CORO

The Biggest Cyber Security Threats Coming in 2022

Best practices to keep your business protected

Contents

Introduction

Since the start of 2020, a cyber warfare perfect storm has been brewing. An entire swath of the global economy – hundreds of thousands of mid-sized businesses – lies in its path of destruction, with each company falling into one of two categories: **those that have already suffered a security breach and those that will in the near future.**

How do we know this? We've studied the data. Over the course of 2020 and 2021, Coro undertook a research effort focused exclusively on mid-market businesses. We analyzed data from over 4,000 companies that employ between 100 and 1,500 people and operate in six industries:

- Retail
- Manufacturing
- Professional Services
- Healthcare
- Transportation
- Education

Our findings should serve as a wake-up call to both the mid-market segment and the cyber security industry that is currently undeserving it. In just the past two years, attacks against mid-sized companies overall have **increased by 150%**, with attacks against specific sectors ranging from just about doubling to nearly tripling over that two-year period. At the same time, mid-market companies' defenses against these growing attacks have not kept pace.

The combined growth in attacks and stagnation of security solutions offer a grim prognosis for mid-market cyber security preparedness in 2022 and beyond. That said, not all hope is lost. With a proper shift in the cyber security paradigm, growing companies can find protection against this looming and ever-increasing threat.

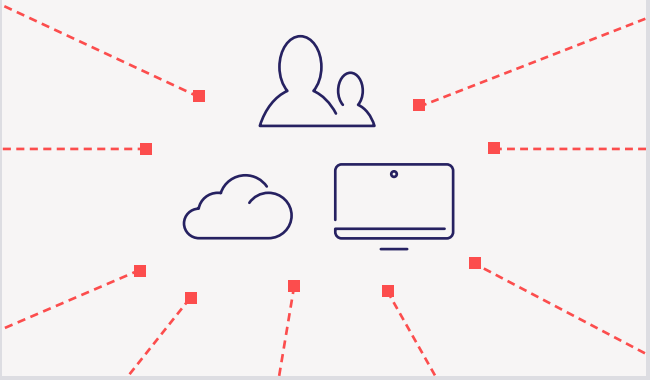
In just the past two years, attacks against mid-sized companies overall have increased by 150%, with attacks against specific sectors ranging from just about doubling to nearly tripling over that two-year period.

Leading with the Conclusions:

Seven Unavoidable Truths Stemming from Our Research

1

Growing companies are getting barraged by cyber attacks with a frequency that is now on par with large enterprises.

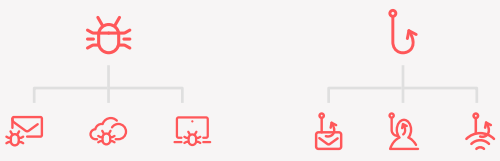


2

No industry is escaping the new attention cyber criminals are directing toward mid-market businesses. Every sector has seen tremendous **increases in attack volume**, putting companies in all sectors at risk.

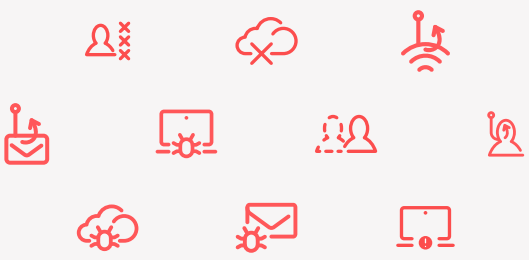
3

While numerous factors contribute to the increasing volume of attacks, one of the more important shifts we've seen is the **expansion of attack vectors.** Phishing and malware attacks now have many more "flavors" than they did prior to the pandemic, opening up entirely new avenues for bad actors to infiltrate corporate networks.



4

Not only has the number of attacks against any given mid-sized company increased dramatically over the course of the past two years, **the level of sophistication of the attack schemes has risen significantly** as well.



5

Automation of attacks against mid-market companies has increased significantly during the COVID era.

6

The vast majority of businesses in our study lack protections against this expanding and increasingly sophisticated array of attack vectors. And for the few companies that have deployed security solutions targeting specific attack vectors, the vast majority of these deployments are misconfigured, rendering the intended protection ineffective.

7

The escalation in attacks against mid-market companies combined with the increasing sophistication seen over the past two years point to dire predictions for 2022 and beyond.

Mid-Market Cyber Security

Another Casualty of the COVID-19 Pandemic

Why is the picture for 2022 and beyond so grim? What changed over the course of the past two years? **While much of the world was largely shut down throughout the greater part of 2020 and on into 2021, the malware industry boomed.** There were numerous contributing factors, but three elements in particular combined to nourish this perfect storm:

1. Digital transformation, accelerated by the social distancing COVID-19 forced on the world in the early days of 2020, pushed companies to a remote work model, corporate applications and IT systems to the cloud, and workers to any available endpoint device.

2. A burgeoning class of cyber attackers, emboldened by the massive increase in online and cloud-based activity and the expanded security perimeters caused by so many remote log-ins, leveraged readily available malicious code, a growing cyber warfare support industry, and increasingly affordable compute power to scale cyber assaults to previously unseen levels across new attack vectors never before seen.

3. The cyber security industry, long focused on developing and selling enterprise-grade security solutions with enterprise-grade price tags, fell woefully behind an expanding array of attack vectors barraging growing companies, all but completely neglecting this enormous market segment and their exploding need for affordable alternatives to enterprise security offerings.

The Result?

A geometric expansion of cyber attacks against unprotected mid-sized companies leading to a proportional increase in the likelihood that each of them will experience a security breach.

Attacks against Transportation companies more than tripled over the course of 2020 and 2021.

Detailed Findings

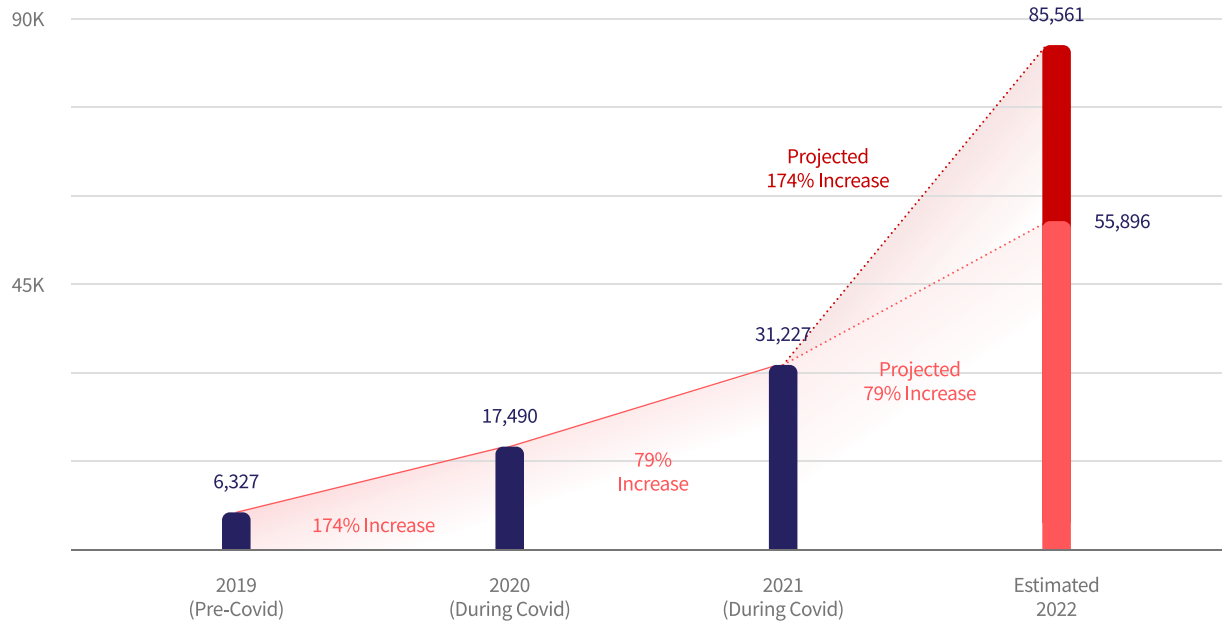
1. Growing companies are getting barraged by cyber attacks with a frequency that is now on par with large enterprises.

When we look back to the days before the pandemic had taken global effect, we see that mid-sized companies suffered roughly 6,300 attacks per company on average over the course of 2019. In 2020 that number had risen to roughly 17,500, and by the end of 2021 the average number of attacks per company soared to more than 31,000 for the year.

These jumps represent **increases of 174%** between 2019 and 2020, and **79%** between 2020 and 2021.

If the percent increase between 2021 and 2022 falls anywhere within these ranges, the typical mid-market company can expect to be **attacked between 56,000 and 86,000 times** over the course of 2022. (See Figure 1.)

Actual and Projected Numbers of Attacks per Company, 2019 through 2022



— Figure 1 —

While these numbers may appear to be extreme, they aren't. If a mid-sized company with 1,000 employees is attacked between 56,000 and 86,000 times in a year, that corresponds to just five to seven attacks per employee per month. It may be that at the end of 2022 we find that these projections were, in fact, significant underestimates.

2. No industry is escaping the new attention cyber criminals are directing toward mid-market businesses. Every sector has seen tremendous increases in attack volume, putting companies in all sectors at risk.

As we studied the increases in attacks against mid-market companies over the course of 2020 and 2021, we saw that no sector was immune to the escalating nefarious cyber activity directed at growing companies. Overall, attacks against educational institutions **effectively doubled** from Q1 of 2020 to Q4 of 2021. Professional Services, Manufacturing and Retail businesses experienced a **2.5x increase in attacks**, and Healthcare and Transportation **nearly tripled** over the same period of time. (See Figure 2)

Percent Increase in Average Attacks Per Company Q1 2020 to Q4 2021

Transportation
195%

Education
97%

Professional Services
119%

Manufacturing
131%

Retail
149%

Healthcare
178%

— Figure 2 —

By the end of 2021, hospitals and other healthcare companies emerged as the most heavily targeted institutions in our study.

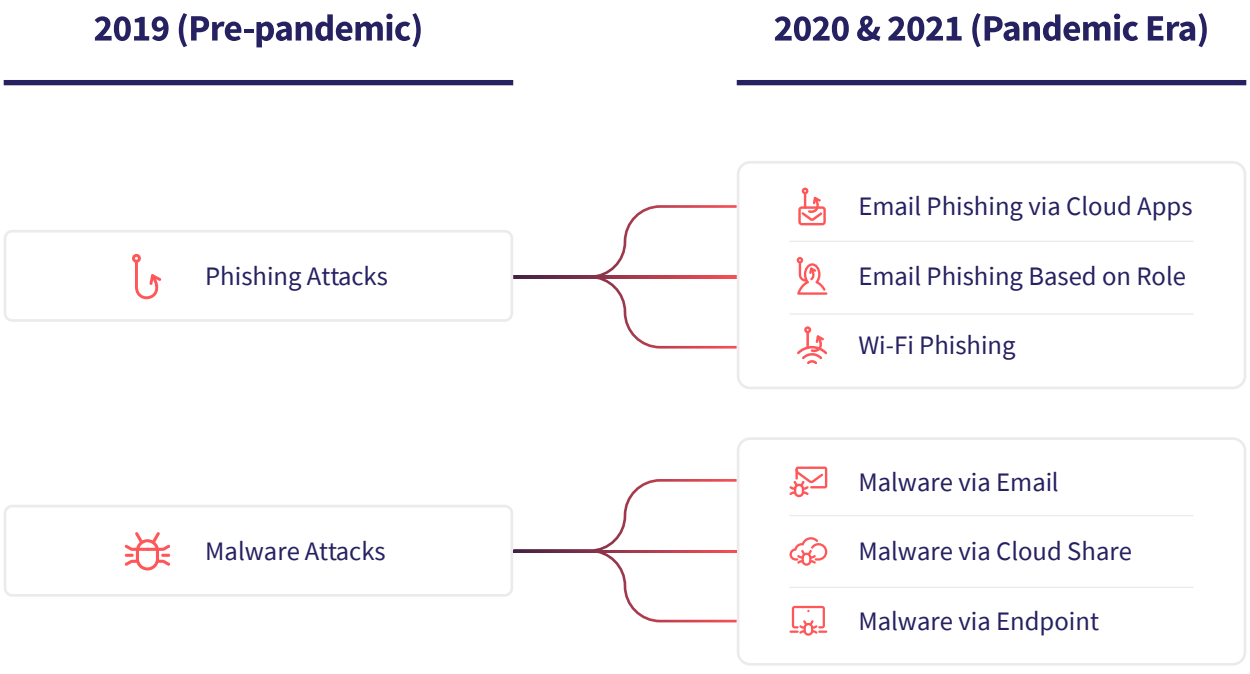
3. While numerous factors contribute to the increasing volume of attacks, one of the more important shifts we've seen is the expansion of attack vectors. Phishing and malware attacks now have many more "flavors" than they did prior to the pandemic, opening up entirely new avenues for bad actors to infiltrate corporate networks.

Pre-pandemic, phishing attacks were carried out via email in fairly unsophisticated campaigns that relied on scale to be successful. Over the course of the pandemic, however, new methods of phishing emerged to exploit the massive increase in remote work. Phishing via cloud apps and Wi-Fi phishing escalated to trick unsuspecting users into visiting bogus websites or joining fraudulent networks. (See Figure 3)

Malware attacks diversified too. Traditionally, malware targeted endpoint devices. Since the start of the pandemic, however, we've seen malware delivered via cloud emerge as a major threat vector. Cloud sharing platforms like Google Drive or Dropbox and others have become vehicles for malware delivery. In an organization relying on cloud applications, once an individual employee's local directory gets infected and that individual syncs their directory with the company directory, the malware payload is uploaded to the cloud.

Then, as other employees sync with the cloud-based directory, each individual's machine unknowingly downloads that malware payload. And because cloud-based data-sharing platforms use encryption, the encrypted malware is able to infect other users' directories without being detected by most endpoint malware solutions.

Phishing and malware attacks against retail companies jumped by more than 2.5x from the start of 2020 to the end of 2021.



— Figure 3 —

The diversification of attack vectors is a big contributor to the overall increase in attacks on mid-market businesses. The following table shows the attack vectors employed in 2019 and how the array of attack vectors expanded over the subsequent two years. (See Figure 4) As a result, we've seen a **390% increase overall in the number of attacks** the typical mid-sized company endured during the past two years of the pandemic.

	2019 Pre-Covid Attack Vectors		2021 Attack Vectors	
Phishing Attacks	Email Phishing General	3,129	Email Phishing General	8,094
			Email Phishing Via Cloud Apps	2,649
			Email Phishing Based on Role	3,193
			Wi-Fi Phishing	2,342
Malware Attacks	Malware via Endpoint	1,813	Malware via Endpoint	1,295
			Malware via Email	821
			Malware via Cloud Share	3,512
Hacking and Access Control	Unauthorized Activities	207	Unauthorized Activities	821
	Abnormal Admin Activities	96	Abnormal Admin Activities	3,512
	Abnormal Login	533	Abnormal Login	6,666
	Dormant Account Activity	93	Dormant Account Activity	532
			Account Takeover	290
			BOT Attacks via Credential Theft	413
Insider Threats	Insider Threats	207	Insider Threats	290
Data Leakage/Loss	Regulated Data Leakage	295	Regulated Data Leakage	413
	Total Attacks 2019:	**6,372**	**Total Attacks 2021:**	**31,227**

— Figure 4 —

As a result, we've seen a 390% increase overall in the number of attacks the typical mid-sized company endured during the past two years of the pandemic.

4. Not only has the number of attacks against any given mid-sized company increased dramatically over the course of the past two years, the level of sophistication of the attack schemes has risen significantly as well.

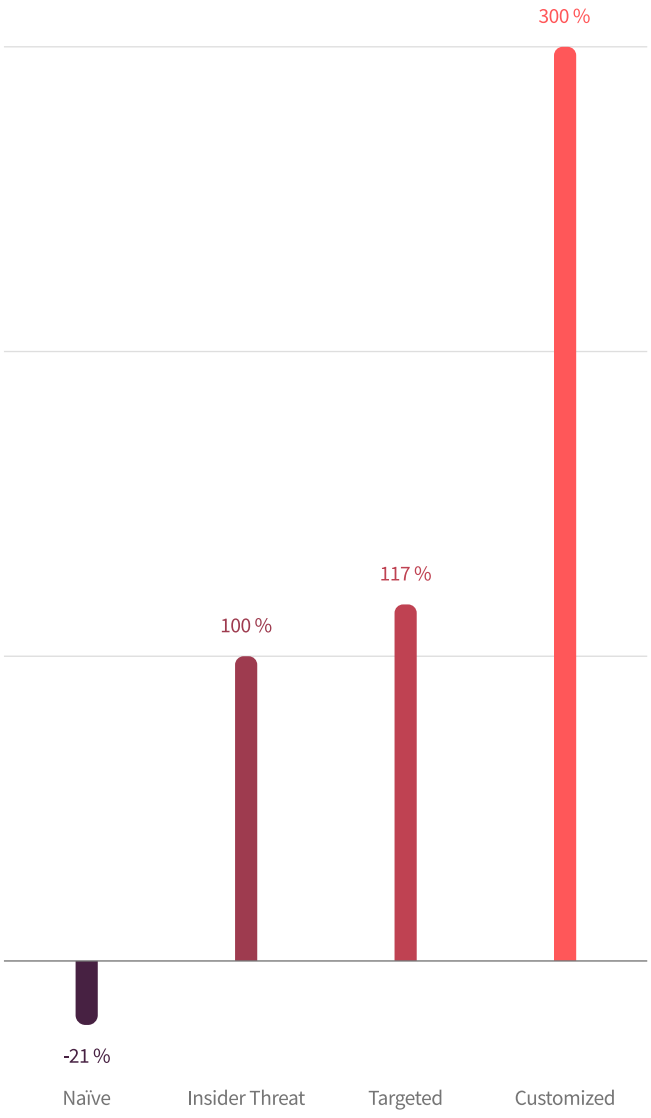
Naïve Attacks

Prior to the pandemic, the preponderance of attacks against mid-market companies could be described as naïve. Naïve attacks do not differentiate among their targets. They can be executed in the form of millions of emails that go out to millions of recipients, hoping that even a tiny fraction of their targets takes a desired action like giving up credentials or visiting a bogus site. Or they may take the form of automated bots that blindly try to take over accounts by randomly generating credentials until they are either successful or get locked out of accounts.

During the pandemic, however, the malware industry continued to mature, with malware products and services propagating quickly due to demand on the part of bad actors. At the same time, compute power continued to grow cheaper, giving cyber attackers the tools and infrastructure to scale their attacks and change the economic equation to one that makes it operationally feasible to pursue smaller, less financially endowed targets comprising the mid-market.

This opened doors for bad actors to launch more targeted attacks and customized attacks at the mid-market level. During the pandemic, **naive attacks dropped by 21%** while the more sophisticated methodologies, including targeted and customized attacks, as well as insider threats, each **expanded geometrically in popularity** among cyber criminals. (See Figure 5)

Changing Prevalence of Attack Type 2020-2021



— Figure 5 —

The shift in attack sophistication resulted in targeted attacks against manufacturing companies more than doubling between 2020 and 2021.

Targeted Attacks

Targeted attacks are devised to appeal to particular personas or people working in specific industries. Think of them as cyber attacks with market segmentation. Customized attacks, then, are really the account-based marketing approach to cyber attacks. Customized attacks are personalized to high-value individuals. Specific executive leaders at specific companies are typically those to whom customized attacks are directed.

Customized Attacks

Currently, customized attacks are the most expensive and labor-intensive to execute, so these highly orchestrated attacks still reside principally in the large enterprise segment, where a company's assets can be orders of magnitude greater than the typical mid-market business. But while relatively few customized attacks are being directed at mid-market players currently, the growth of targeted and customized attacks in an era when cyber warfare is growing increasingly cost effective is a worrisome trend to continue to monitor.

Insider Threat

The insider threat is growing rapidly, too, having doubled over the course of the past two years. While insider threats can result from individuals with specific agendas, it is equally or more likely that insider threats are not malicious in their origin. With the rise of cloud applications that promote easy collaboration between internal and external parties through the simple sharing of files, internal parties will often share unencrypted files with partners, contractors, customers, prospects and others or they may share company data with their own private email accounts. These actions leave sensitive data outside of the control of the company, which can put these businesses at grave risk.

During the pandemic, naive attacks dropped by 21% while the more sophisticated methodologies, including targeted and customized attacks, as well as insider threats, each expanded geometrically in popularity among cyber criminals.

Naïve attacks dropped significantly from 2020 to 2021.

Targeted and Customized attacks increased 2x and 4x, respectively.

Insider threats also doubled over the past two years.

5. Automation of attacks against mid-market companies has increased significantly during the COVID era.

The commoditization of cyber attacks discussed in the previous section has only been possible through the expanded reliance on automation. Commoditization and automation have created economies of scale that favor the cyber attacker and open the mid-market segment to their incursions. We see that bot attacks have well more than doubled over the past two years. (See Figure 6) Further, companies offering malware-as-a-service have sprung up to offer sophisticated and automated attack campaigns to anyone willing to pay for their services.

At the same time, with so many people working remotely, the security perimeter of the typical company has expanded geometrically, leaving all companies (and particularly mid-market businesses) much more vulnerable due to the vast number of endpoints connecting to corporate networks remotely. As workers mix job-related tasks with personal tasks, the opportunity to fall prey to a phishing campaign or an account-takeover attack is tremendous, and attackers utilize automation to cast their nets far and wide.

General Email Phishing

80%

Increase 2020-2021

Bot Attacks

138%

Increase 2020-2021

Malware via Endpoint

56%

Increase 2020-2021

— Figure 6 —

Commoditization and automation have created economies of scale that favor the cyber attacker and open the mid-market segment to their incursions.

6. The vast majority of businesses in our study lack protections against this expanding and increasingly sophisticated array of attack vectors.

And for the few companies that have deployed security solutions targeting specific attack vectors, the vast majority of these deployments are misconfigured, rendering the intended protection ineffective. Here lies the dire truth of this mid-market crisis. Of the 4000+ companies we studied, exceedingly few had security solutions in place beyond general malware and email phishing protection. (See Figure 7) Aside from these two rudimentary forms of protection, mid-sized businesses lay largely exposed to the many new threat vectors that emerged during the past two years of the pandemic.

Malware Protection

50%
of businesses

Email Phishing Protection

16%
of businesses

Insider Threat Protection

Hacking and Access Control Protection

Data Leakage/ Loss of Protection

Less than **1%** **of business have protections against these attack vectors**

— Figure 7 —

Professional services companies struggled to protect sensitive customer data in the face of a doubling of attacks per business from 2020 to 2021.

Here's an additional wrinkle:
Of the security solution deployments we saw within the mid-sized companies we studied, the vast majority were configured incorrectly, which greatly compounds the problem. (See Figure 8) Given that at the enterprise level, security solutions are often supported by hefty service contracts to achieve exacting SLAs, it's not surprising that smaller companies forgo these financial burdens and instead rely on in-house expertise to deploy, operate and maintain the security solutions in which they've invested. As a result, these companies are less well protected than they believe themselves to be and therefore may be less vigilant in trying to identify attacks that these solutions, when properly deployed, would have thwarted.

These dismal statistics point to a skills gap that exists within the IT and security organizations in mid-sized companies. The security industry has not yet stepped in to fill the void, either with modern security products that reflect current market need or for supporting services to help growing companies identify and defend against new and expanding threat vectors. Nature may abhor a vacuum, but cyber criminals love them. These conditions leave the mid-market segment much more likely to experience a breach with each passing day.

— Figure 8 —

7. The escalation in attacks against mid-market companies combined with the increasing sophistication seen over the past two years point to dire predictions for 2022 and beyond.

As we move into 2022, many of the uncertainties brought about by COVID-19's explosion around the world linger. In the business realm, figuring out how best to support and secure remote connections remains at the top of the agenda of IT and security teams. Without a change in the way teams go about procuring and providing security solutions, expanding the security perimeter to address the persistent distributed work model and warding off the rapidly growing barrage of cyber attacks will require an ever greater number of personnel and resources to contend with and orchestrate an increasingly inadequate collection of security tools.

From 2019, when we saw an average of 6,327 attacks per mid-market company, to the end of 2020, when we saw an average of 31,227, the **volume of attacks increased by 390%**. That means the subsequent **likelihood of a breach increased nearly fivefold**.
We anticipate the average volume of attacks to swell to somewhere between **56,000 and 86,000** attacks per mid-sized business.

As attackers grow increasingly efficient in their cyber crime operations, utilizing automation to scale their assaults while also having greater bandwidth to create and launch more targeted attacks, all while too many point security solution providers continue to focus on enterprise customers and forsake the enormous mid-market segment, the outlook for mid-sized businesses in the coming year and beyond is bleak.

The only chance mid-market companies have to reduce the probability of a damaging or calamitous breach is to change their traditional approach to securing their operations.

While attacks against the education sector increased less dramatically than the other industries in our study, this sector still saw the 3rd highest number of attacks per institution in 2021.

A New Paradigm for Mid-Market Security

Even if there were enough point solutions on the market today to cover the ever-broadening array of attack vectors being introduced into the cyber crime market, the IT and security resources needed to research, purchase, deploy, configure and support the collection of disparate technologies would **blow holes in the typical growing company's IT and security budgets.**

And when it comes to the skills gap that plagues mid-market companies that try to configure and orchestrate a mismatched collection of proprietary security solutions, it's clear that the point-solution approach is no longer a feasible option. Instead, mid-market companies should take a platform approach to cyber security. Partnering with a single vendor that provides a **comprehensive solution** to securing email, cloud applications and endpoints against the gamut of threat vectors that spans malware and ransomware, phishing, access control, insider threats and data loss is the only viable solution. A platform approach can:

Simplify the orchestration of security operations across all business units.

Shift the onus for keeping abreast of new threat vectors away from the company and onto the security provider.

Greatly reduce the complexity of the security technology stack while simultaneously expanding the range of protections growing companies must deploy.

Offer peace of mind to IT and security leaders who are responsible for monitoring company operations, identifying threats, warding them off before they become breaches and mitigating damage when an attack is successful.

In this new era, cyber security requires a holistic approach. Fortunately, there is a better one available today. And certainly, as time goes on and spotlights fall on more reports of damaging mid-market breaches, more security vendors will wake up to the glaring need that exists across the mid-market segment.

That's cold comfort to the growing companies that have already fallen victim to successful attacks. In order to avoid falling into either that category of mid-market businesses or the other category of those for whom a damaging breach is just a matter of time, mid-sized companies need to act now to embrace the security platform approach.

Methodology

This report comprises data aggregated from analysis of over 4,000 growing companies **spanning six industries across the following distribution**:

Company Size (by Number of Employees)	Transportation	Manufacturing	Retail	Professional Services	Healthcare	Education
Up to 100	12	27	17	26	88	40
101-500	56	307	155	707	363	125
501-1,500	314	344	26	631	488	105
1,501+	27	20	21	28	59	15
Total Attacks	**409**	**698**	**219**	**1392**	**998**	**285**

All data reflects actual counts, with the following exceptions:

The ratio of growth in attacks from 2019 to 2020 was assumed to be **80%** of growth from 2020-2021.

Increases in attacks in each sector and across each attack vector for the months of November and December 2021 are extrapolated from actual percent increases over the first ten months of 2021 and the percent increases for November and December 2020.

For any questions about methodology,
please contact us at coro.net.

About Coro

Coro is one of the fastest growing security solutions for the mid market, providing all-in-one protection that empowers organizations to defend against malware, ransomware, phishing and bots across devices, users and cloud applications. Built on the principle of non-disruptive security, more than 5,000 businesses depend on Coro for holistic security protection, unrivaled ease of use and unmatched affordability.

The Coro platform employs innovative AI technology to identify and remediate the many security threats that today's distributed businesses face, without IT teams having to worry, investigate, or fix issues themselves. Investors in Coro include JPV, MizMaa Ventures and Ashton Kutcher's Sound Ventures. For more information, **please visit coro.net.**

All-in-one Cyber Protection

Unparalleled defense. Unrivaled ease of use. Unmatched affordability.

User Protection | Cloud apps Protection | Email Protection | Devices Protection | Data Protection