MORPHISEC

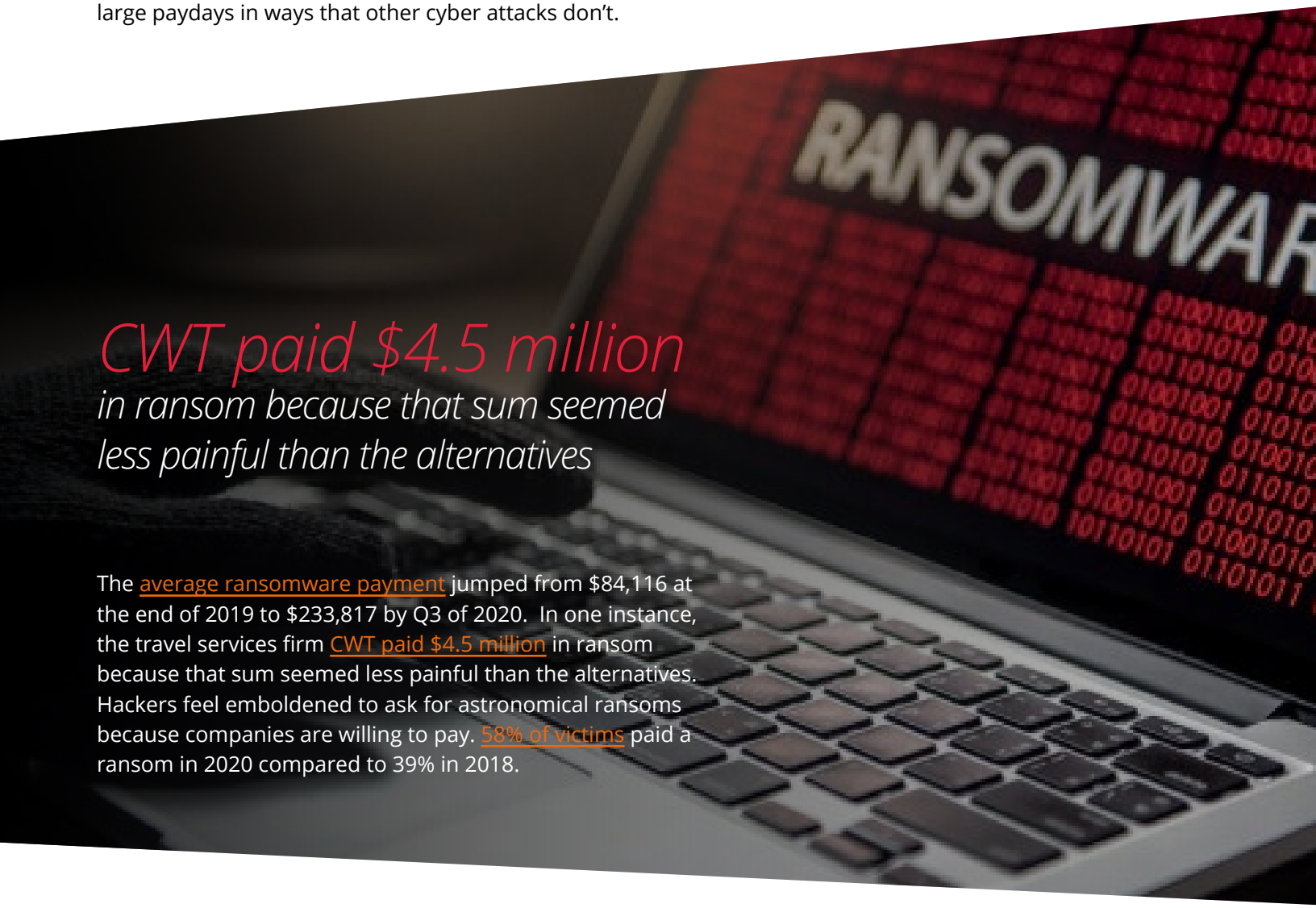
THE RANSOMWARE PREVENTION GUIDEBOOK

INTRODUCTION

Ransomware took the gloves off in 2020. It started the year as one of many different cyber threats on a company's radar. By the end of it, however, ransomware ranked among the most frightening risks facing every organization in the world – something no one could ignore any longer.

Were it not for COVID-19 and a presidential election, ransomware would have been the dominant headline in 2020. Even with so much going on, high-profile attacks on corporations like Garmin and Cognizant (and the multi-million dollar ransoms they paid) drew widespread attention. Less reported on was the fact that these attacks were hardly anomalies: ransomware compromised many companies in 2020 and pushed cybercrime to new depths of ruthlessness.

Between 2018 and 2019, instances of ransomware increased by 140%. That looks like nothing compared to what happened in 2020 when attacks increased by 715% according to one estimate. Ransomware attacks are no longer a rarity. More hackers are using them more often for the simple fact that encrypting people's data yields large paydays in ways that other cyber attacks don't.



CWT paid $4.5 million
in ransom because that sum seemed less painful than the alternatives

The average ransomware payment jumped from $84,116 at the end of 2019 to $233,817 by Q3 of 2020. In one instance, the travel services firm CWT paid $4.5 million in ransom because that sum seemed less painful than the alternatives. Hackers feel emboldened to ask for astronomical ransoms because companies are willing to pay. 58% of victims paid a ransom in 2020 compared to 39% in 2018.

Perhaps even more alarming than how much hackers managed to steal with ransomware in 2020 was who they chose to target. Hospitals, schools, and local governments all became common victims because of their high propensity to pay ransoms (not paying isn't an option for these essential services). A ransomware attack on a German hospital was even initially blamed for the first death ever attributed to a cybersecurity incident. If hackers considered any target to be "off limits" before, indiscriminate attacks on sensitive targets – the sick, children, and public infrastructure – prove that many groups no longer view those targets in the same light.

Having seen the profitability of ransomware, bad actors will emphasize this attack ever more in 2021 and beyond. Expect to see sophisticated attacks arrive with greater frequency and larger demands (not just one-time ransoms). More urgently, don't expect to be immune. Recent history has shown that anyone can be a target of ransomware, and targets usually turn into victims.

This guidebooks gives you the tools to fight back and outlines how to treat ransomware prevention like the mission-critical priority it needs to be:

- SECTION ONE highlights what today's ransomware looks like, how it evolved to this point, and why these attacks are more expensive than you think.
- SECTION TWO explores why the cyber defenses currently in place do such a poor job of stopping ransomware and can't be relied on moving forward.
- SECTION THREE unpacks why the ransomware problem is likely to get much worse from here, in terms of the ubiquity of attacks, the damage they cause, and the effort it takes to shut them down.
- SECTION FOUR shows you how to take a proactive approach and breaks down the specific strategies and technologies you need in your defensive arsenal.

SECTION 1 | THE STATE OF RANSOMWARE

The first strain of ransomware appeared as far back as 1989. However, it remained rare for the next 20 years, until around 2011 when the number of ransomware strains and attacks began to explode. We're seeing another explosion right now – one that eclipses every development that came before and elevates ransomware to the status of existential threat.

Attacks are more frequent, as we outlined earlier, but they're also more successful thanks to a change in tactics that appeared over the last year. These are some of the key features of today's ransomware:

SPEARPHISHING CAMPAIGNS

Before, ransomware usually arrived inside a phishing campaign that loosely targeted multiple recipients. Hackers cast a broad net and hoped to catch a few victims. Today, they're doing the opposite: targeting spearphishing campaigns at one specific company or person. The personalized nature and insider details included in these campaigns make the red flags very hard to spot. Hackers will also capitalize on pressing issues – the pandemic, stimulus, social unrest, etc. – to stoke recipients into urgent action. Spearphishing campaigns go to great lengths to evade suspicion, and the high rates of ransomware infections in 2020 make it clear they work.

HUMAN-OPERATED ATTACKS

Older ransomware variants automated the attack. They used a programmed method to compromise a weak server before proceeding on a pre-set path through the network to reach the ultimate target: the domain controller. If an automated attack ran into a roadblock, it usually failed. The attacks in 2020, by contrast, often had a human at the controls. When they encountered resistance, they could resort to a Plan B, resulting in a higher number of attacks bypassing defenses and reaching the domain controller. With this and the previous trend, hackers are putting much more effort into ransomware than they did before 2020. The next trend suggests why.

LONG-TERM EXTORTION

Hackers have found multiple ways to monetize a single ransomware attack. First, they demand a ransom to restore access to key data and applications. Then, hackers threaten to release copies of a company's data, especially anything considered sensitive, if they don't pay again. As long as a hacker maintains a copy of the data, they can demand a payment as often as they want in whatever amount they think a company will pay to keep its secrets safe. The threat of making private data public helps explain why so many organizations paid ransoms in 2020 and why those sums were often astronomical by previous standards. This has an alarming implication: ransomware victims can't make the damage stop. One successful attack could turn into a long-term financial drain and a never-ending reputational risk. Hackers have raised the stakes significantly.

COVID-19 pandemic caught hackers, like everyone else, off guard. But they quickly reset and threw their weight behind a prolonged campaign of antagonism.

The confluence of these trends turned ransomware into a formidable threat in 2020. The outbreak of the COVID-19 pandemic caught hackers, like everyone else, off guard. But they quickly reset and threw their weight behind a prolonged campaign of antagonism. Leading hacking organizations have even abandoned their old tactics to make ransomware their primary weapon. More will surely follow considering that just one ransomware strain, Ryuk, netted $150 million in stolen funds for its operators.

Companies need to be concerned about dozens of different threats, cyber and otherwise. But after the events of 2020, ransomware should be very high on the priorities list. Anything less exposes an organization to a poisonous problem unlike anything they've dealt with before.

SECTION 2 | WHY CYBERSECURITY ISN'T STOPPING RANSOMWARE

Once a ransomware attack finds the domain controller, it's too late. Hackers have reached their final target – possibly through a human-driven process of exploratory trial and error – and have nothing stopping them from seizing control (and copies) of data and applications. Cybersecurity becomes symbolic past that point because the proverbial bomb has already exploded.

This highlights the paradox of cybersecurity in the face of ransomware: In an era of reactive defenses, when we put most of our efforts into detection and response instead of prevention, we leave the door wide open to ransomware. To put it differently, the way we defend against most threats makes us more vulnerable to the worst threat of all. What's remarkable isn't how bad ransomware has become but how long it took to reach this low point.

It's a mistake to think that reactive cybersecurity built on the back of antivirus and EDR tools will stop ransomware attacks. That being said, it's also wrong to assume that ransomware is immune to cybersecurity. In fact, many of the traditional recommendations for preventing ransomware put effective obstacles between the attack and the domain controller. Those include:

ENFORCING MULTIFACTOR AUTHENTICATION

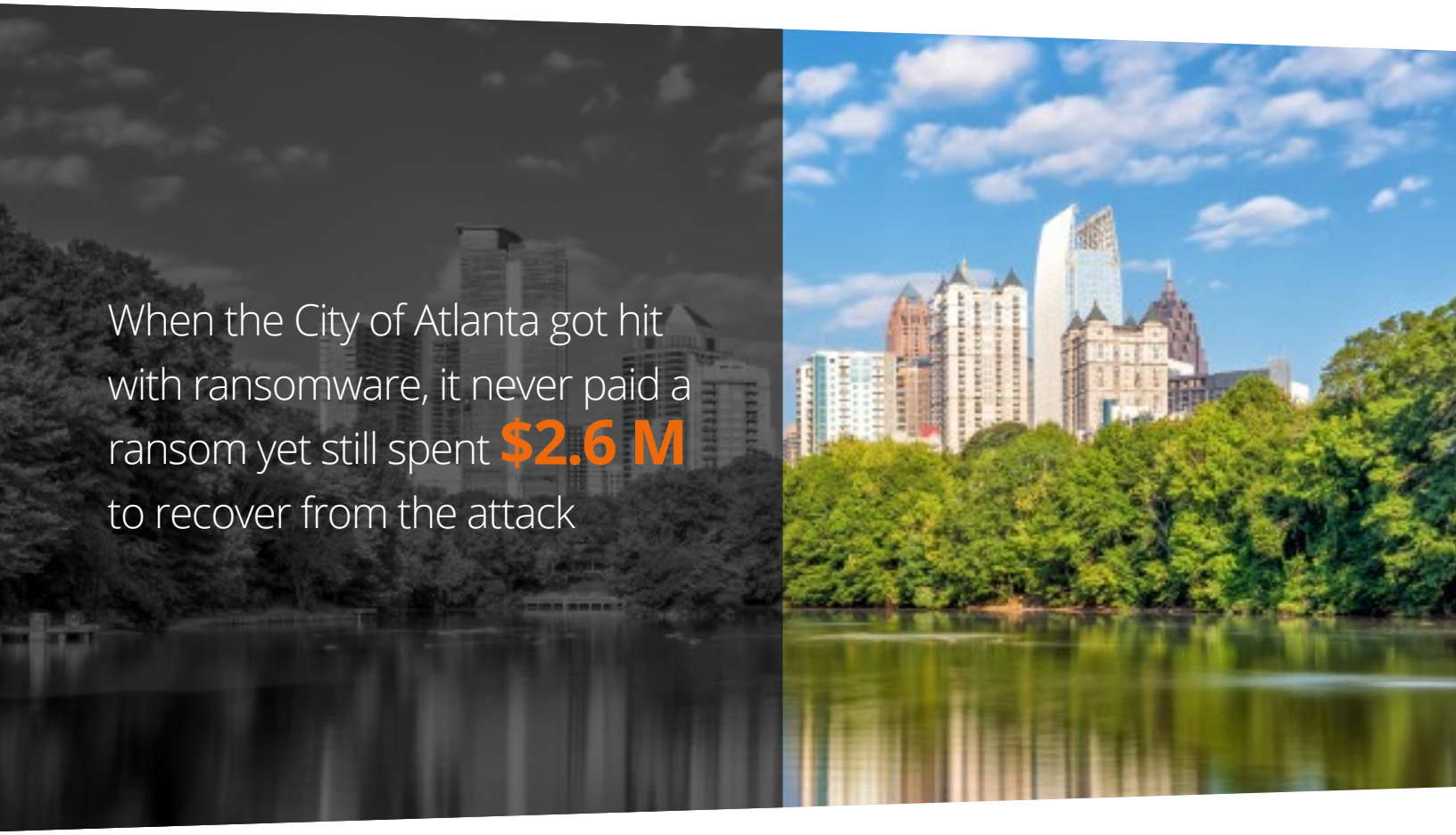
Since hackers often use credential theft to bolster their spearphishing campaigns or to jump through networks, multifactor authentication can make their path more difficult.

MINIMIZING ADMIN ACCESS

Hackers will exploit administrative privileges to reach the domain controller faster. Remove admin access wherever possible, and be rigorous about maintaining this policy as IT evolves.

HARDENING SERVERS WITH A ZERO TRUST/DENY APPROACH

If weak servers are where ransomware attacks often gain entry, they're the first and best place to install defenses. Use a zero trust approach that denies access to everything until it can provide the necessary credentials.



Too many organizations neglect even these basic steps. More problematically, they lean on them entirely too much. Things like server hardening and access controls can stop some attacks and slow down some others – but they can't prevent every attack. Worse, their ability to prevent attacks declines as hackers devise more sophisticated and persistent offensive strategies. It's risky to operate without these preventions in place; it's similarly risky to rely on them exclusively or to expect EDR solutions to provide any kind of backstop. A cybersecurity strategy that doesn't put a significant amount of weight into prevention makes it a matter of time before ransomware weaponizes a company's own IT. Nothing significant stands in the way.

This should be a major cause for alarm considering that it takes around 20 days to recover from an attack, during which companies hemorrhage revenue. They will often pay over and above the ransom as well since resolving at attack may involve third-party consultants, negotiators, analysts, lawyers, and others who all work on a fee. When the City of Atlanta got hit with ransomware, for example, it never paid a ransom yet still spent $2.6 million to recover from the attack.

Any ransomware attack that reaches the domain controller, no matter what it does next, will be expensive to resolve. Yet very few organizations have the defenses in place to prevent an attack. More than just a gap in cybersecurity, the inability to stop or minimize ransomware leaves a company open to sudden disaster...even complete collapse.

SECTION 3 | RANSOMWARE AS A SERVICE: SELLING NETWORK ACCESS

Every indicator suggests that ransomware will continue to get worse. In fact, there's reason to believe we're seeing an evolution in ransomware specifically and cybercrime generally into something much worse than it was before. With time, 2020 might seem like a tipping point.

Experts are so alarmed about the potential of ransomware because of the underground economy springing up around it. Unlike many other cyber attacks, which are purely disruptive or else slow to monetize, ransomware pays off quickly, generously, and repeatedly. That will make these attacks look highly attractive to threat actors the world over. Ransomware might also appear more viable than other kinds of crime since demanding ransoms has such substantial upside. All these factors will multiply interest in ransomware among threat groups who previously focused on other methodologies.

Anyone committed to launching a ransomware attack now has the means regardless of their technical ability. They can purchase an off-the-shelf ransomware attack simple enough for any novice to deploy. Hackers for hire can make it even easier. The extremely low barrier to entry deserves much of the blame for the recent explosion in ransomware attacks.

Blame the success of those attacks on state-sponsored hackers. Weapons-grade attacks built by elite hacking groups for geopolitical purposes are now in the hands of mid-level hackers driven purely by profit. As expected, those attacks are extremely hard to defend against. Less expected is that they're easy to iterate upon, spawning a number of new ransomware variants and sowing the seeds for many more.

Powerful attacks are filtering from the top of the cybercrime pyramid downwards. Simultaneously, waves of new hackers are flooding into the bottom. Where they meet in the middle is where ransomware exists right now: an extremely dangerous, highly effective attack that's available to anyone who wants it.

To illustrate what today's attacks can do – and highlight the upward trajectory they're on – consider the attack that hit Garmin: WastedLocker. Developed by a gang of Russian cybercriminals ominously called Evil Corp, the attack masquerades as a software update. Upon download, WastedLocker moves laterally inside a host by elevating the user's privileges and bypassing defenses/obstacles, deleting backups along the way. The last move is to encrypt the data and demand at least $500,000 to restore access. This attack, like most ransomware variants currently in the wild, is efficient, effective, and merciless. In the very near future, all ransomware attacks will have these same features. Companies ignore this fast-rising risk at their own peril.

SECTION 4 | A PROACTIVE PLAN FOR PREVENTING RANSOMWARE

The only way to prevent ransomware is to neutralize the attack before it reaches the domain controller. Action must come swiftly and systematically – especially since new or human-operated attacks utilize unpredictable strategies. For the same reason, prevention works best using a tactics-based approach: where users defend against the tactics hackers deploy instead of tailoring defenses to individual attacks. The MITRE framework proves useful here. It highlights each stage a ransomware attack will go through to reach the domain controller. Fight back at each stage using the comprehensive approach outlined below:

INITIAL ACCESS

When an attack first gains access to a network

- Patch any servers or applications that may be exposed. Use virtual patching as necessary
- Change passwords and use multifactor authentication to prevent credential theft
- Educate users about identifying and avoiding phishing and spearphishing attempts

EXECUTION

When an attack launches its first stage

- Implement application control in a way that doesn't compromise accessibility
- Commit to a zero trust framework
- Implement a solution like moving target defense from Morphisec to prevent in-memory exploits.

PERSISTENCE

When an attack locates a stable place to dwell.

- Configure user access controls
- Minimize administrative privileges
- Audit privileges regularly to rollback unnecessary access

LATERAL MOVEMENT

When an attack proceeds towards the domain controller

- Block items the EDR flags without auditing them first since preventing ransomware depends on acting quickly.
- Require multifactor authentication to close down lateral pathways
- Avoid sharing folders or privileges between business units to make it harder for hackers to leap from one place to another.

EXFILTRATION

- Block inbound and outbound internet connections to servers
- Use an external firewall
- Practice data loss prevention

IMPACT

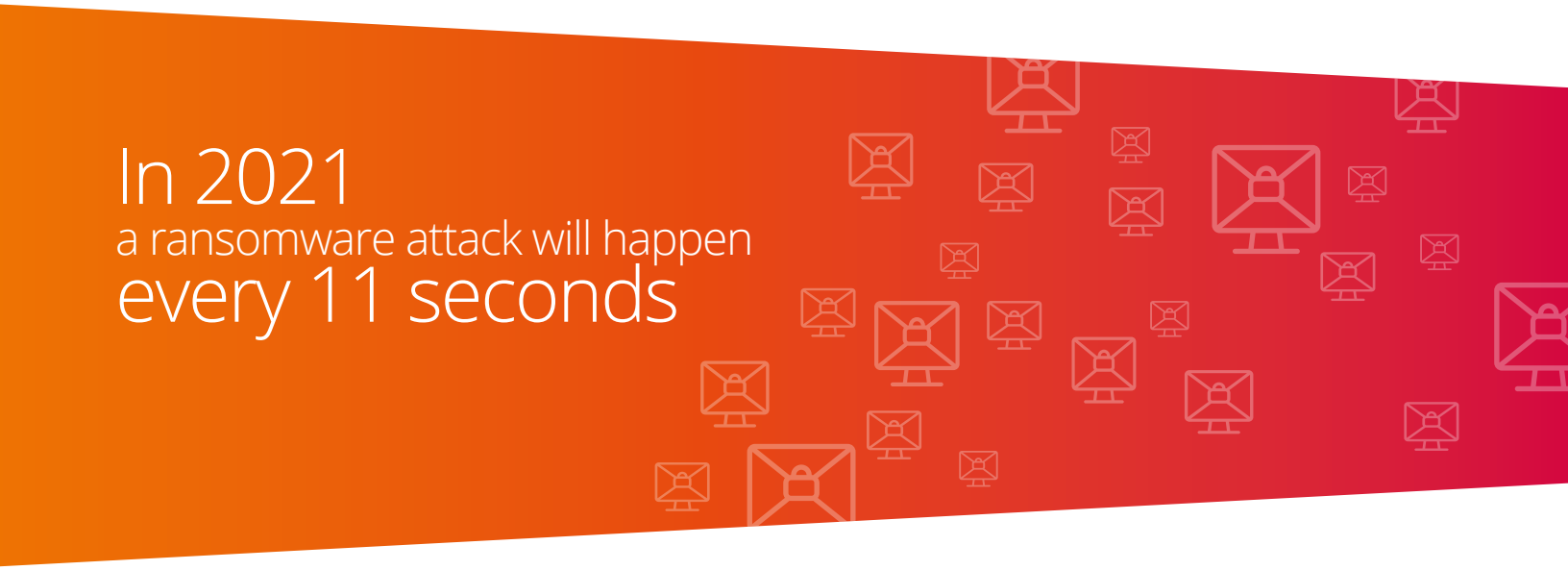
- Test backups systematically
- Separate networks

All these steps matter, and it's risky to neglect any of them. That being said, the first two stages of the attack – initial access and execution – deserve the greatest focus. After an attack gains entry and executes successfully, the odds of shutting it down decline significantly.

Preventing initial access is mostly about practicing good cyber hygiene. A rigorous program of patching and updating combined with smart password policies can thwart a large number of attacks. Comprehensive and continuous user training is just as important since ransomware attacks so often utilize social manipulation to gain entry.

Preventing execution represents a bigger challenge. Hackers have myriad targets to choose from and plenty of ways to move quietly while covering their tracks. Instead of giving them static targets which they can compromise in stealth, the zero trust runtime solution powered by moving target defense from Morphisec puts the target on the offensive. Our solution morphs the application memory (the target) so attacks can't identify it. Then it creates a decoy copy of the memory that lures the attack into a safe environment where it can be neutralized and analyzed. Determined ransomware attacks are sure to make it past the initial access stage even when following best practices for cyber hygiene. Moving target defense keeps them from proceeding any farther. It's a crucial component for preventing ransomware and many other cyber threats.

BEING REALISTIC ABOUT RANSOMWARE



2020 was a wake-up call. One of the loudest lessons was that ransomware can't be underestimated. It's hard to spot, challenging to stop, and devastating when successful. Additionally, any organization can be a target regardless of its size, industry, or social status. With everything about ransomware getting (much) worse, prevention must be a priority from here out.

In 2021, a ransomware attack will happen every 11 seconds, and businesses will pay a projected $20 billion in ransom, which is 57 times more than in 2015. Those figures will only get worse with each successive year. Knowing what's coming, ransomware prevention becomes a non-negotiable component of cybersecurity and risk management more broadly. Fortunately, it also qualifies as a smart investment since prevention costs vastly less than a successful attack.

If you're ready to get serious about ransomware prevention, Morphisec offers a singular solution. Our moving target defense product helps users prevent ransomware and secure endpoints, all while they invest less time and staff into cybersecurity. We don't claim to offer a silver bullet – especially against a threat as unruly and aggressive as ransomware. But Morphisec can help defuse many ransomware variants by outsmarting the attack early, while it's still benign.

See how moving target defense aligns with your current security stack and checks the boxes of ransomware prevention – schedule a demo with Morphisec.

ABOUT MORPHISEC

FUNDAMENTALLY ALTERING THE CYBERSECURITY LANDSCAPE

Morphisec is transforming endpoint security with our pioneering Moving Target Defense. Our solutions deliver operationally simple, proactive prevention unbound by the limits of detection and prediction. We protect businesses around the globe from the most dangerous and sophisticated cyberattacks immediately, efficiently and absolutely.