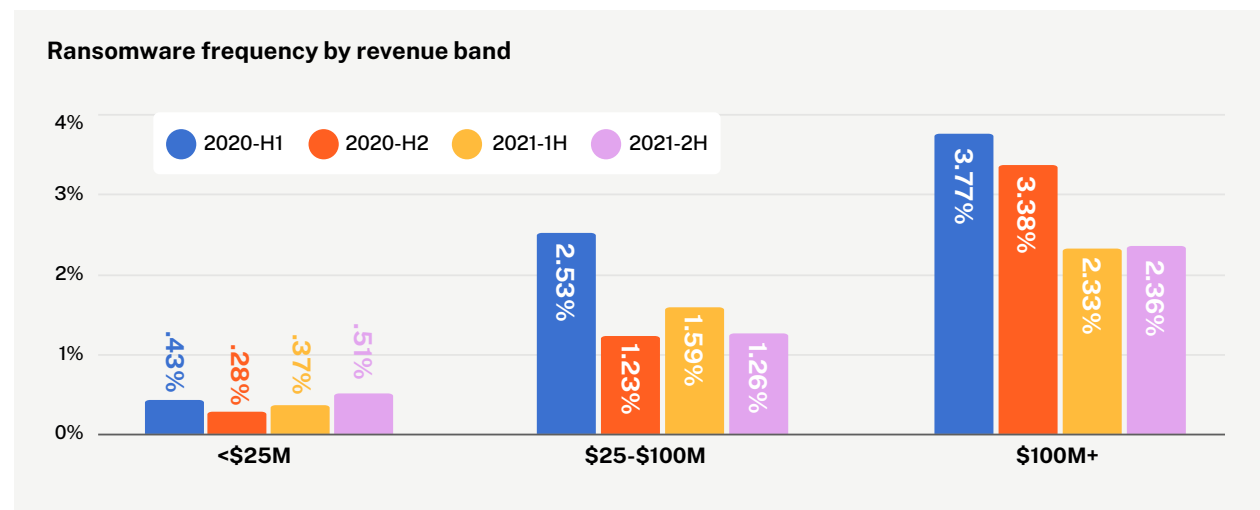
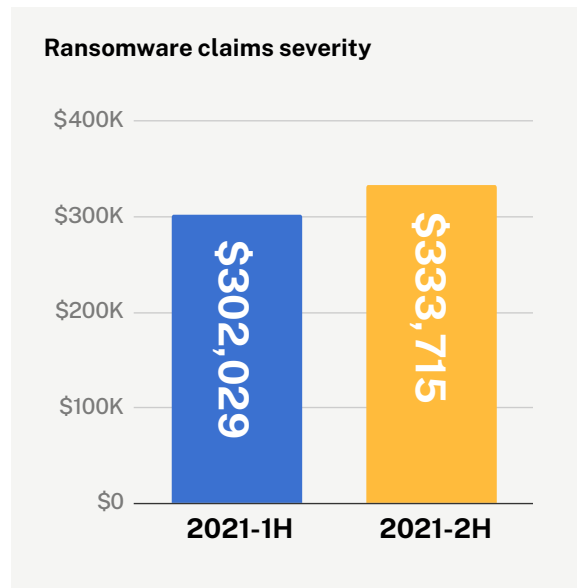
Ransom demands continue to increase, while claims severity has started to plateau.



Deciding whether or not to pay a threat actor’s ransom demand is only further complicated by the fact that many threat actors require payment via cryptocurrency. Additionally, the federal government began to implement tighter regulations on ransomware payments. In September of 2021, The U.S. Department of Treasury’s Office of Foreign Asset Control (OFAC) issued an [Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments](#), highlighting potential sanctions risks associated with making ransom/extortion payments in response to a ransomware event.

Coalition policyholders have access to our active risk monitoring, which provides them with alerts about potential vulnerabilities and access to security methods that help remediate and reduce their risk of a cyber incident. Additionally, our in-house Coalition Incident Response and Claims teams are available 24/7 to quickly react to potential incidents. While ransomware events are notoriously complex, our team has successfully remediated incidents and, when possible, restored business operations through backups. **As a result, we saw a 16% decrease in ransomware payments in the second half of 2021.**

Not all industries have been impacted equally by the ransomware epidemic, and healthcare organizations suffered an epidemic of ransomware attacks. Threat actors capitalized on the frantic nature of the continued COVID-19 pandemic to attack a vulnerable industry that was focused on providing critical patient care. Over the first half of 2021, the claims frequency for healthcare increased 67% and increased another 20% in the second half of the year.





**CASE STUDY**

## Healthcare provider pays ransom to protect patient data

- **Industry:** Healthcare
- **Revenue:** \$45M
- **Employees:** 251-1,000
- **Coverages**
  - Cyber Extortion
  - Breach Response

A healthcare provider serving an underserved community was hit with ransomware that encrypted most of their network and some endpoints. The insured quickly reached out to Coalition, and we helped connect them with a forensic team to assess their backups and counsel. Thankfully, the backups were viable, and the remediation team restored their systems to the point before the encryption event. Additionally, the team helped the insured create disk images for investigations. It seemed like an open and shut case with no reason to pay the ransom.

Healthcare providers maintain — and are required to protect — sensitive patient data. Under HIPAA, sensitive data includes diagnoses, treatment information, medical test results, and prescription information. In today’s day and age, this also includes COVID-19 vaccination status. While we typically discourage the payment of extortion demands to prevent disclosure, there are unique circumstances where payment may be reasonable. In this case, the threat actor extracted or compromised patient files, and the healthcare provider was concerned that a release of the information could cause harm to the community and the patients.

As a result, the policyholder requested Coalition process payment to the threat actor. Additionally, as with any investigation, we brought on counsel to review the impacted files and help the healthcare provider notify the affected patients.

# The average ransom demand increased 20% to \$1.8M.



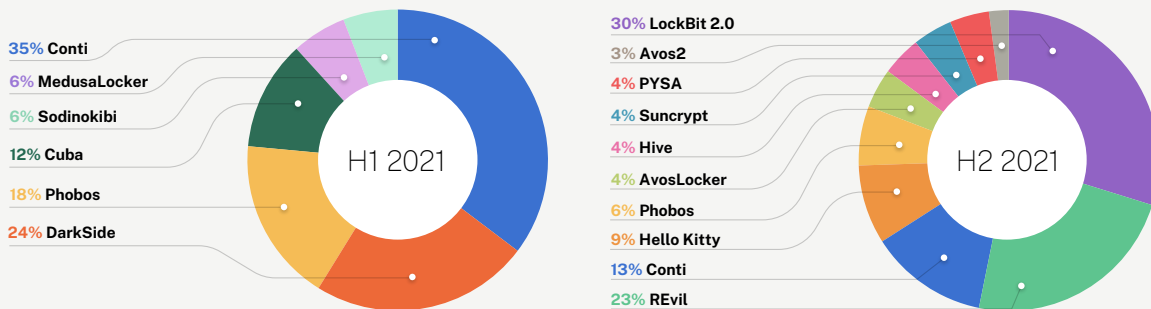
## Top ransomware variants

In 2021, we saw ransomware evolve from an emerging attack vector to a viable criminal business model. Threat actors benefit by taking hostage of their victim’s data, infrastructure, economic output, intellectual property, or even privacy. After exhausting all possible options to restore operations, organizations may feel compelled to pay cyber extortion fees and begin the recovery process. Ransomware-as-a-Service (RaaS) is a business model that leases variants out to threat actors; RaaS kits may include support, bundled offers, reviews, and access to forums. However, threat actors may not feel brand loyalty toward ransomware gangs

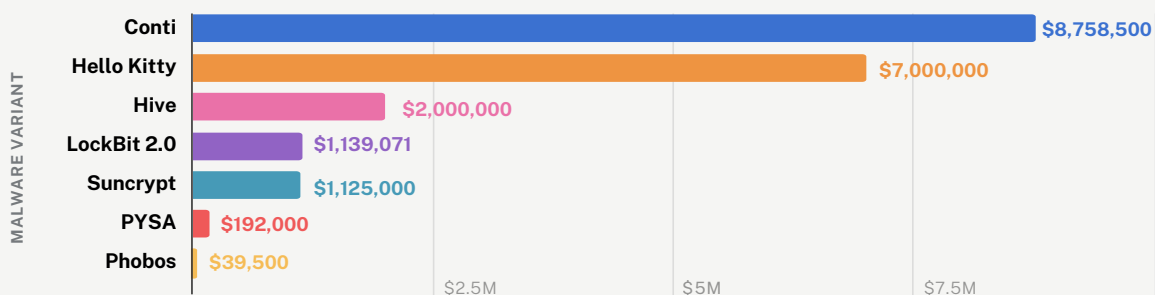
and instead are likely to align themselves with whatever variant is accessible and inflict the most damage.

In the first half of 2021, we observed an explosion of new and invasive ransomware variants. Surprisingly, the second half of the year saw a near-complete shift: only Conti ransomware was consistently seen among our top ransomware variants. Seeing a wide shift in ransomware variants across the same year points to the opportunistic nature of cyber criminals – just as they target organizations irrespective of size and industry, they will utilize whatever ransomware variants are accessible, easy-to-use, and successful.

Top ransomware variants by number reported



Average ransom demand in H2 2021



Note: ransom demand not reportable for all variants.

**CASE STUDY**

## Tips for ransomware recovery and prevention

Recovering from a ransomware attack can be a long process for any organization — even those that have good backups and cyber insurance. To prevent future incidents, organizations should utilize a combination of security tools and best practices.

### 1. Maintain good backups

A good data backup can mean the difference between a full loss and a full recovery after a ransomware attack. Develop a regular schedule to backup critical and non-critical business data and test backups to ensure they are viable. We recommend maintaining copies of your data, with two different backup formats, and one backup stored offsite (AKA 3-2-1 rule) to store essential data completely separate from the primary network. Often, onsite backups use the same credentials as the rest of the network and there are ransomware variants that will delete or encrypt backups.

### 2. Keep servers updated/patched

Keeping servers up to date as soon as security patches are released can make the difference between a minor inconvenience, and a full blown

ransomware incident. Threat actors scan for, and exploit servers which have not been updated following the release of major security vulnerabilities such as ProxyLogon, and Log4j. A company that keeps all servers updated is much less likely to experience ransomware, as an unpatched server can become patient zero.

### 3. Implement strong passwords and multi-factor authentication (MFA)

We recommend organizations [adopt strong password guidelines](#).

Additionally, a combination of multifactor authentication (MFA) and strong passwords can help mitigate a threat actor's success rate at stealing user credentials.

### 4. Disable Remote Desktop Protocol (RDP) and implement zero trust protocols

Remote access points (especially Remote Desktop Protocol or RDP) are one of the most common methods for ransomware gangs to infiltrate your network. Many organizations turned to RDP to support remote or hybrid work models, but they also can serve as an easy entry point for threat actors if not properly configured and secured. To safely offer remote access, we recommend implementing a virtual private network (VPN).



# 03

## Funds Transfer Fraud:

The low-tech attack that disproportionately target small businesses

Cyber criminals are opportunistic, often opting to target businesses based on technology and processes rather than industry. One of the easier methods to monetize cyber crime is funds transfer fraud (FTF), which is often perpetuated through social engineering techniques like phishing or business email compromise (BEC). Once a threat actor has access to your business mailbox, they can manipulate your contacts and modify payment instructions, sometimes without even triggering any security alerts. Threat actors can also send you a change in payment instructions that purports to come from a customer or vendor via a lookalike email domain or by compromising the customer or vendor's email system.

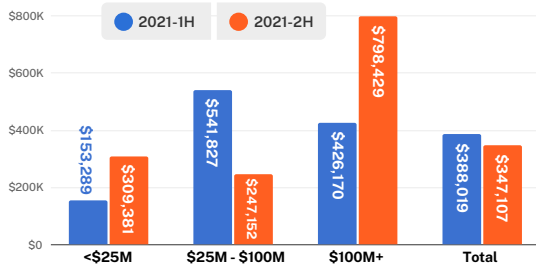
Funds transfer fraud skyrocketed in the first half of 2021. The initial FTF loss, defined as the loss before we were able to recover funds, surged to an average of \$388,000 before accounting for recovered funds. Over the second half of the year, the average initial loss decreased by 11% to \$347,000. While a small decline may initially appear optimistic, this is still a 78% increase in initial losses from 2020.

Furthermore, we observed some organizations were disproportionately impacted. For small organizations with less than \$25 million in revenue, the initial FTF loss increased by 102% in the second half of 2021. The frequency of these attacks also increased dramatically for small businesses under \$25M in revenue, rising 54% from H1 2021. Organizations of this size are likely especially vulnerable to funds transfer fraud attacks. They often have a smaller digital footprint than larger organizations, leaving threat actors with fewer options to pivot inside a network and less infrastructure and data to hold hostage in a ransomware attack.

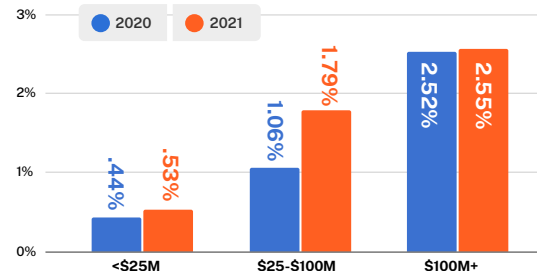
**From 2020 to 2021, overall FTF losses increased by 69%. The frequency rose by 21% for organizations with under \$25M in revenue and 68% for organizations with \$25M-\$100M in revenue.**



### Initial funds transfer loss before recoveries - by revenue band



### Funds Transfer Fraud frequency by revenue band



#### CASE STUDY

## Funds transfer fraud coverage remediates double claim

- **Industry:** Manufacturing and Staffing
- **Revenue:** \$2.6M
- **Employees:** 26-50
- **Coverages**
  - Funds Transfer Fraud
  - Breach Response

In early October, a manufacturing company received an invoice from their staffing firm. The accounts payable department transferred the \$207,000 payment, sensing nothing out of the ordinary, only to be surprised when the staffing firm reached out to check on the status of their late payment. Realizing they had sent a fraudulent payment, the manufacturing company reached out to Coalition. When our Claims team responded to the incident, they knew a funds transfer fraud incident had taken place. Because attempting to clawback funds is a time sensitive process, we immediately filed an IC3 report with the FBI and put in an interbank agreement to freeze the funds.

Digital investigations revealed no signs of a threat actor in the manufacturing company’s network, leading Coalition Incident Response (CIR) to suspect the staffing firm was the source of the compromise. As it turned out, the staffing firm had been compromised by a business email compromise (BEC). The attacker then changed the banking information in their payment invoices. Unexpectedly, both the manufacturing company and the staffing firm were Coalition policyholders.

CIR worked to remove the threat actor from the staffing firm’s network and ensure no sensitive data was compromised. Additionally, we were also successful in clawing back all \$207,000 for the manufacturing company, thereby successfully remediating both incidents.



## Recovering from funds transfer fraud — speed is essential

Funds transfer fraud losses can be devastating for any business, but there are steps your organization can take in the event of a fraudulent transfer. We recommend policyholders take immediate action to maximize their chances of recovery.

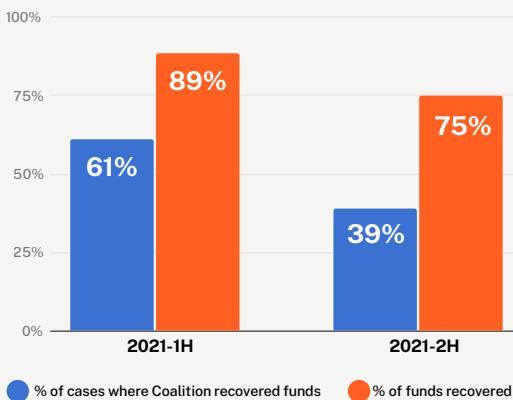
1. Notify Coalition’s claims team of the loss as soon as possible, ideally within 72 hours of the transfer.
2. Immediately notify your bank of the fraudulent transfer, and request a clawback of the funds.
3. File a report with the FBI at IC3.gov.
4. File a report with your local police department.
5. Repeatedly inquire with your bank and the receiving bank on the status of the recovery.
6. Additionally, we recommend implementing multi-factor authentication (MFA) to reduce the risk of a BEC attack and a cybersecurity education program to enable employees

to recognize and report potential email compromise attacks.

While ransomware spent much of 2021 in the limelight, FTF cases continue to rise like never before. Time is of the essence with FTF cases, and we encourage our policyholders to reach out as soon as they notice an incorrect payment as we are more likely to recover funds within 48-72 hours of the transfer. In the latter half of the year, many organizations were slower to report losses, which unfortunately makes it less likely that we can recover the funds.

We saw a decrease in the percentage of cases where we were able to recover funds, from 61% in H1 2021 to 39% in H2 2021. We recovered 75% of the FTF losses in H2 2021 cases, where our claims and incident response teams managed to claw back funds. This is a slight decrease from earlier in the year when we recovered 89% of funds in cases with successful clawbacks. We attribute this difference to threat actors covering up losses better by diverting emails, making it challenging for policyholders to realize an improper payment has taken place for up to weeks.

**Funds Transfer Fraud recovery**



### How to combat FTF

The primary defense against funds transfer fraud is a defined process for how your organization processes new requests and change payment requests. The procedures should include calling the requesting party on a known good number to confirm the demand — never use the contact information provided in an email as these are often manipulated via phishing. These verification procedures should also have a defined, two-party approval process for transfers and required reviews for payment change details.





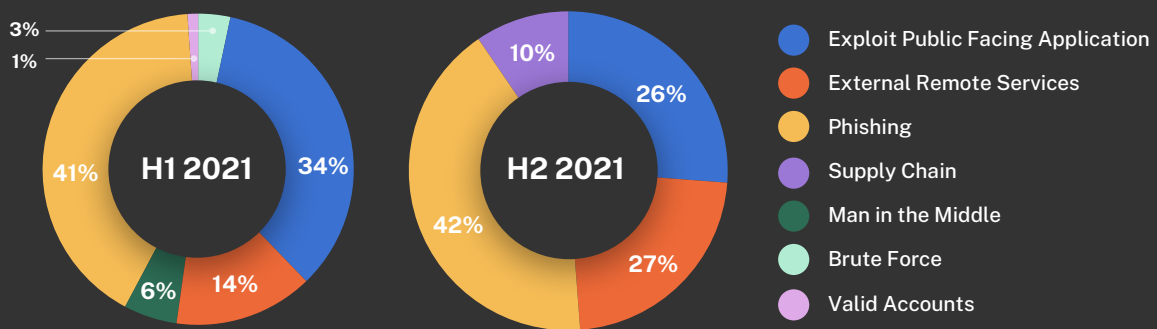
# 04 Emerging attack techniques:

## Tactics and techniques threat actors used to execute cyber crime

Over the last two years, the COVID-19 pandemic fueled a fast transition to remote work to remote work, and organizations found themselves reliant on insecure technologies to facilitate this change. As a result, we previously observed that remote access tools such as remote desktop protocol (RDP) led to an explosion in ransomware and funds transfer fraud cases. Over time, these tactics have become the main ways that immediately monetize cyber crime.

Threat actors use a wide array of attack tactics and techniques to gain access to systems, and while some are less newsworthy, they are no less dangerous to organizations and the data they protect. We examined the common attack techniques that were used against our policyholders, and found that while cyber criminals continue to expand their techniques, phishing and social engineering remains the most common tactic. Here is how criminals executed cyber crime in the past year.

Percentage of reported claims by attack technique



Note: attack vector data is not known in all cases. These charts reflect attack vectors for reported claims where the attack vector was known. Vectors are categorized according to the MITRE ATT&CK taxonomy of adversary tactics and techniques



### **Phishing**

A popular technique used to target victims, phishing attacks can also precipitate other types of cyber crime. Once an attacker is inside your email inbox, they have access to a treasure trove of sensitive business information they can use to phish others in your organization, redirect funds, or deploy ransomware. In H1 2021, email phishing was the initial vector of attack for 41% of reported claims where this data was available.

### **Stolen credentials from valid accounts**

Attackers can also gain access to a system by exploiting a username and password, either by brute force, a type of trial and error hack, or credential stuffing where they utilize login data that has previously been exposed in data breaches.

### **Brute force**

When all else fails, attackers can brute force their way into networks by guessing passwords by exhausting all possible combinations or using dictionaries of common passwords and their variations. This attack technique occasionally does work if employees are using extremely weak passwords or leaked passwords, though it can be easily defeated by multifactor authentication. This can be especially risky when the weak password is used on a risky remote access technology, such as RDP.

### **Exploiting public-facing applications**

Adversaries are constantly scanning the internet for vulnerable, external-facing applications. These can be VPNs, firewall devices, web servers, and more. When a server becomes vulnerable, it can be exploited easily by an adversary if it is publicly-facing. After exploitation, adversaries will try to move laterally to deploy ransomware. Coalition's Active Risk Platform scans for these external-facing applications and notifies policyholders a vulnerability is identified.

### **External remote applications**

While remote access helps organizations stay connected through remote work, it can also create an open door for attackers to target. Employees using weak or reused passwords to connect to remote access technologies pose a risk to the security of their organizations. Attackers will abuse these accounts to connect to the network and attempt to exfiltrate data or deploy ransomware. It's important to enforce MFA and VPN, keep remote access technologies updated, ensure they're properly configured, and limit administrator logins.

### **Man-in-the-middle attacks**

These attacks allow threat actors or adversaries to position themselves between your device and the connection to your organization's network. Once you attempt to connect, they can steal your credentials and gain network access. Internet-facing applications are accessible via the public internet and provide a service to the public or allow access to an internal network. Threat actors exploit these applications to gain access to a network and launch other attacks.

## **Aggregate digital risks: your vendor's attack perimeter becomes your attack perimeter**

Traditionally, the digital perimeter of a company, which protected business information, employee information, and customer information, was a straightforward castle and moat model. The physical office, or castle, was protected by a moat, or traditional firewall and VPN solutions.

The transition to a hybrid work culture upended that model. Organizations must now protect their critical business data from attacks against



their own digital perimeter and that of their vendors and employees. Most businesses partner with several third-party vendors — it is simply the cost of doing business in a fastpaced world. Examples of vendors include IT service providers, online software, cloud computing providers, or third-party services that are part of your network infrastructure.

In the first half of 2021, we observed several high-profile attacks against vendors: Mimecast, Kaseya, and Microsoft Exchange, to name a few. These attacks are sometimes referred to as supply chain attacks; however, that is an oversimplification. Often organizations directly partner with these vendors to provide IT functions such as email, firewalls, VPN access, and more. Cyber criminals attack vendors and, through successful compromises in the vendor’s digital perimeter, can victimize a large number of connected organizations at once, rather than just one. At the time, we correctly predicted that the increased reliance on vendors would mean organizations would continue to struggle to control such risks, and new attacks would continue to surface.

## Microsoft Exchange: the vulnerability that continues to evolve

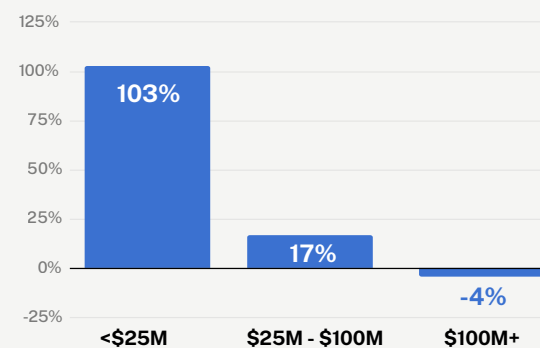
In March 2021, Microsoft announced it had detected multiple exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. The exploit, which would later come to be known as ProxyLogon and ProxyShell, utilized a zero-day attack against vulnerabilities in Exchange Server. Several patches were released in 2021 as threat actors found additional ways to exploit Exchange. They later leveraged the ProxyShell vulnerability which allowed threat actors to take control of an

on-premises Exchange server and access email accounts or install malware, which could be used for other, long-term attack activities.

During the initial set of Exchange vulnerabilities, roughly 1,000 Coalition policyholders were exposed to the Microsoft Exchange vulnerability. Coalition’s in-house CIR and Security teams acted quickly, and **we were able to notify and remediate the vulnerability for 98% of our impacted policyholders within a week** of the disclosure.

In August of 2021, another vulnerability related to Exchange was discovered by a security researcher. At this time, we released a dedicated scanning module to handle Exchange events. Using our Active Risk Platform, we scan and notify our policyholders if they have exposed Exchange vulnerabilities. The personalized notifications enable our policyholders to actively address and mitigate digital risk.

**Increase in claims for organizations using Microsoft Exchange**



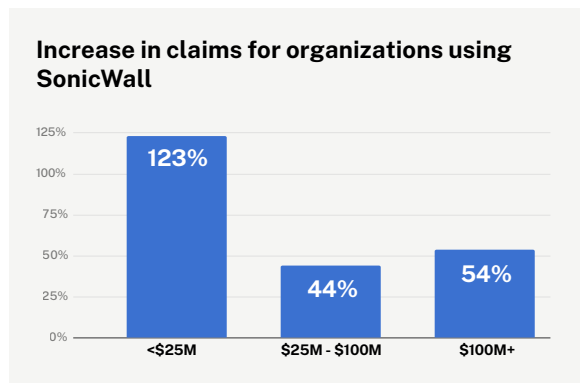
Small organizations under \$25 million in revenue that use Microsoft Exchange had a 103% increase in claims relative to organizations that don’t use the tool — a staggering increase given how widely it’s used amongst small and midsize organizations.



Given the complicated nature of the entire Exchange ecosystem, we expect to continue to see vulnerabilities discovered as attackers go after the broad range of capabilities and sensitive data it stores. We will continue to adapt our tooling to actively scan and alert our policyholders.

### SonicWall: remote access tools remain insecure

In the second half of 2021, SonicWall announced that their Secure Mobile Access (SMA) VPN appliance was impacted by a series of vulnerabilities that could allow a threat actor to take control of an affected system. SMA is a tool that many organizations use to provide their employees with remote access to internal resources.



In H1 2021, we observed that many organizations were relying on remote access utilities to facilitate remote work. However, tools such as Microsoft Remote Desktop (RDP) and SonicWall have become targets of cyber criminals as the same tools that make it easier for employees to access company resources make it easier for hackers to target and access the same information.

There was a staggering increase in claims frequency among Coalition policyholders utilizing SonicWall to facilitate remote access. Overall,

we saw a 123% increase in claims frequency and a significant impact on losses amongst small businesses. Due to the relatively recent nature of this vulnerability, and the fact that many organizations are still supporting hybrid work models that necessitate remote access, we anticipate seeing the frequency of SonicWall claims to continue to rise into 2022.

### Log4j: introducing a new threat

In November of 2021, security researchers discovered a new critical vulnerability in Log4j, a Java-based software library that puts program data into logs. Log4j is built into many programs and platforms, such as the HR system Chronos or the popular virtualization platform VMware. As a result of how many platforms utilize Log4j, this vulnerability impacts countless organizations that are likely unaware they are even at risk. Attackers use remote code execution to target systems with a vulnerable library. From there, they can pivot to other parts of the system and launch other, more deadly attacks.

Coalition had a responsibility to scan our policyholders and identify who was at risk. We examined our policyholders externally — just like a hacker would — and determined a minimal number were vulnerable. At the end of 2021, we have not seen any cases directly related to the Log4j vulnerability. However, we anticipate this number will change over time as attackers find new ways to exploit vulnerable libraries.

### Coalition's success against these digital threats

Our H1 2021 claims report revealed that our policyholders experienced 70% fewer claims than the industry average (compared to the latest



available National Association of Insurance Commissioners (NAIC) data at the time of this report).<sup>2</sup> This is thanks to our active protection capabilities that work to detect, monitor, and alert policyholders to fast-moving digital risks.

We use a data-driven approach to help our policyholders understand their risk profile and provide active protection to identify and mitigate risk before it strikes. Active Protection is one key aspect of Coalition's unique methodology to continuously monitor, prevent, and resolve cyber incidents — a solution we call: Active Insurance. (See our section on "Active Insurance" on page 24.)

To provide this protection, Coalition develops and deploys custom scanning technology to actively identify vulnerabilities that have the potential to impact our policyholders. In the example of the previously described Microsoft Exchange (ProxyLogon) vulnerabilities, we built a dedicated scanning module to handle Exchange events in the future. This proactive effort kept our insureds safe when a new Exchange vulnerability (ProxyShell) was disclosed and exploited in August of 2021. More recently, we deployed a similar approach to protect against the Log4j flaw and will continue to refine our scanning and alerting process as threat actors test new methods to exploit this vulnerability.

In the case of malware, we use a wide array of threat intelligence data to determine if an organization has previously been compromised. In 2021, when our data indicated malware infections were present on a policyholder's network, they were 135% more likely to experience a claim. The correlation is more acute when malware is present for a longer period of time where the threat actor can gather more information. As a result, policyholders with malware infection present in their networks for over seven days were 195% more likely to

experience a claim. Ransomware is also malware. Banking trojans and exploit frameworks are precursors to ransomware. When we identified precursor malware infections in a network, we found a policyholder was 229% more likely to experience a ransomware claim.

46%

Percentage of incidents that Coalition's Claims and Incident Response team fully contained (with \$0 cost to the policyholder and zero erosion of the policy limit).

When vulnerabilities do result in cyber incidents, Coalition's Active Response capabilities enable us to intervene quickly to help contain and sometimes eliminate losses. Many Coalition policyholders are able to have their claim fully remediated and covered by the policy with no additional expenses incurred. In 2021, we resolved 46% of claims at no additional cost to the policyholder using our in-house claims and incident response teams.

Coalition's proprietary Active Risk Platform provides a robust data set on the security conditions that lead to financial losses. As a result, we understand that stopping critical attacks such as ransomware isn't just a technology problem; it's a risk management problem.



# 05

## Predictions for 2022

At Coalition we have unique insight into the cyber threat landscape and its impact on our policyholders. We expect the market will continue to evolve and our claims, incident response, and insurance teams share the following predictions for the upcoming year.



### **Cyber insurance will become harder for many businesses to access.**

In 2021, the insurance market continued to harden and this is unlikely to slow down. In the first half of 2021, we predicted the insurance market would continue to harden throughout the year and it would become harder to qualify for cyber insurance. Over the second half of the year we observed more than one carrier pause underwriting cyber

insurance policies entirely — after previously rolling out price increases, coinsurance, and sublimits on critical coverages. We predict the market will stay hard for some time, particularly in response to the insecurity surrounding potential government oversight and intervention. As the world's focused Active Insurance company, Coalition has not pulled back coverage and is instead focused on **preventing digital risks before they strike**. Our Active Cyber and Active Executive Risk products help organizations assess, prevent, and cover digital risks.



### **Government scrutiny regarding ransomware payments and cybersecurity will continue.**

Previously, we predicted more regulation and public frameworks



from governmental entities regarding the disclosure of cybersecurity incidents. In 2021 we saw an uptick in ransomware events along with increased government scrutiny surrounding payments. Coalition, along with other technology industry leaders, has been advising a part of these governmental discussions including President Biden’s White House meeting regarding cybersecurity; discussions with the executive branch regarding ransomware; and overhauling the NIST standards regarding cybersecurity. We anticipate lawmakers to continue to navigate this gray area in 2022 and for cybersecurity to remain a part of public discourse for the foreseeable future.



### **Supply chain attacks will continue to plague affected businesses in emerging ways.**

As Log4j and the many other vendor hacks of 2021 revealed, attacks on software are increasing and the impacts can be far-reaching. Although Log4j did not turn out to be the cyber armageddon many vendors and news outlets had predicted, it can take weeks or months for bad actors to identify ways to monetize the supply chain attacks.

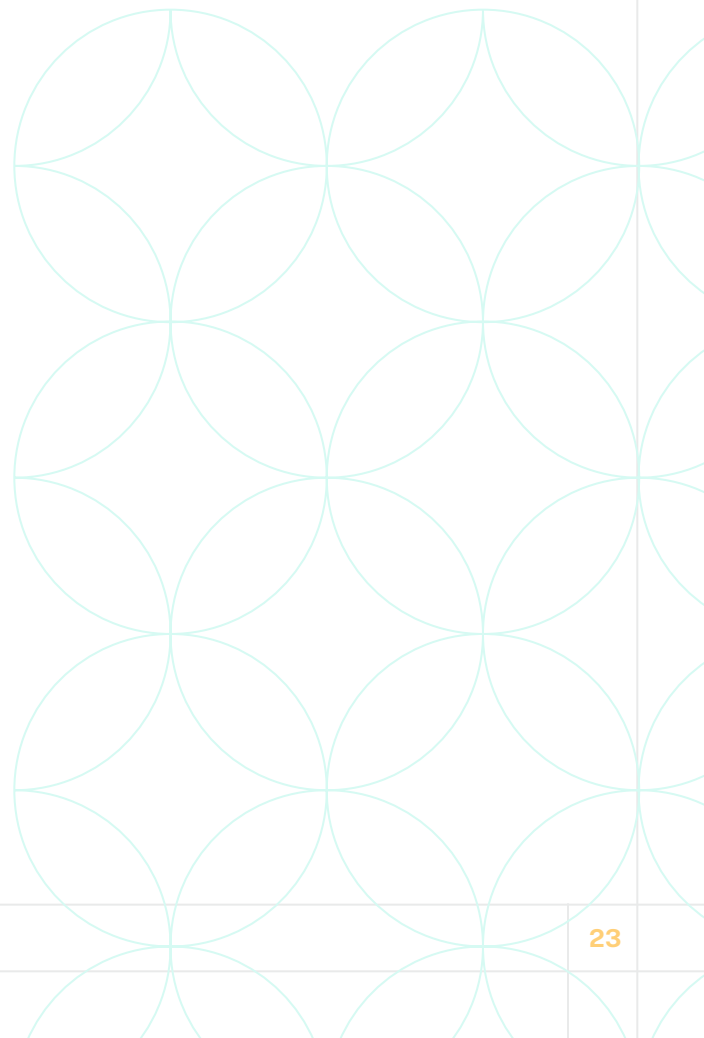
We’re likely to see a very long tail of attackers trying different applications and ways to exploit these supply chain vulnerabilities. We expect these attacks to increase in 2022 with threat actors focusing on new extortion techniques for monetary gain, and nation-states seeking intelligence.



### **Continued impact of vulnerable and unpatched boundary devices.**

The devices designed to protect or provide access to organizational networks (such as firewalls, VPNs, and remote access appliances) proved highly vulnerable in 2021. As return-to-office plans were delayed or scrubbed, and temporary setups became permanent, these assets drew attention from threat actors and the patch cycle for firmware at many organizations is far slower than operating system and software updates.

We expect to see continued attacks targeting tools like SonicWall, VMWare, and others that provide remote access and collaboration features.





# 06 Active Insurance

## How Coalition continuously combats digital risk

Coalition was founded to solve digital risk and create a safer digital economy where everyone can thrive. What sets Coalition apart from other insurers is that we not only mitigate and transfer digital risk — we actually help solve it. We're innovating around the very core of insurance to provide a new type of protection.

We've done this by building the world's first Active Insurance company: a new kind of insurance for today's new kind of risk. Active Insurance introduces a new model of coverage built for the digital economy. It combines the power of technology and insurance to help organizations identify, mitigate, and respond to digital risks.

**Coalition was founded to solve digital risk and create a safer digital economy where everyone can thrive.**

Coalition's Active Risk Platform uses artificial intelligence (AI) to analyze data and scans from the public web with signal intelligence from the dark web and claims/ incident data to create an incredibly-accurate picture of an organization's digital risk. With this individualized profile, we can provide:

- **Active Risk Assessment**

With an accurate profile of near-real-time risk, we can more accurately price coverage, speed up the quoting process and identify potential issues that most traditional insurers and many insurtechs never see.

- **Active Protection**

With an accurate profile of your digital systems and ongoing scans, we're able to alert customers when new vulnerabilities to your software are discovered and work with your IT owner to get them resolved quickly.

- **Active Response**

When potential incidents occur, our Incident Response and Claims teams can be granted fast access to our digital records to help you solve the issue and get back up and running faster than ever.





Taken together, these capabilities provide a better model of protection for our policyholders.

**Our H1 2021 claims report revealed that our policyholders experienced 70% fewer claims than the industry average<sup>3</sup>**, and we expect to soon show similar results for 2021 as the industry data becomes available. We also solved 46% of all reported incidents at no cost — helping our policyholders get businesses back up and running. Active Insurance simply keeps policyholders safer, reducing their exposure to

new cyber incidents and responding quickly to resolve issues when they do occur.

The events of the past year have shown just how dynamic digital risk can be. While familiar attacks like phishing and malware persist, new supply chain vulnerabilities and other digital risks like Microsoft Exchange and Log4j continue to expand the boundaries of risk. It may take months or even years to understand how these new risks will impact organizations.

**Digital risk is different**, and this unpredictability highlights the need for Active Insurance solutions that can provide continuous protection in addition to comprehensive coverage in the event of an incident. Our capabilities and expert team are protecting 140,000+ customers and we partner with over 30,000 brokers today.

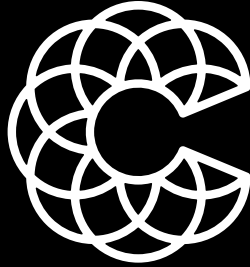
**Learn how Coalition's Active Insurance solution can provide continuous protection from digital risks in 2022 and beyond**

To offer this coverage as a broker, look into getting appointed today: Visit [signup.coalitioninc.com](https://signup.coalitioninc.com).

To apply for this coverage for your own business, contact your broker — and check out your own free Coalition Risk Assessment for your organization: Visit [control.coalitioninc.com](https://control.coalitioninc.com).





**Endnotes**

- 1. IDC FutureScape: Worldwide Digital Transformation 2021 Predictions
- 2. National Association of Insurance Commissioners report, NAIC, 2021
- 3. Coalition H1 2021 Claims Report



# Coalition<sup>®</sup>

[coalitioninc.com](http://coalitioninc.com)

-  Coalition, Inc.
-  @SolveCyberRisk
-  Coalition, Inc.
-  [help@coalitioninc.com](mailto:help@coalitioninc.com)

1160 BATTERY ST. SUITE 350  
SAN FRANCISCO, CA 94111

Insurance products underwritten by Coalition Insurance Solutions, Inc. (CA License # 0L76155).  
This is marketing material only, and does not form part of the policy.

Copyright © 2022. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc. or its affiliates.