KnowBe4
Human error. Conquered.

REPORT

The 2018 Threat Impact and Endpoint Protection Report

There's no greater security worry than the fact that so many organizations today, despite their best efforts, are still falling prey to ransomware attacks, cryptojacking infections and data breaches. Cybercrime organizations have a clear vision of how they can make money, by either taking your data and selling it, holding it for ransom, or stealing CPU cycles.

In 2017, Ransomware was a multi-billion dollar business, seeing the number of new ransomware variants continually grow quarter over quarter. The increase in ransomware-as-a-service provides everything from a turnkey to a completely customizable solution has made it even easier for those with little or no developer know-how to get into the game of holding organizations for ransom.

Data breaches are seeing their own forms of "success" as well. Despite the presence of security, organizations are still falling victim to data breaches with record counts into the hundreds of thousands, and the overall costs reaching well into the millions.

So, how are these threats continuing to grow at a time when security is at an all-time high?

With two-thirds of malware attacks coming from phishing, according to a recent GTIC Threat Intelligence report, the volatile combination of your users, their endpoints, email, and malware should be at the forefront of your organization's security focus, if you are to prevent ransomware attacks and data breaches. It's reasonable to assume most (if not all) organizations are concerned about protecting themselves from malware-based attacks, and are taking steps to address the potential threat. The question is what are they specifically doing and how effective will those measures be at stopping the threat.

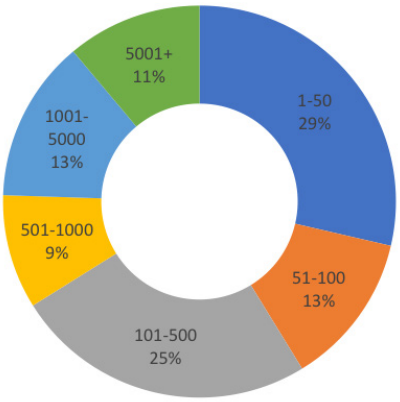
"In 2017, Ransomware was a multi-billion dollar business, seeing the number of new ransomware variants continually grow quarter over quarter."

To find out, KnowBe4 surveyed over 500 organizations about the current state of their endpoint protection, whether they'd been a victim to ransomware and/or external attacks resulting in data breaches, what was the impact, and what they did to remediate the attack.

In this report, we'll begin by looking at the state of two specific attack types – ransomware and external malware attacks resulting in data breaches – working through the various impacts each of those attacks has on an organization. We'll then take a look at the endpoint protection in place in an effort to understand what solutions are aiding in the fight against all forms of malware attacks – and which of those are truly effective.

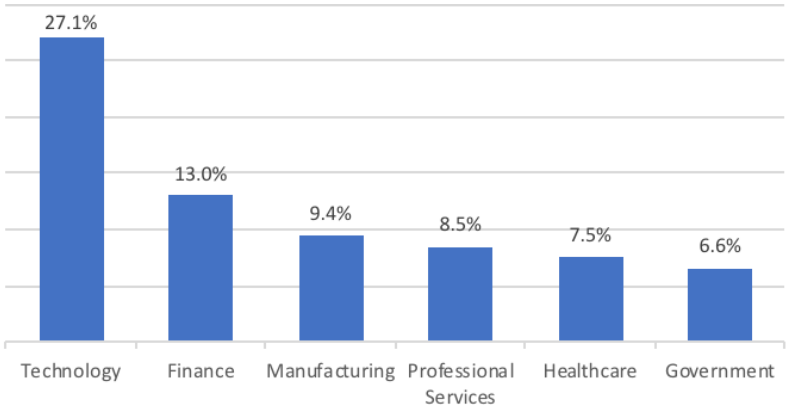
About Our Respondents

Over 500 organizations participated in this year's report, representing over 50 countries, of which the United States had the greatest representation (74%).



Response by organization size (shown at right) provided us with a solid representation of organizations of every size. Organizations ranged from the small business (with less than 50 users) up to the enterprise (with more than 5000 users).

The top 6 industry verticals represented in this report are shown below. The other industries included Energy, Education, Transportation, and more, each contributing less than 6% of the total respondents.



Top 6 Industry verticals represented in this report

The Impact of Ransomware

It's estimated the business of ransomware raked in over $5 Billion in 2017, according to a recent Cybersecurity Ventures report. With the number of ransomware samples materially increasing, according to McAfee's Quarterly Threat reports, it's evident this is a problem that's not going away.

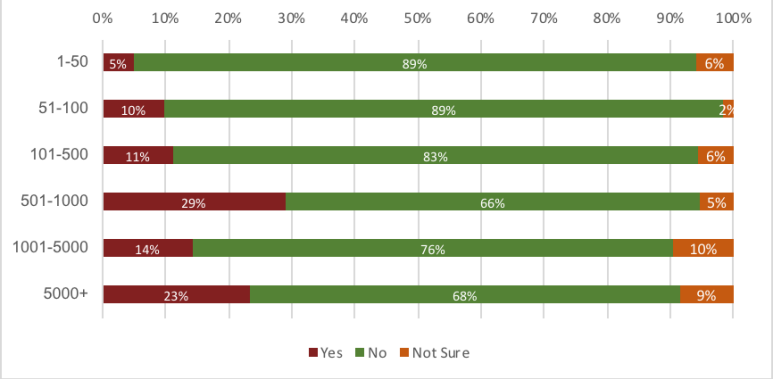
In this survey, we sought to understand each of the impacts a ransomware attack has on organizations, beginning with who's at risk, what's being held for ransom, what does it take to remediate, and how does it impact the organization. In the following pages, we'll walk through each impact ransomware has on your business, providing a detailed look into what is truly at risk when an attack hits.

"13% of businesses on the average experienced a ransomware attack within the previous 12 months."

Ransomware Impact – Who's at Risk?

Regardless of your business size or industry vertical, every organization today is a potential victim of ransomware. The widespread, opportunistic nature of many attacks, mixed with an improvement in phishing-based social engineering, has led cybercriminals to take the "shotgun" approach, targeting every organization for whatever ransom can be paid.

We've seen a material improvement in organization's abilities to fend off ransomware. This year, 13% of businesses on the average experienced a ransomware attack within the previous 12 months. This is a decrease from last year's average of 33%. Considering malware is on the rise, according to security vendors like McAfee and Symantec, this decrease implies that organizations are being more successful at strengthening their security stance and stopping ransomware before it impacts the organization.



The % of organizations experiencing a ransomware attack within the last 12 months. (by org size)

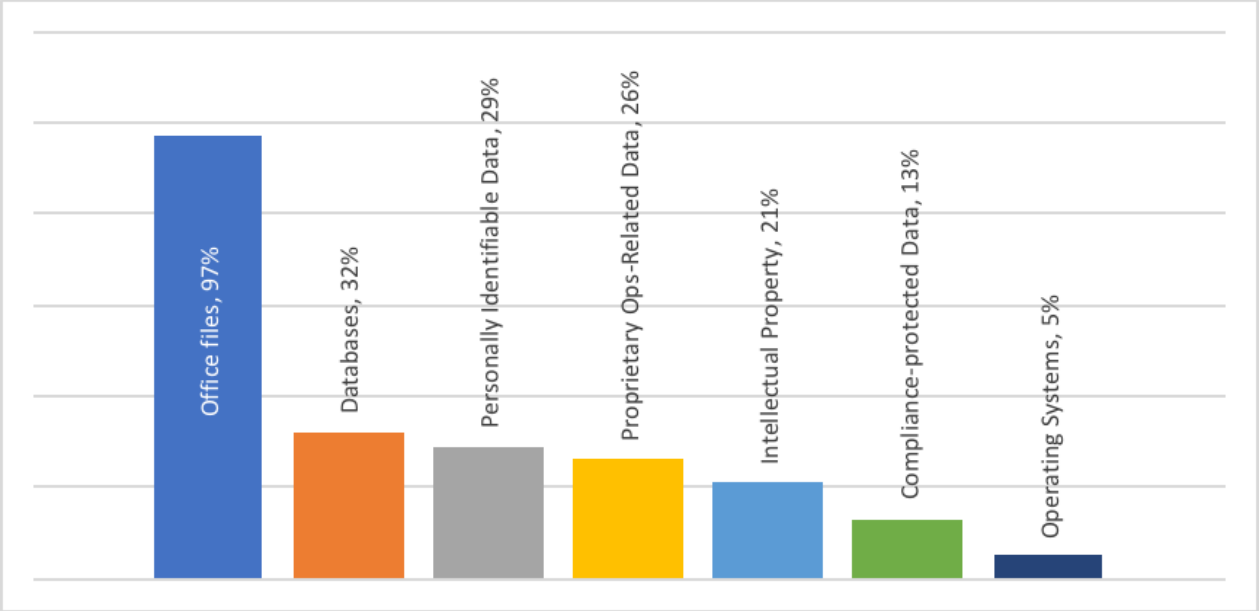
Midmarket organizations were hit the hardest at 29% (as shown above), almost matching last year's overall attack average. Organizations in the manufacturing, technology, and consumer-focused industries experienced the most ransomware attacks (both manufacturing and technology were in the top three in last year's report as well).

Ransomware Impact – Systems & Data

The more pervasive ransomware can be within an organization, the higher the likelihood of the criminal organization to obtain a paid ransom. We found that an average of 16 workstations and 5 servers were affected in a given attack. This is a material increase from last year's average of just 6 workstations and 2 servers. There were only 7 instances found in our research of successful ransomware attacks affecting a single

endpoint. As shown below, only 5% of ransomware attacks involved the encryption of an entire operating system.

The more critical the data is to the organization, the higher likelihood of the ransom being paid. But what constitutes importance is different for each organization. So, we asked organizations what data was encrypted as a result of the attack. As shown below, the overwhelming majority (97%) of encryption impacted common Office-type files. However, the kinds of information held within those files included critical, sensitive, and proprietary data – all spelling a potential payoff for the ransomware authors.



The various kinds of data that was encrypted during the ransomware attack

Ransomware Impact – the Ransom

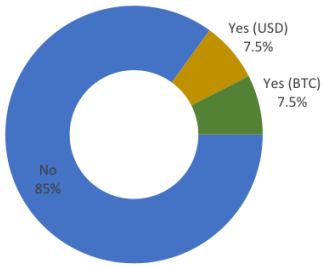
The notion of whether to pay the ransom or not is generally determined by just three factors:

1) What data specifically was encrypted?
2) Do we have backups / how long to recover?
3) How much is the ransom?

It's a cost-to-value determination. If the data or systems affected are easily replaceable, most organizations skip paying the ransom and go straight to remediation activities. But if the data is important, it's simple math of "will it cost more to recover manually, or is it better to just pay the ransom?". There is no right answer – other than to proactively prepare and have backups of all critical data and systems. Then, and only then, are you truly prepared.

As shown at the right, the majority of organizations today (85%) do not pay the ransom.

Ransoms in USD ranged from $500 to $1 Million (making it difficult to cite an average ransom), while those organizations paying ransoms in bitcoin provided very specific details around the number of bitcoins and the equivalent dollar value. Most bitcoin-related ransoms were 1-3 bitcoins, with the bitcoin value (at the time of ransom) ranging from $600 to $11,000, giving us a ransom range of $600 - $33,000.



% of organizations paying the ransom and how it was paid

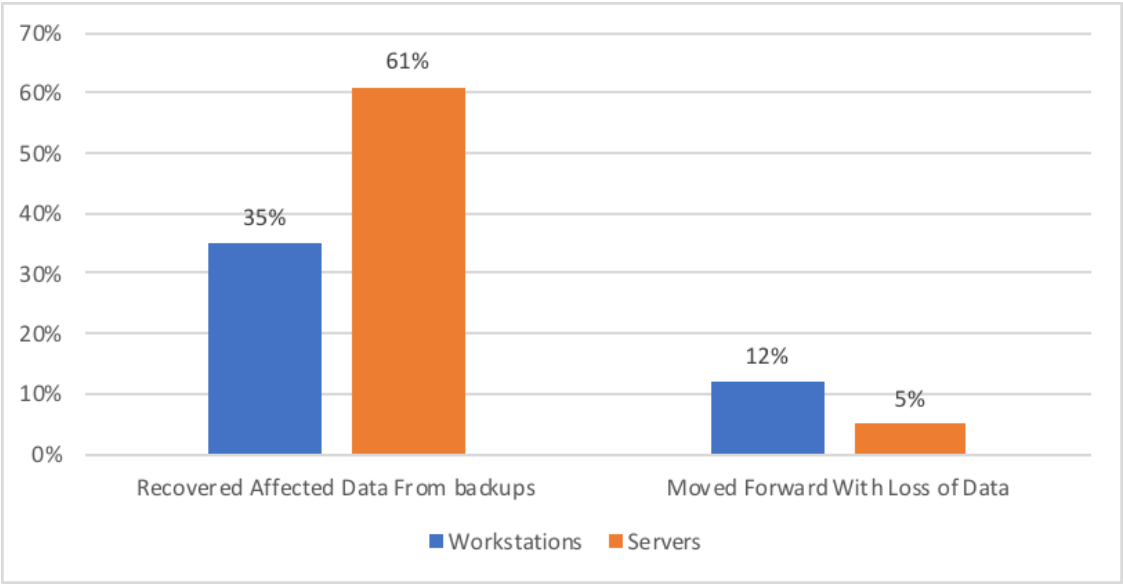
Ransomware Impact – Remediation

Beyond the question of whether or not to pay the ransom, there still remains the need to remediate the damage done to operations. Your encrypted data obviously needs to be returned to a known-good state – that's step 1. But, with everyone focused on the encrypted data, often overlooked is the fact that ransomware is malware – and, so, the affected endpoints also need to be addressed.

So, how are organizations remediating a ransomware attack?

Affected Data

Organizations today are realizing the value in maintaining backup copies of their data, with 61% of organizations recovering server data from backups, and a surprising 35% recovering workstation data, as shown below.

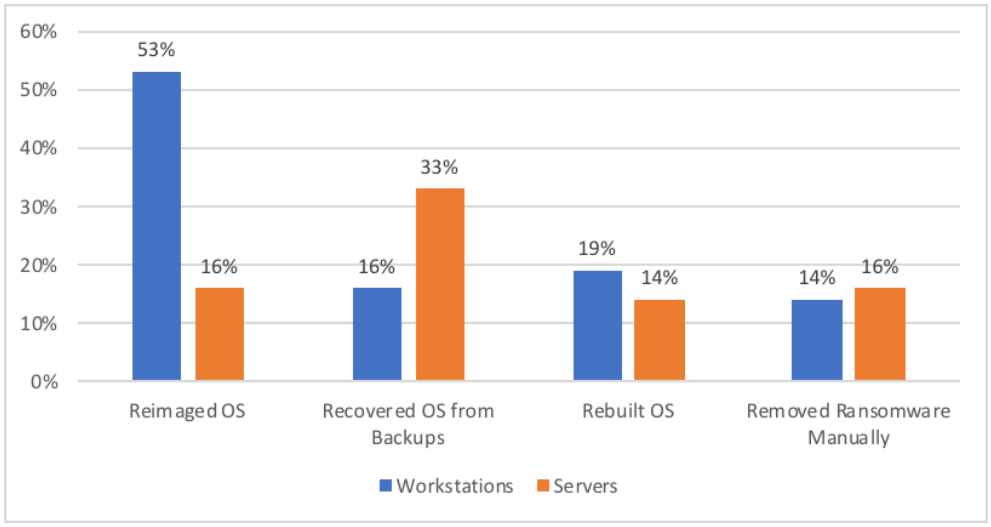


How organizations recovered their encrypted data

It's still evident that less important data resides on workstations, as the % of organizations willing to simply move forward and take the loss on a workstation is more than double that of servers.

Operating Systems

Once infected with ransomware, you still need to eradicate the malware from the endpoint. There are a number of ways to accomplish this. As shown below, IT organizations are far more apt to take the route of reimaging workstations and recovering servers from backup.



How organizations eliminated ransomware from the endpoint

Ransomware Impact – Time Spent

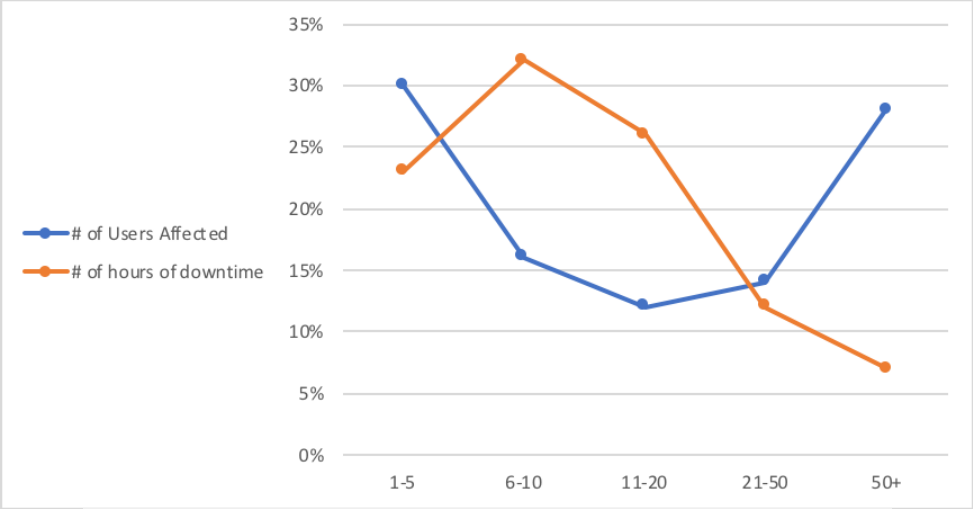
All this remediation takes IT away from their regular duties, planned initiatives, and ongoing projects. Given the average infection involving 16 workstations and 5 servers, we sought to find out how much time was spent on each response task. As shown above, multiple techniques were used in a given attack response. Below you can see the average number of hours each response task took.

ID Infected Machines	Reimage OS	Recover OS	Rebuilt OS Manually	Recover Affected Data	Remove Ransomware Manually
9 hours	8 hours	8 hours	6 hours	12 hours	5 hours

Number of hours needed for each remedial response action

Ransomware Impact – Users & Downtime

Another way to look at the impact of a ransomware attack – beyond the time IT takes to remediate – is how users and productivity is affected. The average number of users impacted in a given ransomware attack was 22, with an average downtime of 14 hours. It was interesting to note a bell curve-like response around the number of users affected – in the majority of incidents, the ransomware infection had little user impact (1-5) or had a material impact (50+). Those organizations with the most hours of downtime tended to be the mid-market (1000-5000 employees) and enterprise (5000+) organizations.



Counts of users affected and hours of downtime as a result of a ransomware attack

It should be noted that there is no direct correlation between the number of users and the hours of downtime (e.g. 50+ users doesn't necessarily equate to needing 50+ hours).

The Impact of External Attacks / Data Breaches

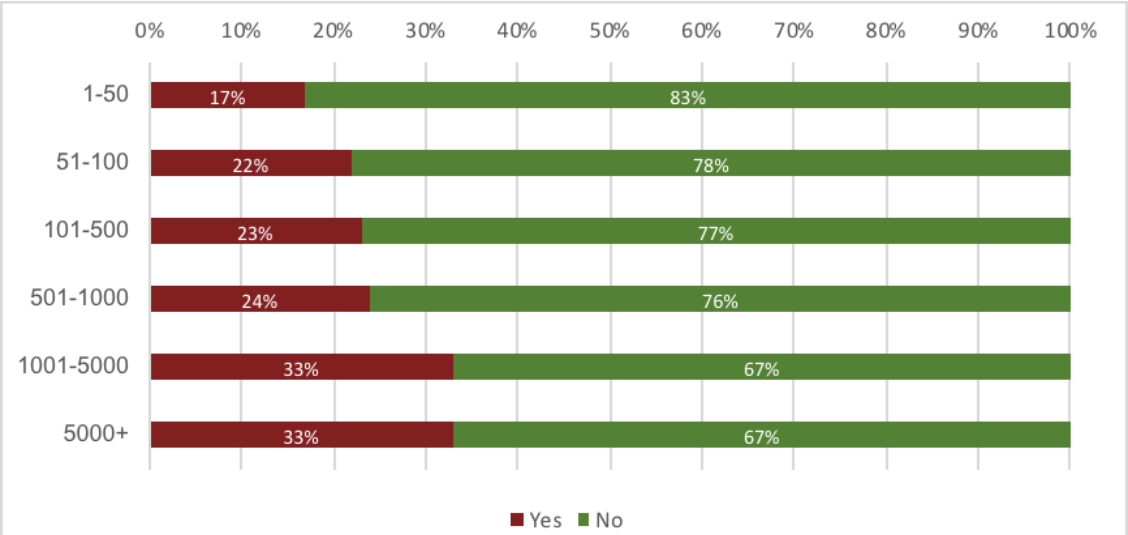
Next to ransomware, organizations today need to be vigilant against data breaches. With 75% of them being committed by external parties, according to the 2017 Verizon Data Breach Investigations Report, and with the #2 attack method used being malware, organizations need to expect endpoint-focused attacks. According to a recent Ponemon study, The Cost of a Data Breach, the expectation for all organizations is that there is a 27.7% likelihood of a data breach within the next two years.

But what's the reality of an external attack, and the resulting potential data breach?

In this survey, we sought to understand each of the impacts an external attack as part of a data breach effort has on organizations, beginning with who's at risk, what does it take to remediate, how many records are stolen, and how does the attack impact the organization. In the following pages, we'll walk through each impact an external attack has on your organization, providing a detailed look into what truly at risk when you're under attack.

External Attack Impact – Who's at Risk?

Like ransomware attacks, external attacks using malware leverage the same opportunistic nature. With financial gain as the number one motive (according to the Verizon 2017 DBIR), it makes sense that no business is safe from a potential attack. On the average, 24% of all organizations have experienced an external attack in the last 12 months, with consumer-focused businesses, non-profits, technology, and professional services sectors hardest hit.



The % of organizations experiencing a malware-based external attack within the last 12 months. (by org size)

The increase in the percentage of organizations experiencing an attack as the size of organization increases shouldn't come as a surprise; there are more endpoints creating a greater potential for infection, more data sets that may be of external value (think business units, subsidiaries, branch offices, etc.), and an overall greater opportunity for financial gain for the attacker.

It's also interesting to note that only 28% of those organizations experiencing an external attack also experienced a ransomware attack in the last 12 months.

External Attack Impact – Systems

Usually when hearing about an attack, the context is presumed to be a single attempt to infect one endpoint brought to success or failure. But, the reality is attacks today cast a wide net in an attempt to maximize the chances of gaining control over one or more endpoints within an organization.

We found that the number of systems impacted during an external attack was far more than a single endpoint – the average malware-based external attack impacts 5 workstations and 1 server during a single attack.

External Attack Impact – Remediation Time Spent

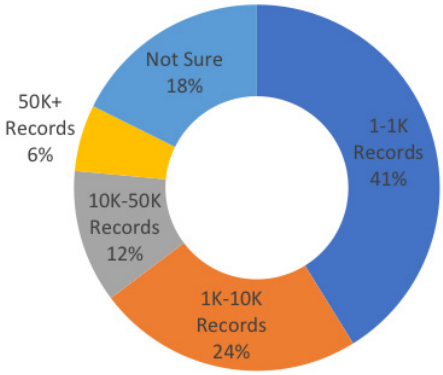
Like responding to ransomware, IT needs to identify infected systems, eliminate the malware, bring all endpoints into a known-good state, fix security gaps that allowed the successful attack, as well as to identify whether data has been exfiltrated. As shown below, IT spends slightly less time addressing malware that may be used in a data breach, than ransomware. This is likely due to the added steps of needing to recover the ransomed data and/or systems back to an operation state.

ID attack entrance point & method	ID all machines infected with malware	Reimaged or recovered endpoint OS	Locked down vulnerabilities, exploits, security gaps, etc.	Identified accessed or exfiltrated data
4 hours	5 hours	6 hours	7 hours	6 hours

Number of hours needed for each remedial response action

External Attack Impact – Data Breached

Of those organizations citing they had experienced a malware attack, 82% of them stated the external attacks resulted in no identifiable breach. But, of those with documented data breaches (shown at right), we saw a wide range of records breached. The majority (41%) saw less than 1000 records breached, with the average number of records being slightly higher than 15,000. Those organizations with the highest record counts – which included record counts as high as 100K – tended to lean towards mid-market and enterprise-sized organizations.



Breakout of record counts involved in a confirmed data breach

Preventing Attacks: Focus on the Endpoint

Cyber attacks, like any business, are looking for a way to be the most successful, while putting forth the least amount of effort and resources. Which is why a majority of malware now use evasive techniques to avoid detection by email scanning, sandboxing, and AV solutions, looking to leverage ways to bypass security controls and find their way directly onto your endpoints. So, it's critical for organizations to realize that malware will find its way to your endpoints – making them your last line of defense.

Every organization puts some measure of defense in place to keep malware at bay. There are a number of tactics used by IT organizations today:

- **Rely on security-focused software –** Fighting evil technology with good technology has been a staple in most IT security strategies. We saw a large investment this year in multiple endpoint protection solutions to create a layered defense (more on that later).
- **"Break Room" Training –** We've all done it; group everyone in a room once a year and cover the current state of phishing, malware, external attacks, and ransomware, hoping employees will remember to remain vigilant when it comes time for them to not click that suspicious email link. It's a method filled with good intent, but a lot changes in the art of the attack within a year's time.
- **Monthly Security Training –** Usually done via email or using videos, users can educate themselves on topics related to ransomware, phishing, and other threats – and how to not become a victim. Keep in mind they aren't forced to participate.
- **High-Risk Employee Phishing Testing –** These infrequent tests focus on employees with access to more sensitive or critical data within the organization. They are subject to a mock phishing attack, with remedial training for those that fail the test.
- **Build a "Human Firewall" with Security Awareness Training and Testing –** These organizations rely on the user to thwart ransomware. It's accomplished by first baselining how Phish-prone the organization is, mandating all employees continually participate in on-demand online training to stay current, followed by monthly year-round automated phishing attacks to test users.

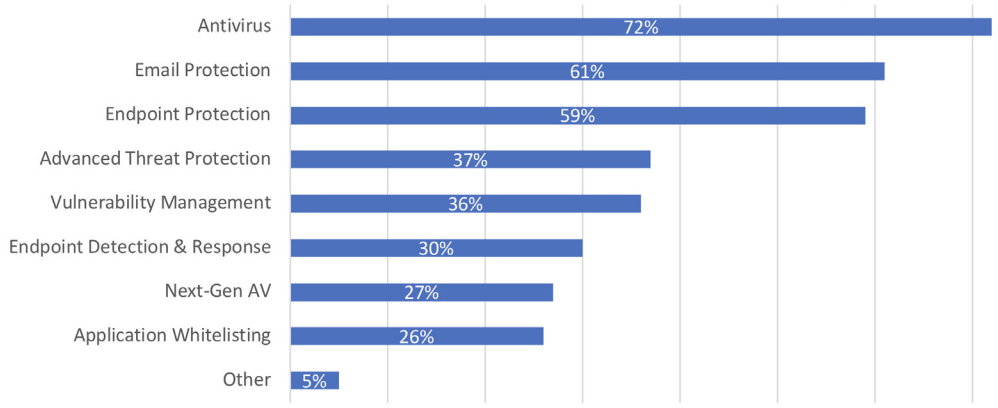
We found that organizations are clearly reliant on security software (shown below), with user education, phishing testing, and security awareness training & testing all gaining ground as part of the overall security strategy.

Solution	Don't Do	Somewhat Implemented	Mostly Implemented	Completely Implemented
Security software that filters out ransomware	3%	9%	32%	57%
Quarterly/Annual "Break Room"-style training	35%	30%	17%	19%
Monthly security videos / emails	24%	24%	22%	30%
Phishing testing of high-risk employees	24%	19%	18%	39%
Security Assessment Training for all employees with frequent phishing attack testing	24%	22%	20%	34%

% of organizations implementing anti-ransomware solutions

We asked this same question in last year's Endpoint Protection Ransomware Effectiveness report and saw a rise across the board this year in all categories. Looking at the combined totals of Mostly or Completely Implemented responses, the implementation of security software rose to 89% from last year's total of only 76%. Break room-style training rose to 36% from 28%, monthly video and emails rose to 52% vs 26%, phishing testing rose to 57% from 36%, and the use of security assessment training & testing rose to 54% from 34%.

This year, we wanted to gain a deeper understanding around what specifically impacted an organization's ability to fend off attacks. So, we asked what endpoint protection solutions were in place, showing the top solution types below.



Endpoint protection solutions in place

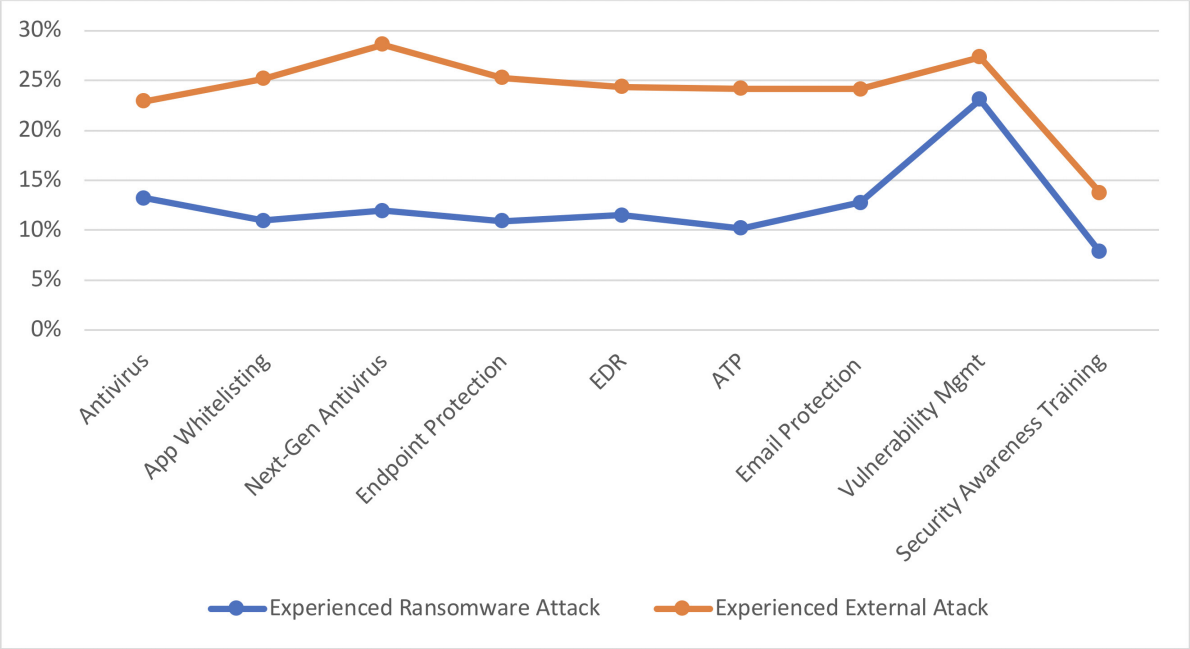
The healthcare, government and financial services sectors were higher in all solution categories, with only slight variances overall based on organization size. Even the SMB organizations seem to get it – as they were only slightly lower than the average, which is good to see.

With so many solutions in place, creating a layered security defense, what's having the most impact at stopping malware (and, therefore, ransomware and external attacks) from being successful?

What's Truly Effective in Stopping Attacks?

At the end of the day, the goal is to put the most effective solutions in place that will stop the most attacks. The list of solutions above reads like a "Who's Who" of security staples. But are they successful in stopping both ransomware and other malware attacks?

As shown below, most of the solutions largely have a similar effectiveness rate of stopping all forms of malware. An average of 13% of organizations experienced a ransomware attack, and 25% of organizations experienced an external attack, regardless of the type of security software in place.



% of organizations experiencing attacks (by solution implemented)

But it's the addition of security awareness training and phishing testing that had the greatest impact. The organizations continually performing security awareness training, as well as periodically testing employees with phishing emails saw the lowest percentage of ransomware attacks (8%) and malware-based external attacks (14%) in the last 12 months. In both cases, the addition of security awareness training and testing saw a 37% decrease in the success rate of malware versus those organizations simply relying on security software.

Effectively Stopping Malware Attacks in 2018

Now that there are thriving business models behind it, malware isn't going anywhere. And, as long as users can still be duped into clicking a malicious link or attachment, cyber-criminal organizations are going to continue to take advantage of it. Security vendors are laser-focused on the current state of threats, working to develop new ways to stay one step ahead. But, so are the bad guys – testing their latest malware against sandboxed versions of security solutions. It's a never-ending battle that only is continuing to evolve in complexity and specificity from both sides.

The impact of a successful attack is clear – hours of IT work, hours of unproductive users, thousands of files encrypted or records stolen, and the potential for material and tangible costs in paying ransoms, or addressing reputation issues post data breach.

In all of this, there are plenty of unknowns. The malware is constantly changing, the files held for ransom and the ransom itself, the data breached - all of the aspects of these attacks are unknowns. All except one factor – your users. They are the only constant in this ever-evolving war.

As this report shows, endpoint protection solutions help protect against a material percentage of malware, but don't actually put a stop to the threat. It's only by adding continual testing and training of employees that organizations create their strongest security posture. The material decrease shown above in the percentage of organizations experiencing both ransomware and external attacks demonstrates that a well-implemented security culture makes an organization much less prone to fall victim to a malware infection of any kind.

As malware-based threats continue to find ways to bypass endpoint security, it's imperative -and by definition the most effective – to create an additional line of defense – your users – to decrease your organization's risk of successful attack.

"The impact of a successful attack is clear - hours of IT work, hours of unproductive users, thousands of files encrypted or records stolen"

Additional Resources

Ransomware Simulator (RanSim)
Find out if your endpoint protection actually blocks ransomware infections.

Free Phishing Security Test
Find out what percentage of your users are Phish-prone.

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do.

Free Domain Spoof Test
Find out if hackers can spoof an email adress of your own domain.

Free Phish Alert Button
Your emloyees now have a safe way to report phishing attacks with one click.

Ransomware Hostage Rescue Manual
Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

To learn more about our additional resources, please visit www.KnowBe4.com/resources

About KnowBe4

KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make better security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com