



# TAKING A PROACTIVE APPROACH TO MITIGATE THE RISK OF RANSOMWARE

## November 2019

**DANIEL NEWMAN**  
Founding Partner + Principal Analyst

**SHELLY KRAMER**  
Partner + Senior Analyst

Published: November 2019

IN PARTNERSHIP WITH



# **TABLE OF CONTENTS**

<b>3</b>	Introduction
<b>4</b>	Executive Summary
<b>5</b>	Ransomware Risks: A Cautionary Tale
<b>7</b>	Most Common Ransomware Threats
<b>9</b>	How to Protect Against Ransomware Threats
<b>11</b>	Ransomware Attack Prevention and Solutions Overview
<b>13</b>	Conclusion
<b>14</b>	Recommendations

# INTRODUCTION

Data is big money in today's digital marketplace, but not always in the way you would expect. Hackers today are finding that temporarily locking companies' access to their own data is an easy way to make millions. How? Through a growing and increasingly expensive type of security breach: Ransomware.

What is ransomware? Imagine that you've just arrived at the office one morning and sat down at your desk ready to get to work. As you take a sip of your coffee, you attempt to open the cloud-based folder where you keep your most sensitive client files. Instead of opening a window to your documents, however, a note pops up on your screen letting you know that your system has been breached. The message is clear: Pay us, get your data. Otherwise, good luck.

The threat of ransomware is very real—and it doesn't happen just to everybody else. Ransomware is incredibly common—so common in fact, that every 14 seconds a company just like yours experiences a ransomware attack and faces a difficult decision: Should they pay the ransom—thereby funding the next iteration of ransomware attacks? Or are they prepared to risk the cost of potentially losing their data altogether?

In today's business world, data is virtually the lifeblood of every business. Operating without data is like flying blind—and in many cases a lack of access to customer data or business data can completely shut a business down. As a result, it is no surprise that many companies are unwilling to risk the potential downtime and associated costs of losing their data. In fact, of those targeted in a ransomware attack, some [40% opt to pay](#) to get their data back.

Unfortunately, it's nearly impossible to know the right answer. Even the FBI, which has traditionally advised companies not to pay, has recently offered more nuanced advice: [don't pay, but if you do, let us know](#). Paying up doesn't guarantee you restored access to your data. Companies that have paid have become the victim again or hackers have demanded even

more money. Paying could also create a vicious cycle that emboldens hackers and never truly solves the ransomware problem.

For hackers, ransomware is big business. The median cost of a single ransomware attack is valued today at \$133,000 and it's estimated that ransomware-related damages will hit [\\$11.5 billion in 2019](#), up from \$325 million in 2015. We expect costs associated with these attacks to continue to rise at a steady pace, largely due to the ease of which a ransomware attack can be executed.

Of the more than [850 million](#) ransomware infections detected in 2018, we know that [70%](#) of these breaches happen at the endpoint. Yet, [75%](#) of affected companies are already running up-to-date end-point protection. What's the solution? Unfortunately, remedial solutions like virus scans aren't the answer. What is? It starts with having a comprehensive understanding of the risks posed by ransomware, taking steps to prevent them, and then having a plan in place to manage the fallout if an attack occurs.



# EXECUTIVE SUMMARY

In 2017, the infamous [WannaCry](#) ransomware attack targeted computers running Microsoft Windows operating system by encrypting data and demanding ransom payments in bitcoin cryptocurrency. In a matter of days, WannaCry infected 200,000 computers in 150 countries with estimated losses of \$4 billion. WannaCry is but one of many security breaches occurring over the past several years, but the breadth of the WannaCry attack garnered immediate attention for the dangers of ransomware the world over.

As we head into 2020, the risk of ransomware attacks is growing rather than decreasing. The FBI estimates that some 4,000 ransomware attacks are sent daily, with a new attack being initiated about every 40 seconds. Not only is this fueled by the abundant success that ransomware developers are experiencing, but also impacted by the ever-increasing number of devices in use in the business environment (both corporate and personally-owned), as well as the explosion of data and our collective reliance on that data for all business operations.

Ransomware generally enters through an endpoint, such as a computer, tablet, mobile device, or cloud environment. Companies can also be targeted with ransomware by way of chat messages, social media messages, by users clicking links on compromised websites, or even by plugging in an unfamiliar USB drive. Ransomware is often introduced to a company's network by way of an email attachment or clickable link received in some other channel that is disguised as something legitimate. Once the user clicks to download, the file immediately encrypts the company's data and adds an extension to all files that makes them inaccessible.

Everyone within an organization, from the C-Suite and board members, to full-time staffers, independent contractors, part-time and temporary employees, and even

vendor partners can unwittingly be a target for a ransomware attack. The [total cost](#) of a ransomware attack is twofold. The first is the hard costs associated with the expense of forensic reviews, system rebuilding and ransom. The second is the total cost of downtime (averaging nearly 10 days), which is typically estimated at 5 to 10 times the actual ransom amount.

There are other factors that can ultimately affect the cost of a ransomware attack that are hard to measure such as reputation damage and loss of trust. And regardless of your organization's decision on paying the ransom, damage to these intangibles could be felt for years to come.

Comparing the potential costs of a ransomware attack to the costs of preventative measures is a simple calculation. Companies use a [risk-adjusted cost](#) of future events to determine if it's necessary to pay for preventative measures. For large enterprises, the yearly cost for preventative measures is around \$125 per employee compared to the potential recovery cost of \$1,000 per employee.

It's clear that ransomware is a threat to every organization, no matter its size, and having a plan for dealing with a ransomware attack should it occur is business mission critical. In this white paper we'll take a deeper look at the risks of ransomware, explore some of the most common ransomware threats organizations face today, and offer suggestions on how to mitigate the threat of ransomware for your organization.



# RANSOMWARE RISKS: A CAUTIONARY TALE

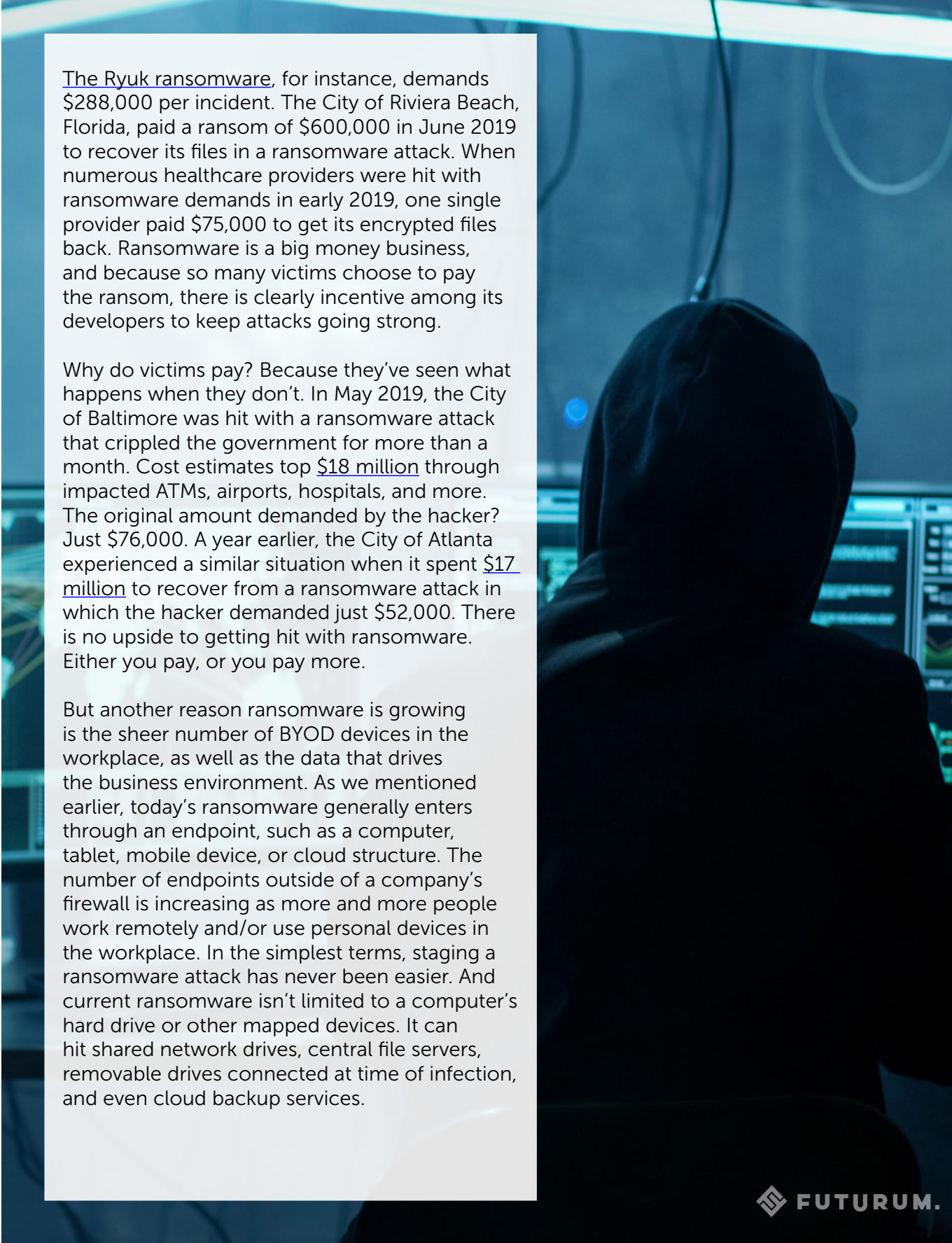


Despite their rise in popularity in the past decade, ransomware attacks were originally developed in 1989 with the AIDS Trojan, which was spread by way of a floppy disk. The first mass-deployed ransomware, however, was in 2012 with Reveton. The Reveton malware would secretly install itself onto a user's computer, causing it to freeze. Then, [a bogus message from the FBI](#) would pop up to indicate that the user had violated a federal law and needed to pay a fine to unlock it. Sounds kind of ridiculous, right? But as silly as it sounds, Reveton netted [\\$44,000 a day](#) in a single country in which it was distributed. It was that success that got a new generation of hackers interested in ransomware technology.

Since Reveton, numerous other types of ransomware have been developed, including Cryptolocker, Torrentlocker, and Cryptowall.

Unlike Reveton and other early ransomware, however, today's hacks don't attempt to freeze the computer; they aim to encrypt company files to make them unreadable. This way, the computer system remains stable enough for the infected party to make a payment and (hopefully) get their data back. Perhaps the most famous ransomware attack in recent years was [WannaCry](#), which infected 200,000 computers in 150 countries, with estimated losses of \$4 billion.

As we head into 2020, the risk of ransomware attacks isn't just large, it's growing at an exponential pace. Part of the reason for this is, as noted above, the abundant success that ransomware developers are experiencing. Ransomware developers simply have no reason to stop elevating their game.



The Ryuk ransomware, for instance, demands \$288,000 per incident. The City of Riviera Beach, Florida, paid a ransom of \$600,000 in June 2019 to recover its files in a ransomware attack. When numerous healthcare providers were hit with ransomware demands in early 2019, one single provider paid \$75,000 to get its encrypted files back. Ransomware is a big money business, and because so many victims choose to pay the ransom, there is clearly incentive among its developers to keep attacks going strong.

Why do victims pay? Because they've seen what happens when they don't. In May 2019, the City of Baltimore was hit with a ransomware attack that crippled the government for more than a month. Cost estimates top \$18 million through impacted ATMs, airports, hospitals, and more. The original amount demanded by the hacker? Just \$76,000. A year earlier, the City of Atlanta experienced a similar situation when it spent \$17 million to recover from a ransomware attack in which the hacker demanded just \$52,000. There is no upside to getting hit with ransomware. Either you pay, or you pay more.

But another reason ransomware is growing is the sheer number of BYOD devices in the workplace, as well as the data that drives the business environment. As we mentioned earlier, today's ransomware generally enters through an endpoint, such as a computer, tablet, mobile device, or cloud structure. The number of endpoints outside of a company's firewall is increasing as more and more people work remotely and/or use personal devices in the workplace. In the simplest terms, staging a ransomware attack has never been easier. And current ransomware isn't limited to a computer's hard drive or other mapped devices. It can hit shared network drives, central file servers, removable drives connected at time of infection, and even cloud backup services.



# MOST COMMON RANSOMWARE THREATS

The only way to avoid a costly outcome is to avoid the ransomware altogether. That means understanding how ransomware infiltrates your system so that you can prevent ransomware attacks from occurring. While there are a variety of ways ransomware can be introduced to a network, here are the most common ransomware threats organizations face:

**Phishing.** According to [Verizon's 2019 Data Breach Investigation Report](#), phishing is the top threat used in successful breaches linked to malware attacks. Most of us have experienced some type of corporate training advising us of the dangers of phishing. This "spray and pray" style hack targets the masses with a fake email message (or message in some other channel) that seems real, similar to the FBI hoax used by Reveton. Unsuspecting employees, wanting to stay on the good side of their superiors, click on an infected link, hoping to rectify whatever issue the message outlined—changing a password, updating customer information, etc. Once they click the link, the system becomes infected.

The Oregon Department of Human Services was the victim of a phishing campaign just this year resulting in a breach involving [1.6 million Oregon residents](#). Contents of the data breached included HIPAA-protected information such as names, addresses, birth dates, and social security numbers.

With phishing, hackers can target victims on a massive scale. All it takes is one unsuspecting employee to endanger the entire network and put their ransom request in place

**Exploit kits.** Exploit kits offer an easy way for hackers to automatically exploit vulnerabilities on companies' computers while employees browse the web. Because they are highly automated, they've become one of the most popular forms of remote access tool (RAT) distribution, often rented by underground

criminal markets in the form of "exploit-kit-as-a-service" programs. One exploit kit, Angler, has generated [\\$60 million](#) in ransomware payments. For the makers of these kits, ransomware is big business.

**Watering hole attacks.** A watering hole attack is a bit more selective than either of the above. In a watering hole attack, the hacker tries to compromise a specific group of end users by infecting a website that those users are known to visit. This could be a group with anything in common, who are known to visit a specific type of website on a regular basis.

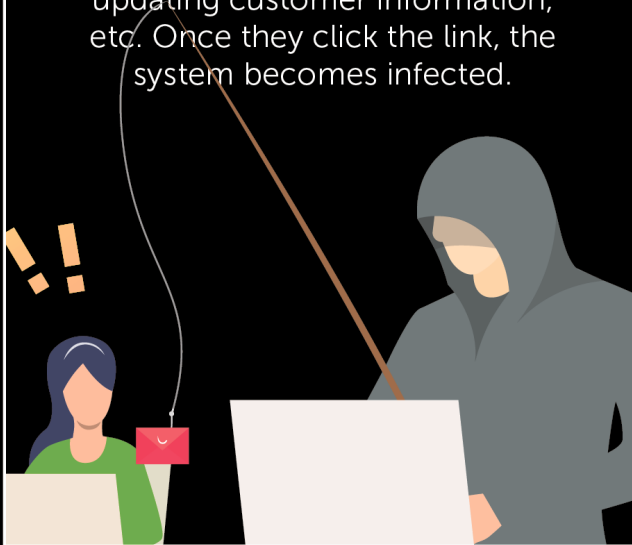
**Malvertising.** Malvertising is a word that blends malware and advertising, and it refers to a technique that cybercriminals use to covertly target unsuspecting users. In a malvertising attack, hackers buy ads on a trusted network and inject malicious code into those ads and webpages. Site visitors trust what seems like a reliable source, then unwittingly click on an ad or CTA that appears to be legitimate, which then spreads the malware.



# COMMON RANSOMWARE THREATS

## Phishing

Unsuspecting employees click on an infected link, hoping to rectify whatever issue the message outlined—changing a password, updating customer information, etc. Once they click the link, the system becomes infected.



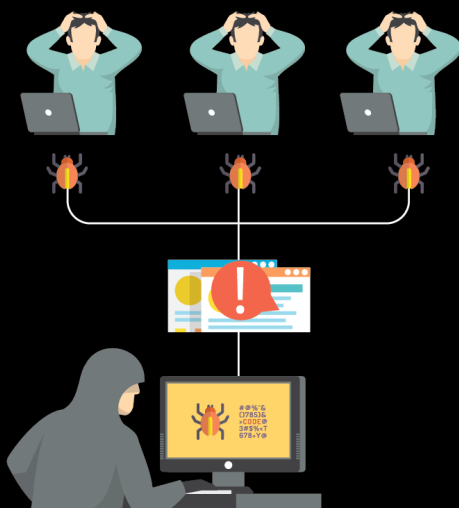
## Exploit Kits

These are highly automated and make it easy for hackers to automatically exploit vulnerabilities on companies' computers while employees browse the web.



## Watering Hole Attacks

In these attacks, the hacker tries to compromise a specific group of end users by infecting a website that those users are known to visit.



## Malvertising

Using a technique that blends malware and advertising, hackers buy ads on a trusted network and inject malicious codes into those ads and web pages. When clicked, the malware is spread.





# HOW TO PROTECT AGAINST RANSOMWARE THREATS

Now that we know the most common kinds of ransomware attacks, let's explore how to protect your organization from them. Seventy percent of ransomware attacks happen at the endpoint but investing in a bunch of endpoint security isn't enough to protect your company. It's not *more* security software that's the answer; it's finding the *right solution* to help manage endpoint security, syncs, backups, and patches easily and consistently to ensure your software is always up-to-date and that no endpoints are left unprotected.



To protect your organization against ransomware attacks, consider the following action steps:

**Simplify.** Most companies today employ on average 10 different endpoint security agents. The problem: Complexity and fragmentation are the enemies of security. You need solutions like that help unify endpoint management and protection capabilities including endpoint security, patch, and configuration management, and endpoint data protection into a single policy based platform.

**Create an incident response plan.** Don't operate on the premise of "If there's a breach, then we ...." operate instead on the "There will most certainly be a breach, here is our plan" mindset. Work with your IT team to prepare processes for quickly identifying the level of the breach, which data has been impacted,

how to retrieve it, how long that process will take and, if necessary, determine in advance how much you are willing to pay in ransom.

**Educate on Security Awareness.** Cybersecurity is not only an IT problem. Employees are most often accidentally responsible for an attack or data breach, and it's often due to a lack of security awareness, training, and/or resources. With a [30% phish-prone rate](#), ongoing and regular education is a top priority for establishing a security-first mindset within the organization, and taking steps to protect endpoints. With the right training, companies can get that number to 2%. It's also important to remember that security awareness should not be treated as a one-and-done undertaking. Regular training, testing, and security exercises should be employed to keep security top-of-mind for everyone within the organization.

**Create proactive policies.** It's important for your IT team to take proactive steps to protect against potential ransomware attacks. That includes things like restricting the execution of programs from temporary folders and prohibiting attachments with executable files in email. We also suggest that IT leaders disable Flash and Windows Script Host.

**Plan for an attack—before it happens.** When it comes to ransomware, the risk is not just in the ransom request, it's in how you handle it. Do you have a plan in place to reclaim your data? At Erie County Medical Center in Buffalo, New York, employees received a ransomware request for \$30,000 to buy back access to hospital data. At the time, they refused to pay it, causing a [\\$10 million crash](#) in

their computer systems. Half of that damage came in the form of computer systems. The other half came in the form of overtime and lost revenue caused by the crash. If they had had a plan in place not just for protecting their systems, but also for how to handle ransomware requests, the damage would likely have been far more negligible.

Bottom line, ransomware security requires smart decisions on every front—not just the endpoints. By taking a proactive approach that includes clear and simplified endpoint security and management, regular and ongoing security awareness education, proactive protection measures, and a plan in place in case of an attack, you'll be able to significantly mitigate your risk.





# RANSOMWARE ATTACK PREVENTION AND SOLUTIONS OVERVIEW

The only way to avoid a costly outcome of a ransomware attack is to avoid the ransomware altogether. But how? Understanding how ransomware infiltrates your system and taking preventive measures accordingly is critically important. Ransomware attack preventive measures include:



**Endpoint protection.** Research shows [70%](#) of breaches happen at the endpoint. It seems the simplest solution would be to add more endpoint protection. However, research shows that endpoint complexity can actually make your endpoints more vulnerable, just like other fragmented security systems being developed around the globe.

Indeed, the average company has 10 security agents on each device. From a cost standpoint, that's an incredibly sizable investment. Endpoint protection accounts for [24%](#) of IT security spend. But the fact is that the risk of failure grows as more security agents are used. More isn't always better in IT security. Most companies are probably spending more than they should while keeping fewer of their endpoints secure.



**Device and patch management.** Because there are so many devices, it's imperative to have one place to perform all security, patch, and configuration management, eliminating the confusion of multiple disconnected tools. This is where a centralized device and patch management program can provide significant protection against ransomware and other cybersecurity risks.

**More frequent backups.** Another way to mitigate data loss would be to back up files more frequently. In order for companies to ensure that valued end point data is continuously backed up and available for recovery, the company must be in control of the backup process. A centralized, policy based solution which eliminates dependencies

on end users to participate in the backup process can provide assurance of the company's ability to recover data and minimize the impact of a ransomware event.

**Education.** The average phish-prone percentage across all industries is [30%](#). Education surrounding phishing—for example, teaching employees how to recognize a phishing email—is an important way to prevent a ransomware attack. There is evidence that the percentage can drop significantly if engaged training is done at least once per month for three months to a year. As we have mentioned before, training to prevent a ransomware attack is not a one-time thing. Creating a security-first mindset is an ongoing and regular exercise in risk prevention as a whole.

**Yes, the threat of ransomware is real, and it is mounting. But understanding the tools you have at your fingertips to prevent an attack will go a long way in saving your company millions in lost data—or paid ransom—later on.**

FUTURUM.

## CONCLUSION

Ransomware is not something that today's businesses can afford to face on defense. At best, they'll end up paying a ransom; at worst, they'll spend millions in damages due to downtime and lost data. If your goal is to keep your organization ahead of the threat, an offensive strategy is your best bet—your organization must take a proactive stance against ransomware attacks altogether.

Throwing numerous different endpoint security software options at your systems won't protect you fully. By 2020, it's anticipated that companies will spend a combined [\\$128 billion](#) in endpoint security, but ransomware creators are showing no signs of slowing down. It's not

more security software that's the answer—it's finding the right solution to help you manage endpoint security, data backups, and patches easily and consistently to ensure your software is always up-to-date and that no endpoints are left unprotected.

Every 14 seconds, a company wonders whether it should pay the ransom or risk the cost of potentially losing its data altogether. But there is a better way. Your company can prepare in advance for such attacks by proactively investing in the right security solutions and determining how you'll handle an attack if it does occur. When in doubt, work with a reputable provider to help you create a solution that works for your company.





## RECOMMENDATIONS

As noted above, there are many things your company can do to help prevent a ransomware attack, or to limit its impact if an attack is made. Securing what matters most: Identities, applications, and data, is the path to protecting your organization from risk. Working with a trusted vendor partner like Micro Focus can help you protect the organization at endpoints and beyond. Here are some recommendations from the security experts at Micro Focus to consider:



**Simplify.** The average company is using [10 agents](#) to govern its endpoints. But as we've mentioned, while throwing expensive security systems at the endpoint feels like a good idea, it could possibly increase the risk of an attack. Complexity and fragmentation are the enemies of security. Solutions like [Connected MX](#) from Micro Focus help unify backup, file sync, and sharing capabilities into a single platform, protecting and improving workforce productivity. Policy-based backups create automatic triggers for certain types of files, which are especially important when dealing with data governed by certain regulatory issues. Its patented **SendOnce** technology does block-level de-duplication within the agent, so data reduction happens before network transmission, eliminating data overload.

Similarly, the Micro Focus [ZENworks](#) endpoint security management performs all security, patch, and configuration management tasks, including cloud-based endpoint protection, *from one spot*,

eliminating the confusion of dealing with many disconnected tools. The result is not just a safer enterprise, but a less overwhelmed IT department overall. A focus on simplifying is the key to increased peace of mind and risk mitigation.

**Create an incident response plan.** When it comes to ransomware, it's essential to always be prepared for an attack. Even though the goal is prevention, the approach must also include preparedness. To limit the downtime associated with malware attacks, work with your IT team to create an incident response plan. Prepare processes for quickly identifying the level of the breach, which data has been impacted, how to retrieve it, and how long that process will take, as well as the chain of command. But don't just write it down—practice this plan. Re-enact a breach, over and over again, until all members of your team are ready to deal with a real-life threat. You'll find that the more prepared you and your team are, the more expeditious problem resolution will be, no matter the situation.



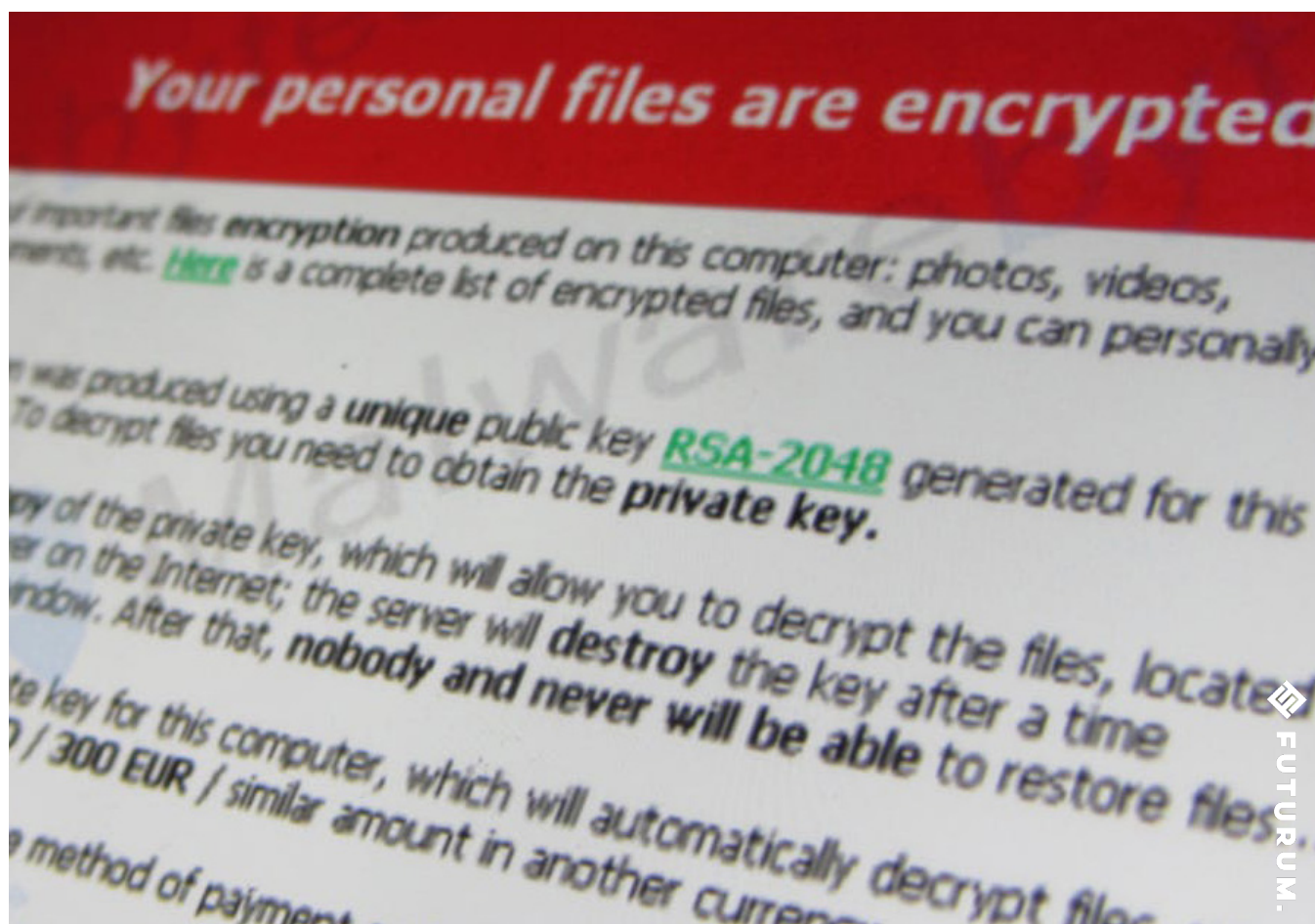
**Educate.** With a [30%](#) phish-prone rate, education is clearly a top priority for protecting endpoints. Research has shown, however, that with the right training, companies can get that number down to 2% within 12 months. What constitutes the “right” type of training? Baseline training, engaging computer-based training, monthly phishing simulations, and measured results are key.

**Create proactive policies.** There are many easy things you can do within your enterprise to limit the potential for a ransomware attack. For instance, consider restricting the execution of programs from temporary folders to ensure that any link opened does not automatically run.

Consider prohibiting attachments with executable files in email exchanges. Disable flash and Windows Script Host, which are common attack vectors. Ransomware security requires smart decisions on every front—not just the endpoint.

**Understand the ROI.** Yes, preventative ransomware strategies may require financial investment, which means it must be understood in terms of ROI for the entire company. By calculating the risk-adjusted cost of not implementing preventative measures vs. the cost of security itself.

**Though ransomware attacks may seem unavoidable and costly in today’s digital marketplace, they do not have to be.** By taking a proactive approach that includes clear and simplified endpoint security and management, your company will be well on its way to keeping your data safe. And when you need a trusted vendor partner to guide you along the way, we recommend the team at Micro Focus. They are uniquely positioned to help defend your IT ecosystem against breach.



# IMPORTANT INFORMATION ABOUT THIS PAPER

## CONTRIBUTORS:

Daniel Newman

*Founding Partner + Principal Analyst, Futurum Research*

Shelly Kramer

*Partner + Senior Analyst, Futurum Research*

## PUBLISHER:

Daniel Newman

*Founding Partner + Principal Analyst, Futurum Research*

**INQUIRIES:** Contact us if you would like to discuss this report and Futurum Research will respond promptly.

**CITATIONS:** This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Futurum Research." Non-press and non-analysts must receive prior written permission by Futurum Research for any citations.

**LICENSING:** This document, including any supporting materials, is owned by Futurum Research. This publication may not be reproduced, distributed, or shared in any form without the prior written permission of Futurum Research.

**DISCLOSURES:** This paper was commissioned by Micro Focus. Futurum Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

## ABOUT MICRO FOCUS

At Micro Focus we help you run and transform your business. Driven by customer-centric innovation, our software provides the critical tools you need to build, operate, secure, and analyze the enterprise. By design, these tools bridge the gap between existing and emerging technologies—which means you can innovate faster, with less risk, in the race to digital transformation.

## ABOUT FUTURUM RESEARCH

Futurum is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

**DISCLAIMER:** The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Futurum Research disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Futurum Research and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Futurum Research provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

## CONTACT INFORMATION

Futurum Research, LLC | [futurumresearch.com](http://futurumresearch.com) | 817-480-3038 | [info@futurumresearch.com](mailto:info@futurumresearch.com)

Twitter: [@FuturumResearch](https://twitter.com/FuturumResearch)

©2019 Futurum Research. Company and product names are used for informational purposes only and may be trademarks of their respective owners.