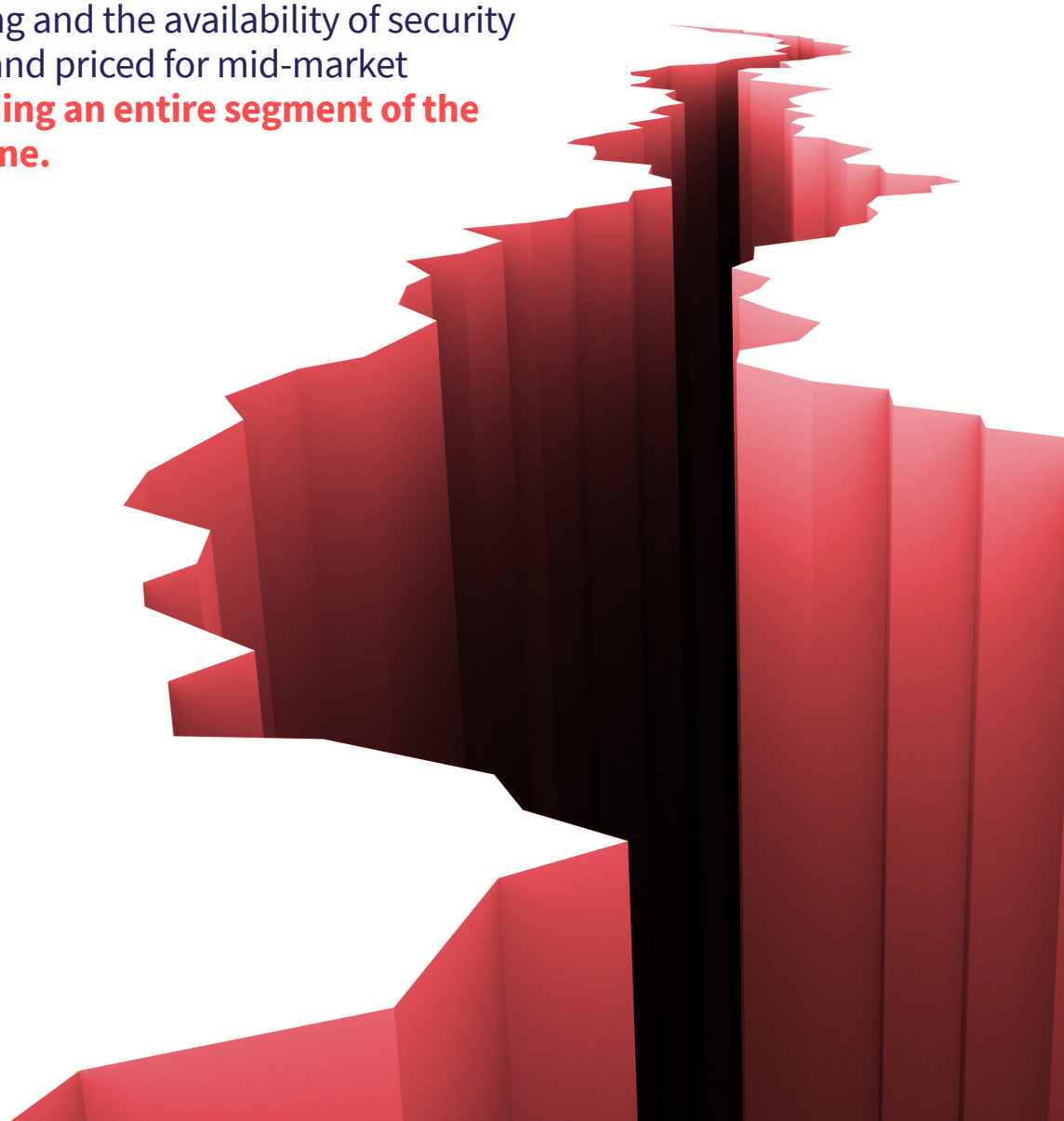
CORO

The Great Cyber Security Market Failure and the Tragic Implications for Mid-Sized Companies

The widening gap between the attack vectors cyber criminals are employing and the availability of security solutions engineered and priced for mid-market businesses is **threatening an entire segment of the global economic engine.**



Contents

Executive Summary

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.**

Three elements have combined to brew 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, 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, has fallen woefully behind the expanding array of attack vectors and completely neglected this enormous segment of mid-sized companies and their exploding need for affordable alternatives to enterprise security offerings.

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

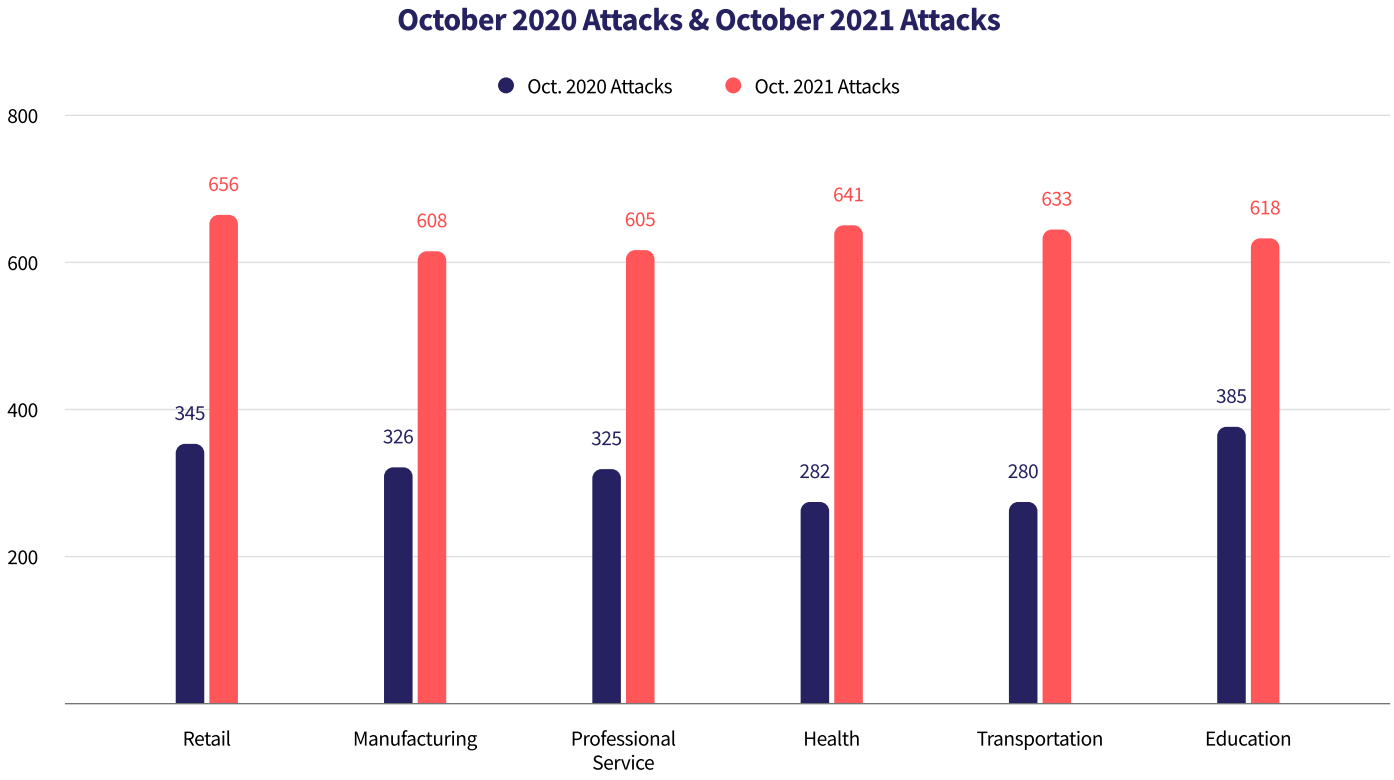
Over the course of 2020 and 2021, Coro has undertaken a **research effort unprecedented in scope and granularity.** We analyzed data from over 4,000 mid-sized companies (defined herein as those that employ up to 2,500 people) operating in six industries:

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

The results of our extensive examination reveal that growing companies are getting barraged by cyber attacks with a frequency that is now on par with large enterprises, and yet these smaller organizations generally lack the resources and technology that large enterprises can direct toward cyber security. The utter failure of security companies to recognize and focus on the needs of mid-sized companies is leaving an entire business sector in a perilous position.

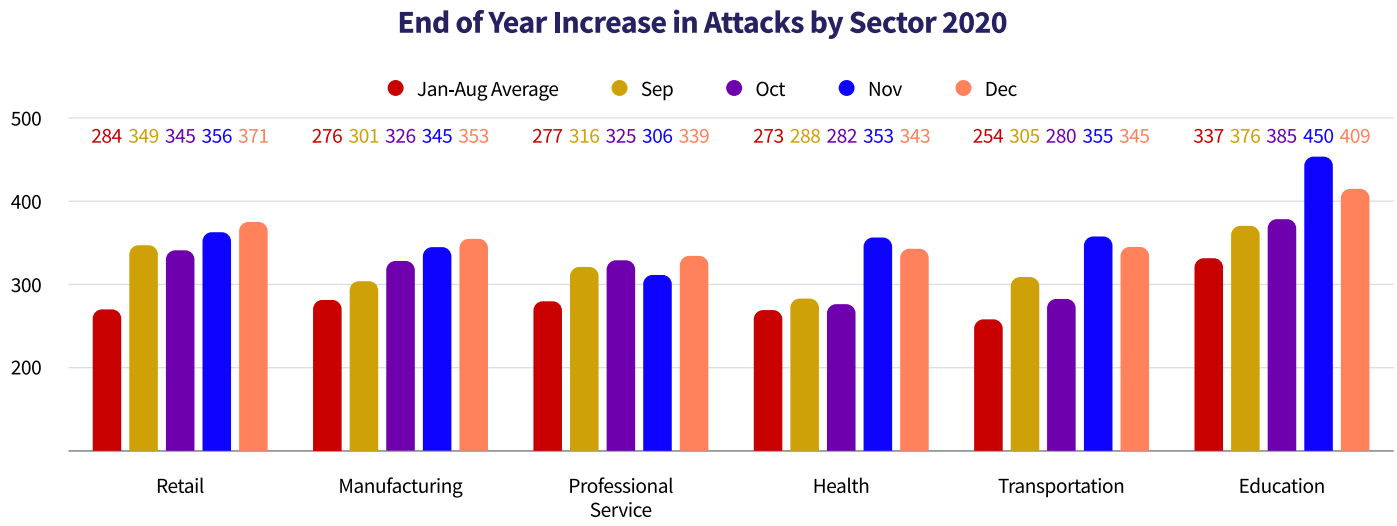
Seven High-Level Findings

1. Over the course of 2020 and 2021, the number of attacks on mid-sized businesses in every sector increased by at least 50% with attacks against Healthcare and Transportation companies leading the way, increasing by more than 125% between October 2020 and October 2021.

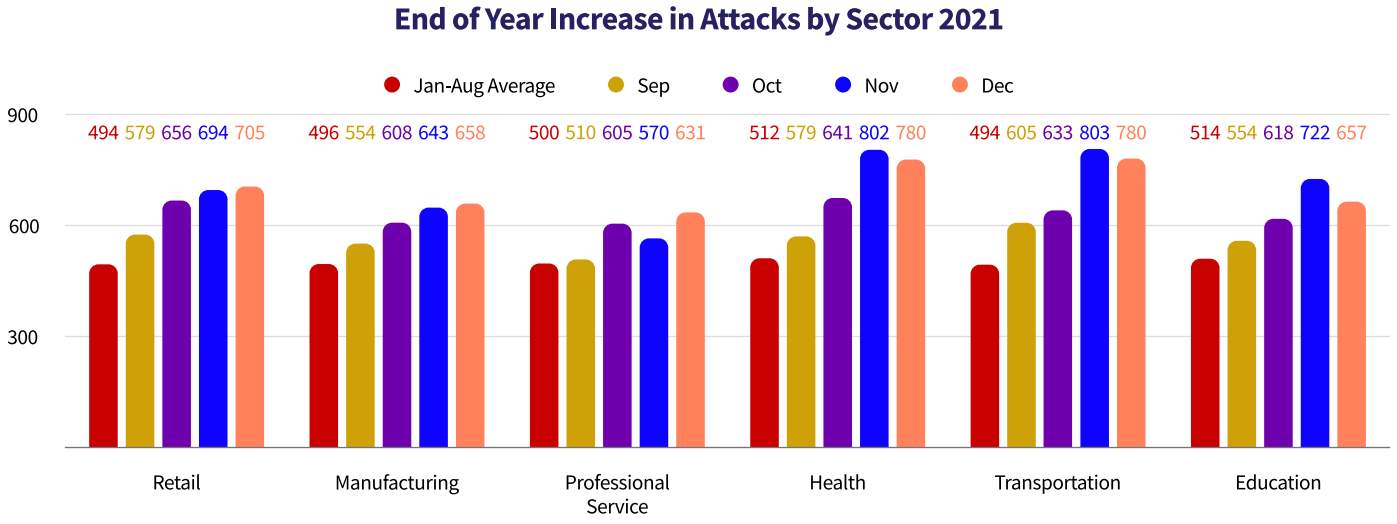


2. Not only are attacks on growing companies increasing year-over-year, mid-market vulnerability increases notably during the final four months of the year:

A. In the last four months of 2020, the attacks on mid-sized businesses in each sector increased between **22% and 36%** compared to the attacks in the first eight months of the year.



B. A similar trend is playing out to date in 2021.[1]



[1] Data for November and December 2021 extrapolated from actual increases through October 2021 and percent increases for November and December 2020

3. In addition to the increasing volume of attacks seen over the past two years, the breadth of attack vectors and the sophistication of attacks have increased, as well.

A. Naïve Attacks

Those attacks involving no attempt to differentiate one target from another – comprised **86%** of all cyber attacks against mid-sized businesses in 2020. In 2021, the proportion of naïve attacks to more sophisticated schemes dropped precipitously from **86%** to **68%**.

B. Targeted Attacks

Attacks which focus on a specific role or persona within an organization, increased from **12% to 26%**.

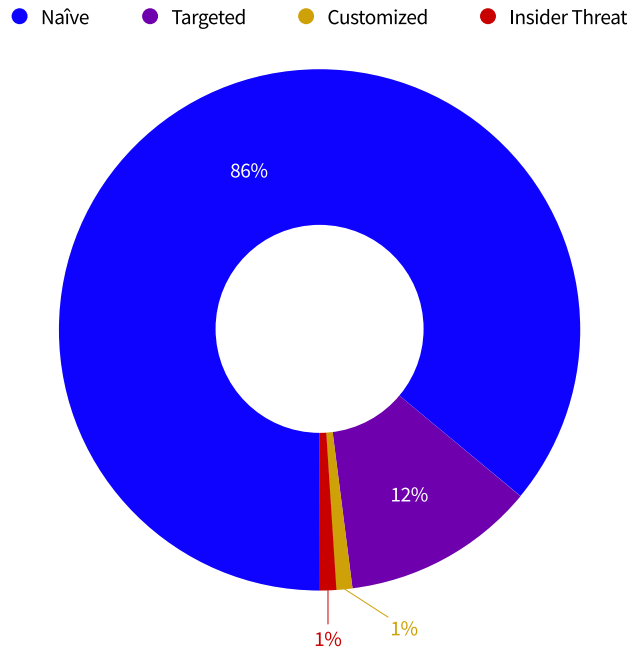
C. Customized Attacks

Attacks which target companies that match a cyber attacker's ideal target profile, grew from **1% to 4%**.

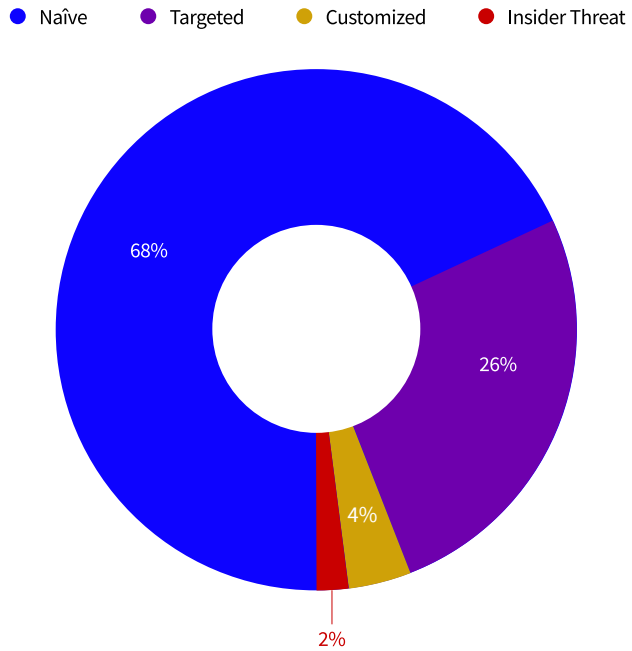
D. Insider Threats

Attacks stemming from insider threats doubled from **1% to 2%**.

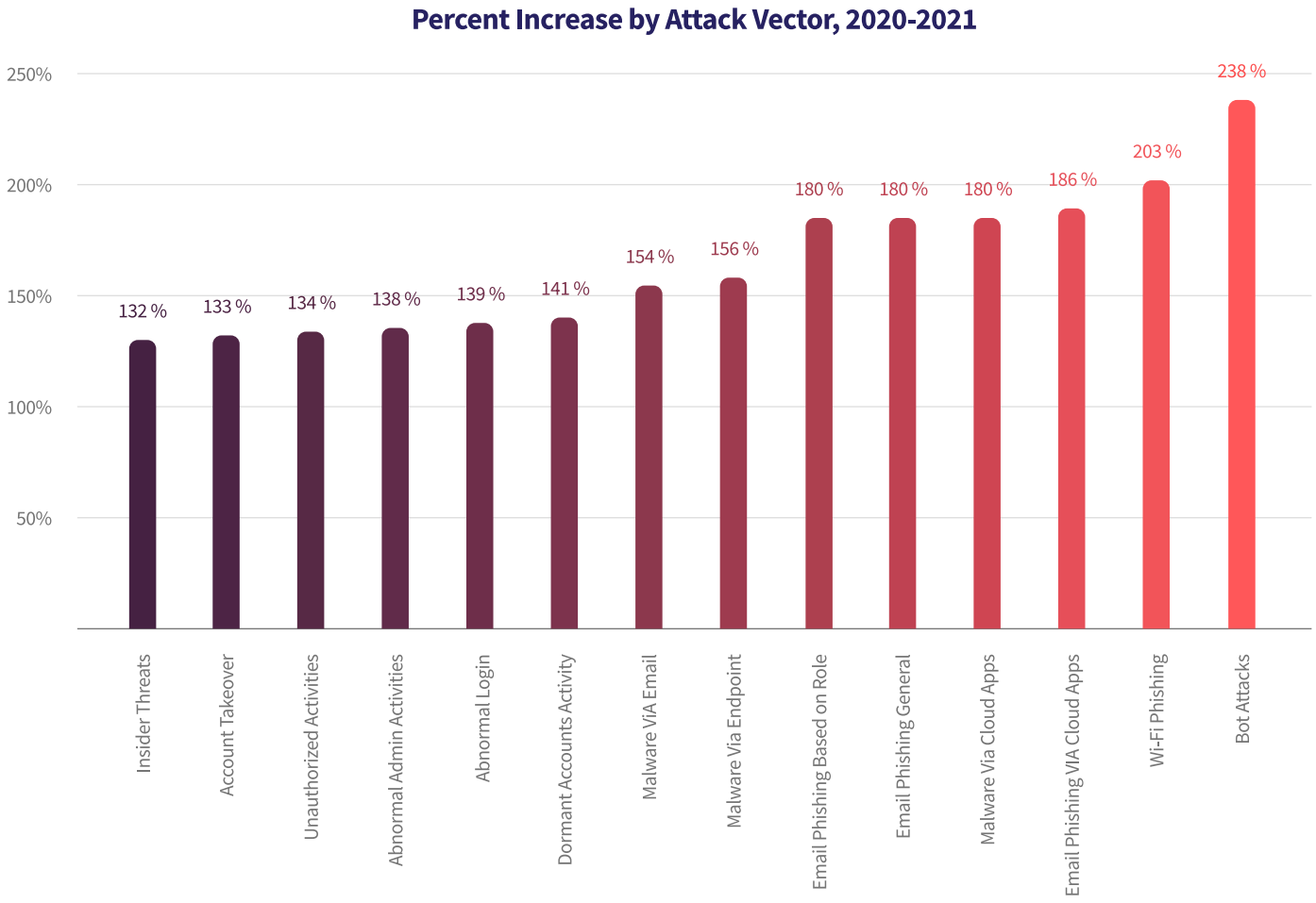
2020 Attack Sophistication



2021 Attack Sophistication

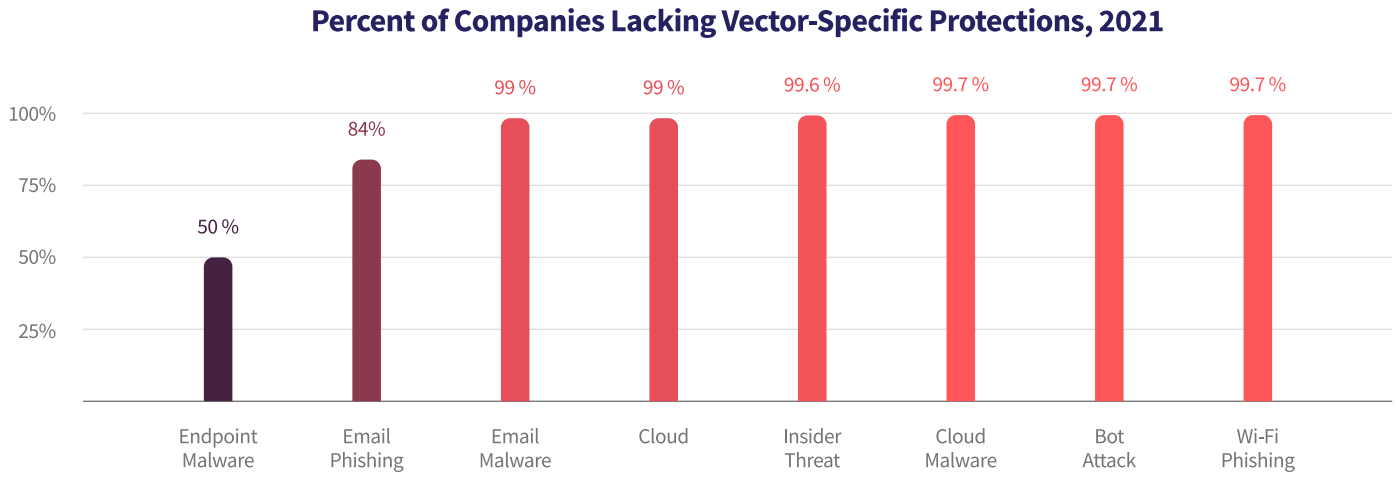


4. Prior to the pandemic, phishing and malware attacks comprised the preponderance of cyber attacks. Since the start of 2020, however, we've seen the rapid emergence of a much broader variety of assault types and every category has grown significantly between 2020 and 2021.

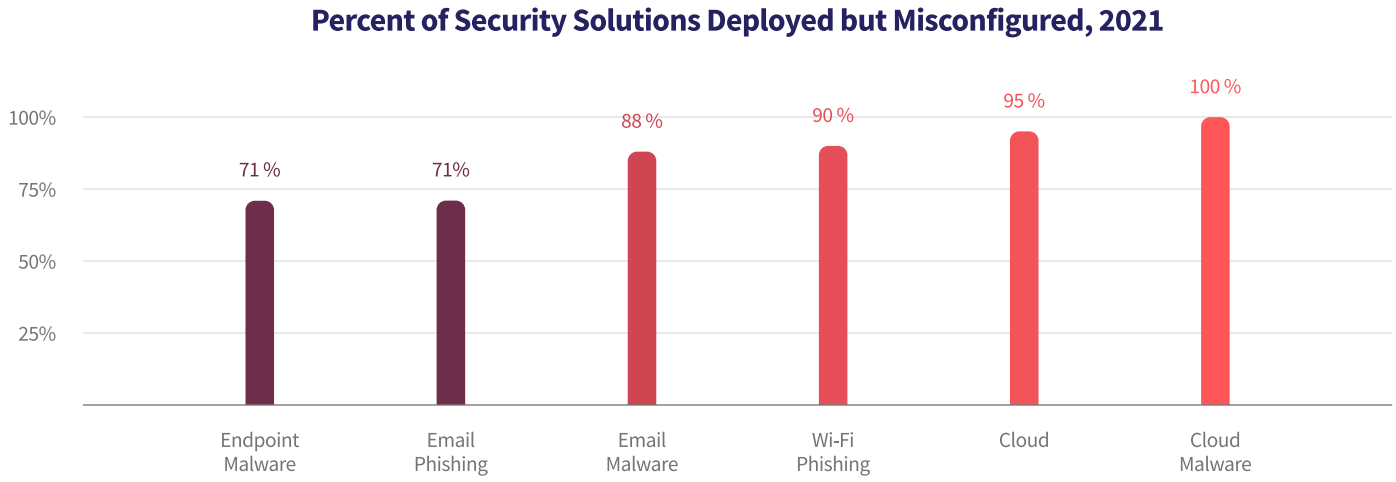


> The cyber security industry, long focused on developing and selling enterprise-grade security solutions with enterprise-grade price tags, **has fallen woefully behind the expanding array of attack vectors.**

5. Exceedingly few growing companies have security solutions in place against this broad array of attack vectors. Most are in the dark when it comes to detecting attacks and completely defenseless when it comes to warding them off.



6. For those mid-market companies that do have point security solutions in place, the vast majority of deployments are misconfigured, greatly compromising their defense against the attacks they were purchased to provide.



7. The culmination of the above six key findings is the following bone-chilling statistic:

Given the growth of cyber attacks and the increase in threat vectors targeting mid-sized companies since the start of the COVID-19 pandemic, combined with the failure of the security industry to provide viable security solutions geared toward growing companies and the widespread misconfiguration of the few security solutions that have been deployed, the likelihood of mid-sized companies experiencing a security breach by the end of this year is **490%** higher than it was back in 2019.

> **The likelihood of mid-sized companies experiencing a security breach by the end of this year is 490% higher than it was back in 2019.**

Total Number of Attacks on Average Per Company, 2019 & 2021

The Enduring Effects of the COVID-19 Pandemic

COVID-19's human toll has been well chronicled. So have been many of the business stories coming out of the pandemic. One of the least publicized economic outcomes, however, may turn out to be one of the most devastating – how the digital transformation accelerated by the shift to remote work and cloud-based IT solutions forced by the pandemic opened the floodgates for cyber attackers to barrage and breach mid-market companies' underprotected networks.

As businesses responded to spiking COVID-19 numbers by sending their employees to work remotely and pushing a greater percentage of their processes online and to the cloud, the move to digital-by-any-means-possible spurred the vast proliferation of cyber attack vectors. Pre-pandemic, cyber attacks were focused mostly on large enterprises, whose customer data and intellectual property promised vast riches to the successful attacker.

But the overall increase in online activity served as the mother of invention in the cyber warfare industry. New attack vectors and a robust industry emerged to support cyber crime, including any number of malware-as-a-service businesses. At the same time, the shrinking cost of compute power made it far easier and more cost effective for cyber criminals to scale their attacks. They became well armed to move beyond the traditional enterprise-level targets, so they trained their sights on the next tier down – the much larger collection of mid-sized businesses.

Unlike the largest corporations, there are hundreds of thousands of mid-market companies, and also unlike large enterprises, growing businesses are much less invested in cyber security solutions. Why? For one thing, mid-market security budgets generally can't support the level of investment required to purchase most of the enterprise-grade security solutions available today.

For another, the security marketplace hasn't expanded quickly enough to address all the new attack vectors that have emerged and become popular during the pandemic.

Research and development is costly, so security companies are developing new security solutions for the customers who can pay for them – the large enterprises. Until the market moves and the security solutions trickle down to the reach of the next tier of companies, mid-sized businesses are in serious trouble.

“The security marketplace hasn't expanded quickly enough to address all the new attack vectors that have emerged and become popular during the pandemic.”

Quantifying the Threat Level Growing Businesses Are Facing

Coro's ground-breaking research report, spanning two years and based on examination of over 4,000 mid-market companies, reveals that mid-sized companies are getting hit by cyber attacks with a frequency that is now on par with large enterprises.

Covid Era Spawns Attack Vectors

While it's true that some of the most widely publicized cyber assaults were carried out against some of the biggest companies, mid-sized companies now provide an equally target-rich environment and are much more vulnerable to, and victimized by, the nefarious activities of bad actors.

In fact, compared to the pre-pandemic era when cyber attacks were largely limited to malware and phishing attacks, the scope and scale of cyber attacks have skyrocketed over the course of the **past two years**: In **2019**, mid-market businesses were seeing on average the following numbers of attacks by available vector:

Traditional Pre-Covid Attack Vectors

Email Phishing general	3,129
Email Phishing Via Cloud Apps	
Email Phishing Based on Role	
Malware Via Email	
Maleware Via Cloud Share	
Malware Via Endpoint	1,813
Wi-Fi Phishing	
Account Takeover	
BOT Attacks Via Credential Theft	
Insider Threats	207
Regulated Data Leakage	295
Unauthorized Activities	207
Abnormal Admin Activities	96
Abnormal Login	533
Dormant Account Activity	93
Total Attacks	**6,372**

Attacks Keep Increasing Across All Vectors

Then, starting in 2020 and continuing throughout the pandemic, new attack vectors emerged and volume across all attack vectors increased, resulting in nearly a **275% increase in attacks** over the course of 2020. When we layer in the actual data for the first ten months of 2021 and include extrapolated data for November and December of 2021 (extrapolated from the actual increases in attacks in November and December of 2020), we can anticipate a **whopping 490% increase in cyber attacks** from the start of the pandemic to the end of 2021!

	Traditional Pre-Covid Attack Vectors	2020 Attack Vectors	2021 Attack Vectors
Email PhishingGeneral	3,129	4,501	8,094
Email Phishing Via Cloud Apps		1,427	2,649
Email Phishing Based on Role		1,778	3,193
Malware via Email		840	1,295
Maleware via Cloud Share		456	821
Malware via Endpoint	1,813	2,257	3,512
Wi-Fi Phishing		3,289	6,666
Account Takeover		401	532
BOT Attacks via Credential Theft		983	2,342
Insider Threats	207	219	290
Regulated Data Leakage	295	312	413
Unauthorized Activities	207	222	298
Abnormal Admin Activities	96	106	146
Abnormal Login	533	594	828
Dormant Account Activity	93	105	148
Total Attacks	**6,372**	**17,490**	**31,227**
Percent Increase Over 2019:		**274%**	**490%**

> “We can anticipate a whopping 490% increase in cyber attacks from the start of the pandemic to the end of 2021!”

A Detailed Look at the Numbers by Sector

1. Total Cyber Attacks by Sector

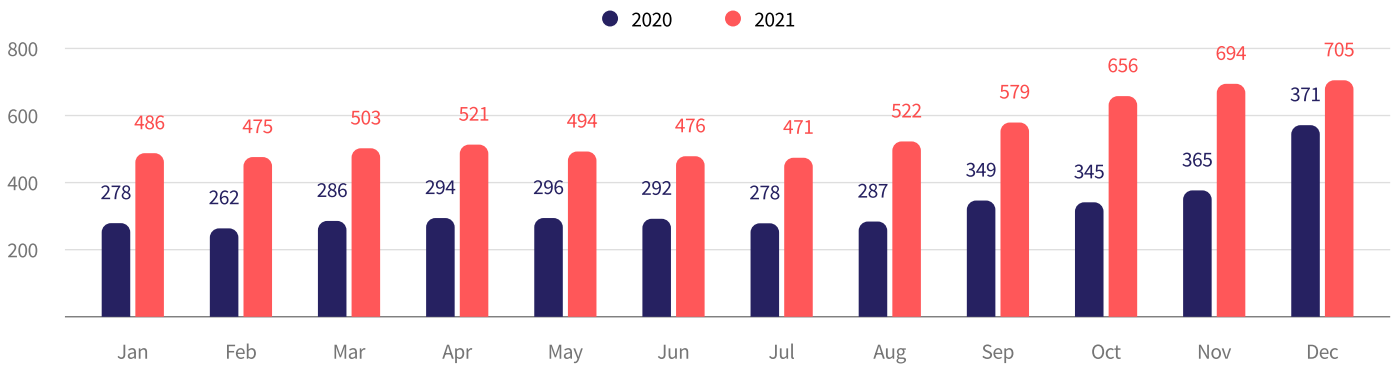
Between 2020 and 2021, attacks on mid-sized businesses in each sector grew by at least **50%**:

A. Attacks against mid-market companies in Retail, Manufacturing, and Professional Services nearly doubled over this time period, increasing between **86% and 90%**.

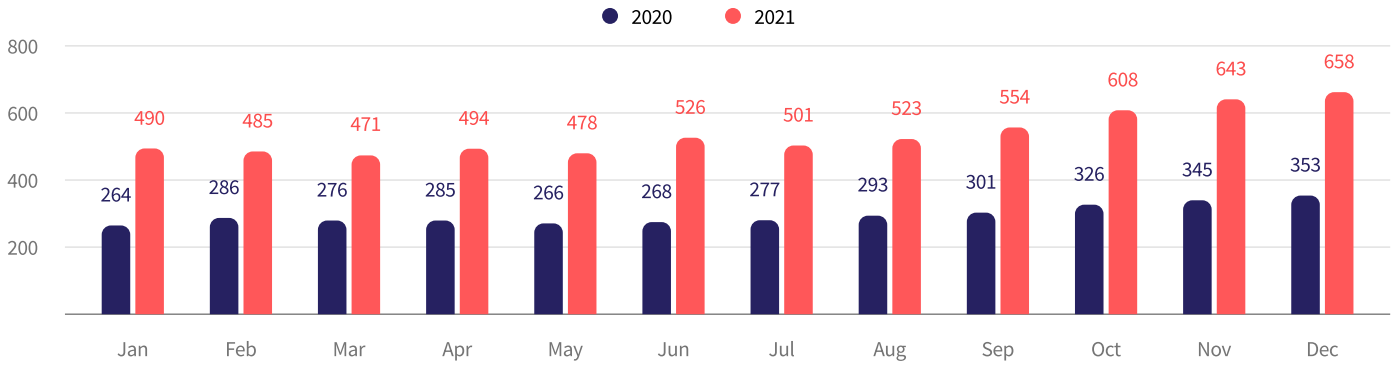
B. Attacks in Healthcare and Transportation stand out as the fastest growing sectors, increasing by more than **125%** between October of 2020 and October 2021.

C. Education, while seeing more modest increases in number of attacks month-over-month and year-over-year, saw a greater volume of attacks on average in any given month than companies in most other sectors.

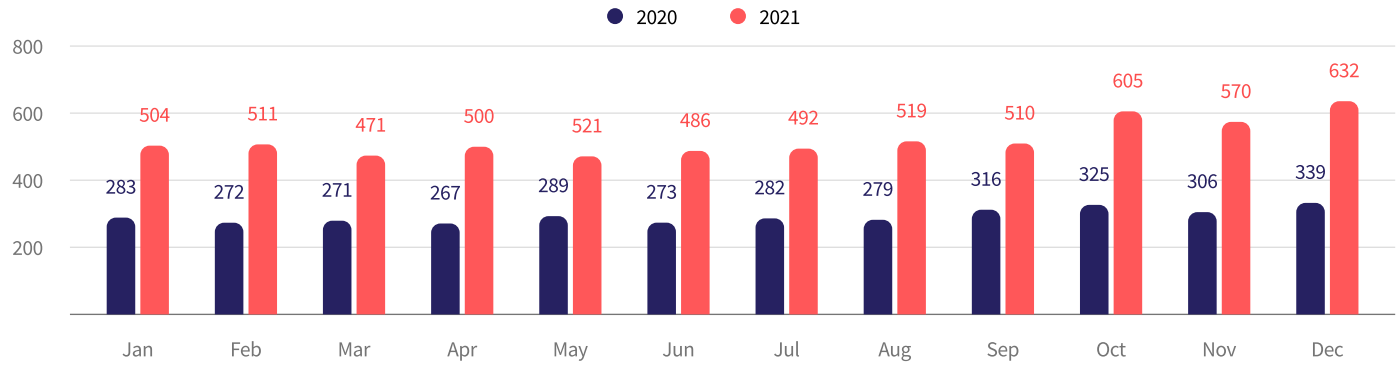
Increasing Attacks in Retail Sector, 2020 to 2021



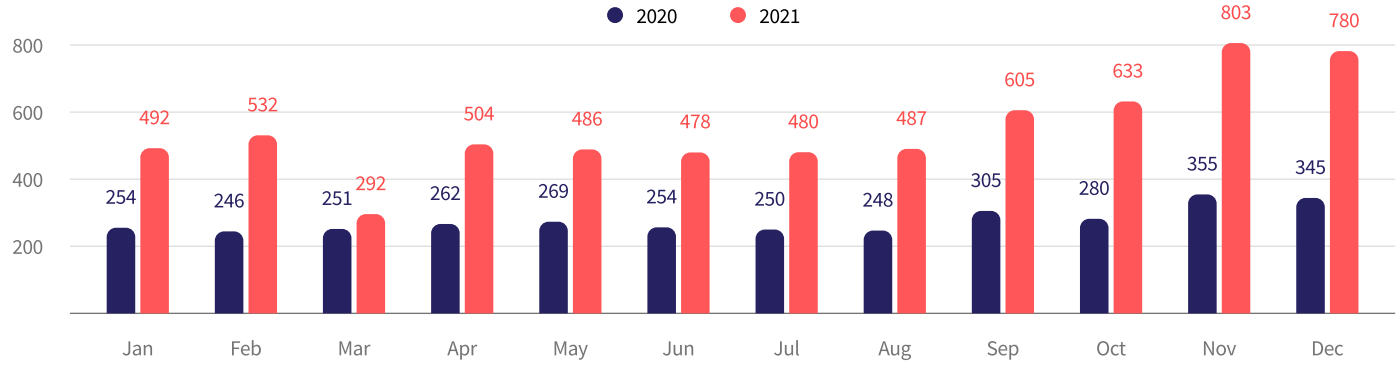
Increasing Attacks in Manufacturing Sector, 2020 to 2021



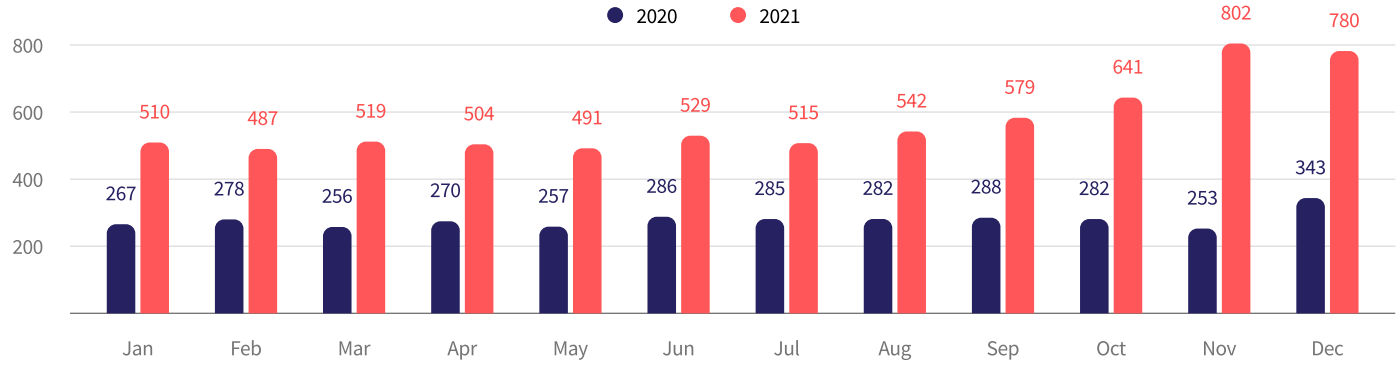
Increasing Attacks in Professional Services Sector, 2020 to 2021



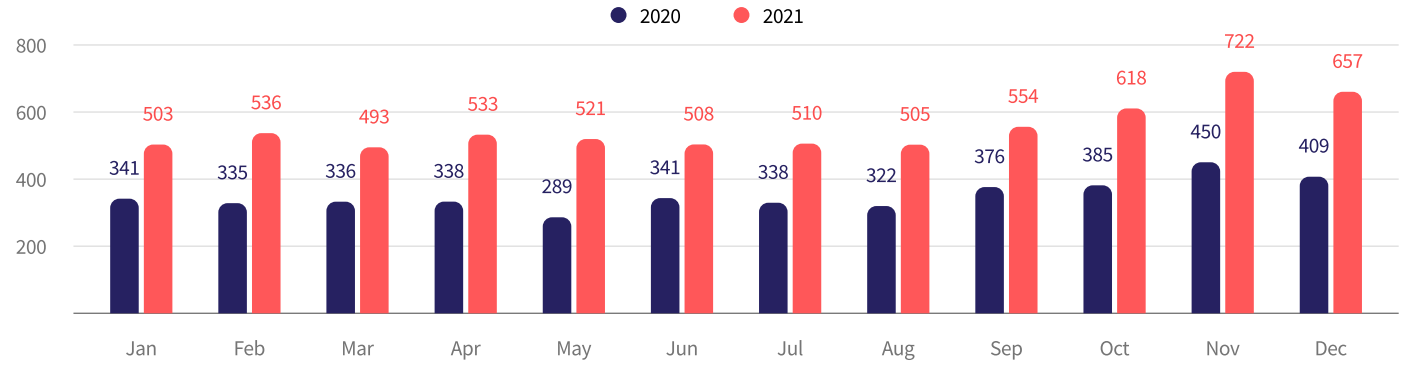
Increasing Attacks in Transportation Sector, 2020 to 2021



Increasing Attacks in Healthcare Sector, 2020 to 2021



Increasing Attacks in Education Sector, 2020 to 2021



2. End-of-Year Escalation in Attacks

Not only are attacks on mid-market companies increasing year-over-year, but mid-market vulnerability increases notably during the final four months of the year. Between the back-to-school and holiday seasons, when we anticipate a robust increase in consumer spending, we would expect to see increases in commerce-related sectors, including Retail, Manufacturing and Transportation. However, every sector experienced a significant jump in attacks in the last four months of 2020 and also to date in 2021.

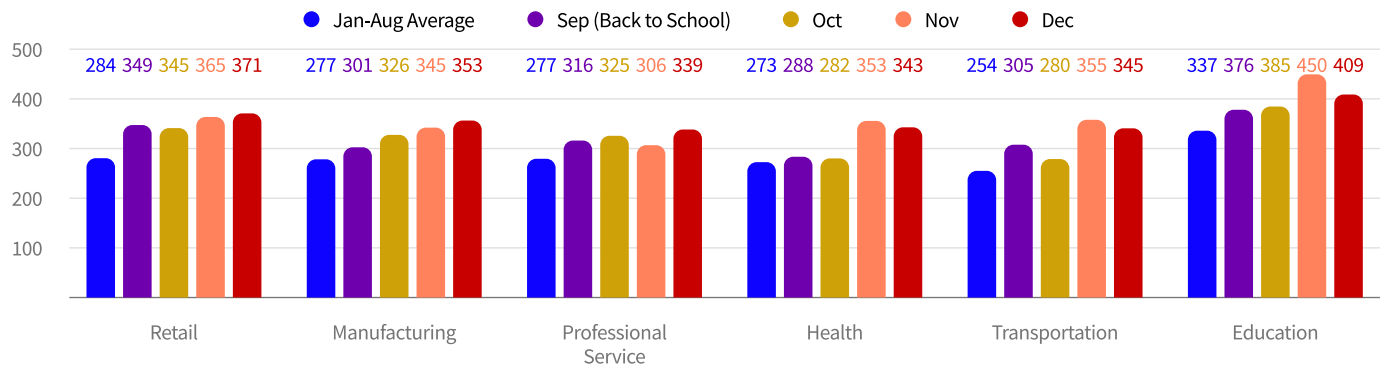
This is a strong indication that cyber warfare automation is behind the spikes. With the accessibility of malware and the affordability of compute power to scale infiltration efforts, automated bot attacks are now able to extend beyond the limited number of large enterprises to reach the vast middle tier of growing companies.

Mid-market businesses not only offer a vast greenfield opportunity for cyber criminals, with the shortage of security solutions being marketed to growing companies, the ground for cyber incursions is extremely fertile.

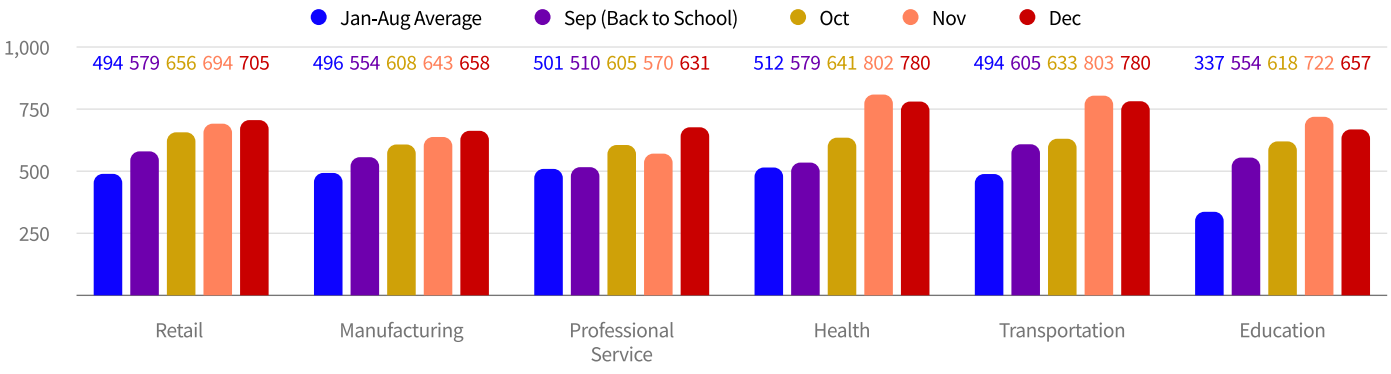
By end-of-year 2020, attacks against mid-market companies in each sector have increased between **22% and 36%** compared to the average number of attacks in the first eight months of 2020.

Using the month-over-month percentage increase in attacks for October, November, and December 2020, we can extrapolate the expected increases for November and December of 2021. Based on the actual data we've seen for September and October we can anticipate another significant increase in attacks over the last four months of the year as compared to the first eight.

End-of-Year Attack Escalation, 2020



End-of-Year Attack Escalation, 2021



3. Distribution over Attack Sophistication

We already know that the near **500% increase** in attack volume today as compared to before the start of the pandemic is causing an equivalent increase in the likelihood that an attack against a mid-market company will be successful. But that's not the only factor putting mid-sized businesses at greater risk: Changes in attack sophistication are acting as a multiplier and pushing the likelihood of an attack being successful even higher.

A. Naïve Attacks

Those attacks involving no attempt to differentiate one target from another and which require brute force to execute – comprised **86%** of all cyber attacks against the mid-market sector in 2020. But in 2021, the proportion of naïve attacks to more sophisticated schemes dropped precipitously from **86% to 68%**, revealing bad actors' ability to scale more intelligent assaults against a broader range of organizations.

B. Targeted Attacks

Targeted attacks, which focus on a specific role or persona within an organization, increased from **12% to 26%**.

C. Customized Attacks

Attacks which target companies that match a cyber attacker's ideal target profile, grew from **1% to 4%**.

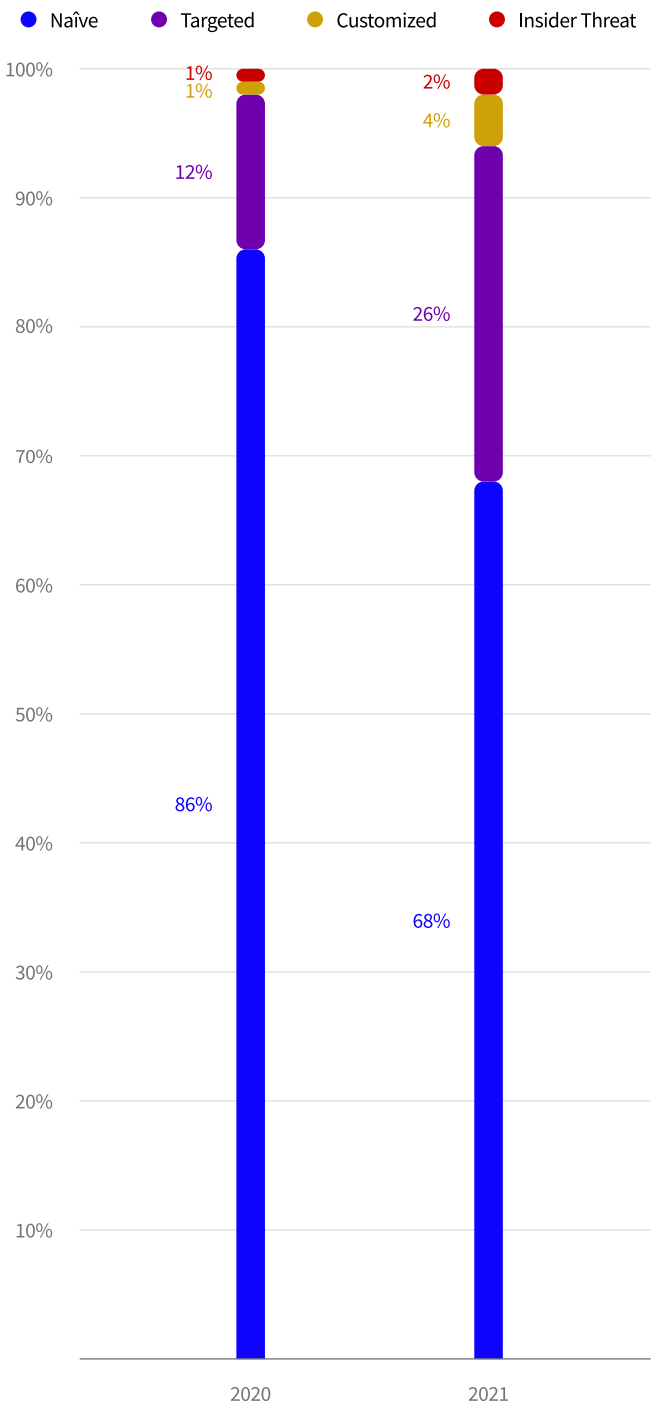
D. Insider Threats

Insider threats doubled from **1% to 2%**.

An increase across the board in attack sophistication is an indicator that more intelligent approaches are more effective. While the above percentages for customized and insider threat attacks appear small today, the rates at which they are expanding – **4x and 2x** respectively – are what is most alarming, especially given that these threat types are the most lethal when successful. These sharp increases do not bode well for 2022 and beyond.

The shift to higher quality assaults is further indicative of cyber criminals' expanded capabilities to launch attacks at scale. It won't be long before naïve attacks are the minority of cyber attack types and a negligible contributor to the overall threat landscape.

Distribution of Attack Sophistication, 2020 to 2021



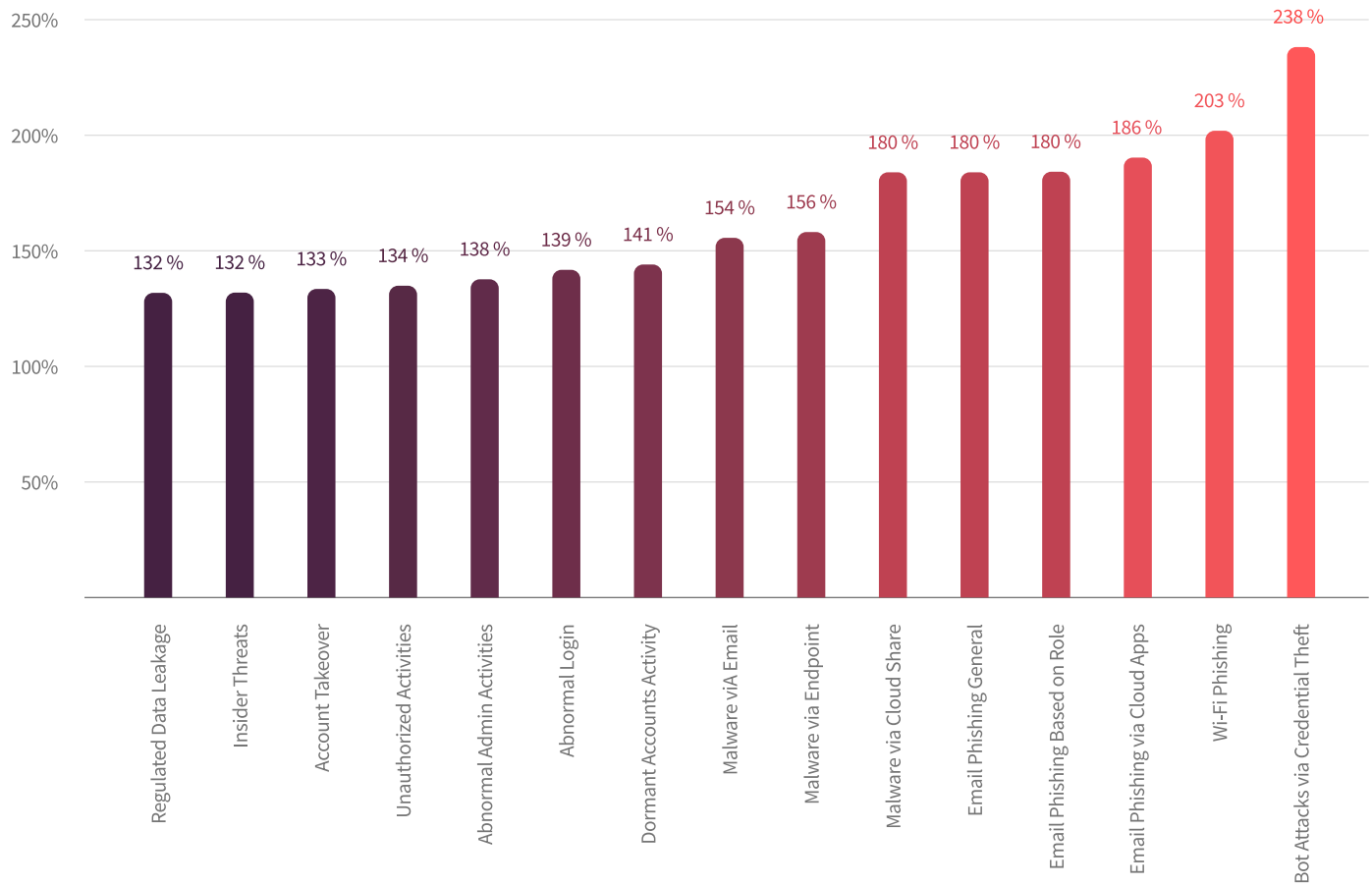
4. The Expansion of Attack Vectors

As noted earlier, before the pandemic hit, cyber attacks mostly fell into one of two categories: malware attacks or phishing attacks. But now, we've seen big increases across every type of assault from 2020 to 2021. The number of times a given attack vector was used more than doubled across every attack vector. WiFi phishing and bot attacks **more than tripled** over the course of the year.

Bot attacks, Wi-Fi phishing, email phishing, malware via cloud applications, malware via email, malware via endpoints, and insider threats all increased by more than 150% between 2020 and 2021.

> **The frequency of WiFi phishing and bot attacks more than tripled from 2020 to 2021.**

Growth in Cyber Vectors, 2020 to 2021

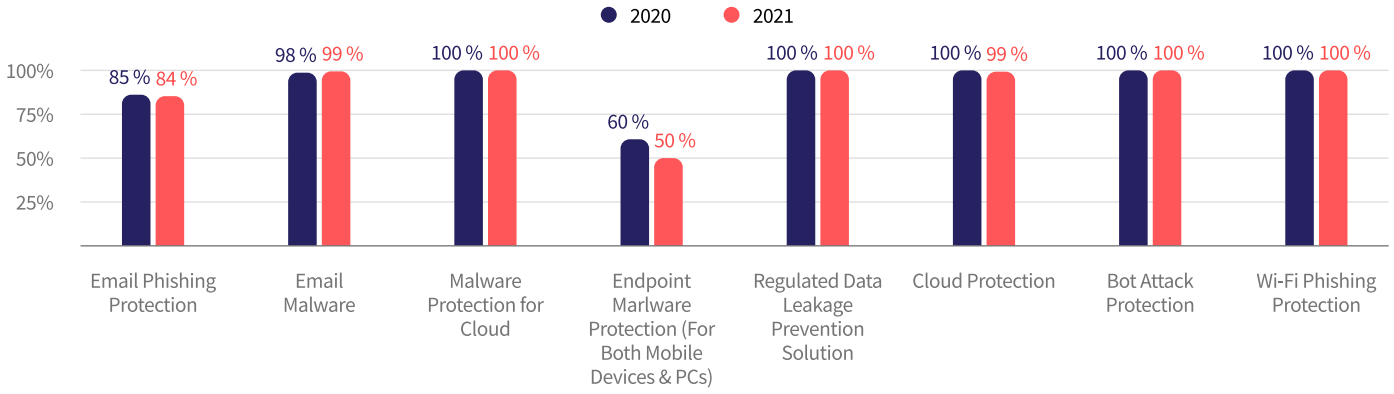


5. The Utter Lack of Protection within Mid-Market Companies

In sharp contrast to the expansion of attack vectors and the increasing frequency of attacks in each vector, we see that mid-sized companies are not positioned to defend themselves against the cyber onslaught. Exceedingly few mid-sized businesses have security solutions in place, leaving the vast majority in the dark when it comes to detecting attacks and completely defenseless when it comes to warding them off.

Only endpoint malware protection and email phishing protection, the two attack vectors that predated the onset of the pandemic, show any traction in terms of being solutions that mid-market businesses are employing with any regularity. Even so, neither of those was adopted by even half of the companies in the sample set. The rest were at or near 0% deployed.

Mid-Sized Companies Lacking Security Solutions by Solution Type, 2020 & 2021

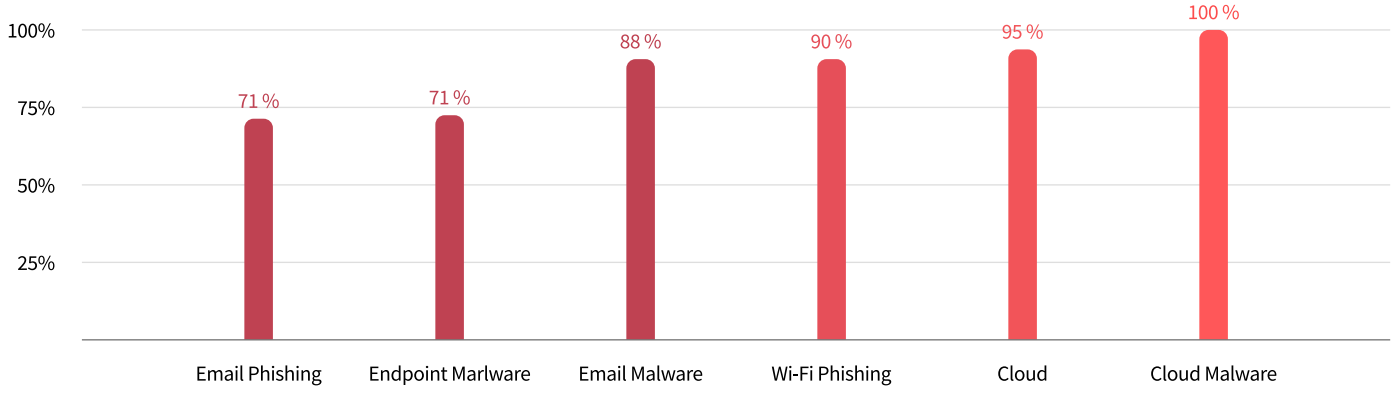


6. Frequency of Misconfiguration of Deployed Security Solutions

Now that it has been firmly established that mid-market businesses very rarely have security solutions in place, we need to turn our attention to those rare instances where mid-sized companies do have security solutions deployed to complete the picture that illustrates how ill prepared mid-sized businesses are to shield themselves from the rising storm of cyber warfare. Even when security solutions are in place, chances are far better than not that the deployed solution will be misconfigured, thereby compromising the protection the solution was engineered to provide.

Of the few instances of security solutions being in place at mid-market companies, at least 70% of all deployments are misconfigured, leaving the business with compromised security capability at best.

Frequency of Security Solution Misconfiguration 2021



Conclusions

The accelerated digital transformation forced on companies as they struggled to respond to the stifling effects of the COVID-19 pandemic has created a security inequality that heavily favors the cyber attacker over the mid-market business. The ability of bad actors to scale their attacks in such a target-rich environment without the availability of a broad selection of security solutions is a near-complete failure of the security industry.

1. Growing companies that are under heavy attack from cyber criminals aren't prepared to deal with the barrage. All sectors are exposed; no industry is safe. Without a fundamental shift by the security industry to address the distinct security needs of mid-sized businesses, an economic calamity is entirely possible and perhaps even probable.

2. The availability of malware and the affordability of compute power to support payload delivery is commoditizing and automating cyber attacks, making cyber crime an increasingly common occurrence for growing companies and an incredibly lucrative pursuit for cyber criminals.

3. Attacks escalate during the back-to-school and holiday seasons, not just against commerce-related industries but across all sectors. This elevation in end-of-year attacks establishes new baselines for the following year both in terms of attack volume and the likelihood of a breach.

4. The security deficiencies within mid-market businesses stemming from a near-total absence of point security solutions engineered for mid-sized companies are exacerbated by a skills gap within these companies' IT organizations in terms of the expertise needed to properly deploy and configure the few point security solutions that growing companies have invested in.

5. In order to be protected against the ever-expanding threat landscape, mid-sized businesses need to piece together the same security infrastructure as the large enterprises have constructed from the building blocks available in the security industry marketplace. At this point, however, mid-market companies are neither financially nor technologically equipped to do so.

6. It is impossible to overstate the severity of the security crisis the mid-market sector is currently facing. As the trends continue through the end of 2021 and into 2022 and beyond, the urgency is only going to increase. Security vendors must step in to fill the void with affordable and effective security solutions that will give the hundreds of thousands of mid-sized businesses the opportunity to survive and thrive in a business world infested with bad actors who will spare no expense in exploiting them.

Growing companies that are under heavy attack from cyber criminals aren't prepared to deal with the barrage. All sectors are exposed; no industry is safe.

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.