Malwarebytes

RANSOMWARE PROTECTION

A Best Practices Approach to Securing Your Enterprise

TABLE OF CONTENTS

INTRODUCTION

Ransomware has taken the world by storm. CryptoWall extorted an estimated $18 million, and WannaCry locked up more than 230,000 computers across the globe in 2017. Companies of all sizes are sitting up and taking notice. Even brands with a strong security investment have fallen victim. We've seen ransomware cripple businesses: nearly 19% of businesses stop operations immediately after discovering a ransomware attack.[1] Hospital emergency rooms forced to turn people away; global shipping logistics experience massive disruption; and even a summer blockbuster movie held up for ransom. The FBI estimates ransomware is now a billion-dollar business.

Ransomware has been around for a while, and it has spiked in recent years. It secured 5th place as the most common variety of malware in 2017, up from 22nd place in 2014.[2] Originally ransomware targeted individuals and was considered a consumer nuisance. It has now become a business menace.

WHAT HAS CHANGED?

The Shadow Brokers hacker group leaked the NSA's EternalBlue exploit, and cybercriminals gained a powerful weapon to execute worldwide ransomware attacks. Enter the arrival of "Ransomware 2.0."

The primary goal of all ransomware is to gain access and to encrypt the endpoint, Malwarebytes Threat Intelligence is used to learn about ransomware and the attacker's tactics, techniques, and procedures (TTPs). Malwarebytes has developed these best practice recommendations for you to keep ransomware from harming your organization.

[1] *Malwarebytes. The Global Impact of Ransomware on Business. 2016*

[2] *2017 Verizon Data Breach Investigation Report*

WHAT IS RANSOMWARE?

Ransomware is a type of malware designed to block access to your system through encryption, until a sum of money is paid, typically in the form of a bitcoin ransom. Once the attacker receives the payment, in theory, they will provide the victim with the decryption key to regain access to their system.

With the increase in ransomware volume and variants, attacker techniques vary. Like most forms of malware, ransomware is most often delivered to end users' computers through:

1. phishing and spam emails
2. malicious websites
3. dropped by another malware

Three Levels of Ransomware

LOW GRADE

Scareware

Fake antivirus tools pretend to detect malware issues and demand payment to fix them

MIDDLE GRADE

Browser or Screen Locking Ransomware

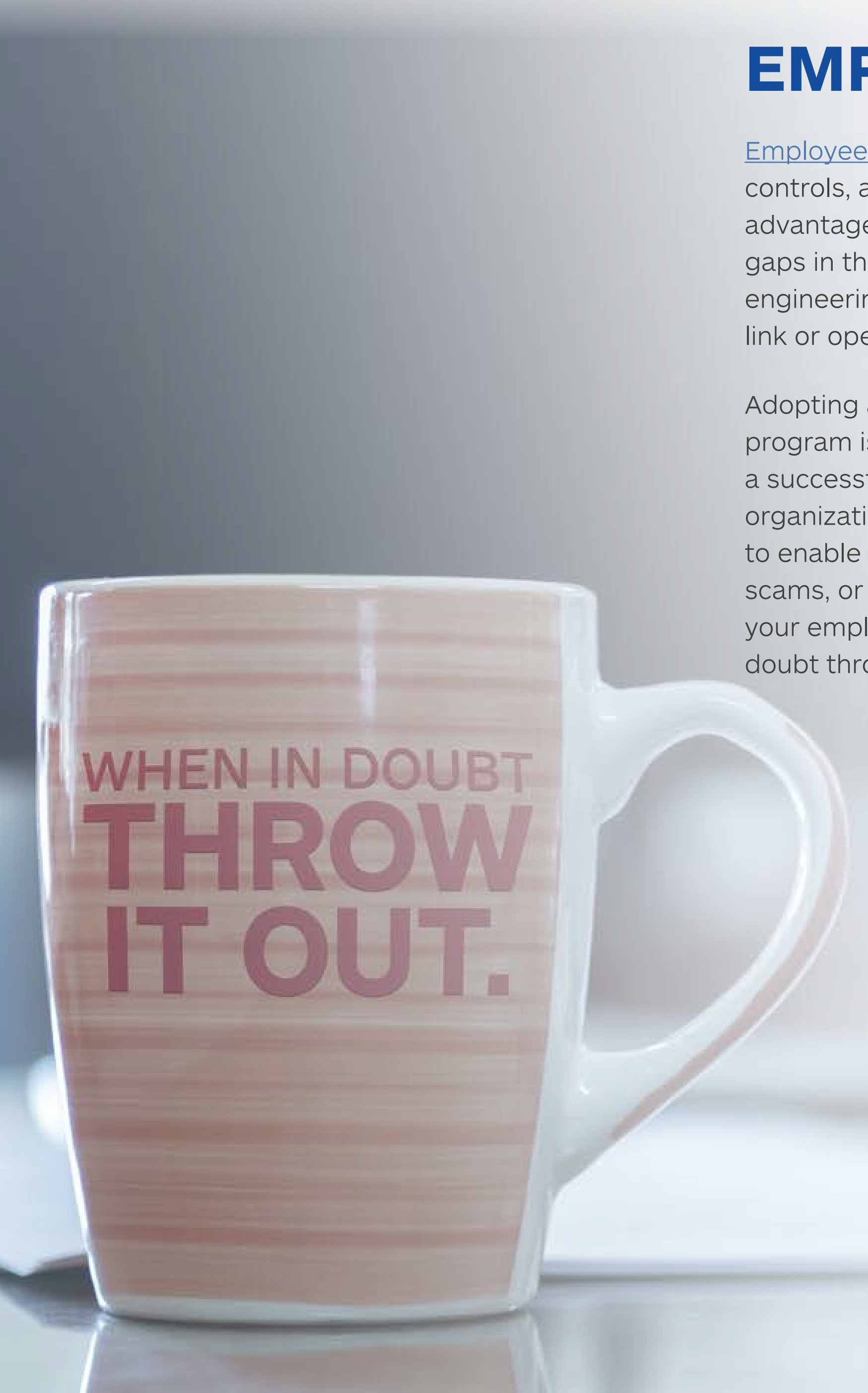
Law enforcement scams use fake FBI or U.S. Department of Justice messages to claim they've detected illegal activity on your computer for which you need to pay a fine

MOST DANGEROUS

Encrypting Ransomware

Pop-up messages say your files are encrypted and demand ransom money be paid by a deadline in order to return them

EMPLOYEE EDUCATION



Employees are the weakest link to your security controls, and ransomware attackers are taking advantage of it. They recognize employees have gaps in their security awareness, and social engineering techniques bait them to click on a link or open an attachment.

Adopting an employee security education program is an important step in preventing a successful ransomware attack on your organization. It makes employees a lot less likely to enable macros or fall for phishing emails, scams, or suspicious links. In the case of email, your employees should follow the rule, “when in doubt throw it out.”

Training requires a commitment from the information security team and should include your entire organization—from the executives to frontline staff. Everyone needs to understand the dangers of ransomware and their role in safeguarding the organization.

Your employees should also be encouraged to speak up right away if something appears to be a security risk. Adopt a process that empowers them to immediately report suspicious emails and computer behavior directly to your information security team. This gives employees a feedback loop that lets them know if an attachment is safe to open. When your employee has reported an attempted ransomware attack this ensures you can immediately put all your employees on high alert.

VULNERABILITY PATCH MANAGEMENT

Patch management is an important, preventative step to your ransomware protection plan. Ensure you have a strong patch management process with the visibility you need to know which patches are your highest priority.

ASSESS

Maintain an inventory of your production systems, operating system types and versions, IP addresses, and your security controls.

ANALYZE

When a vulnerability alert is issued, consult your systems and security controls list to determine if your network is affected and if you're protected. This gives the context to decide which vulnerability patches require your immediate attention and those that you can take time to plan.

PRIORITIZE

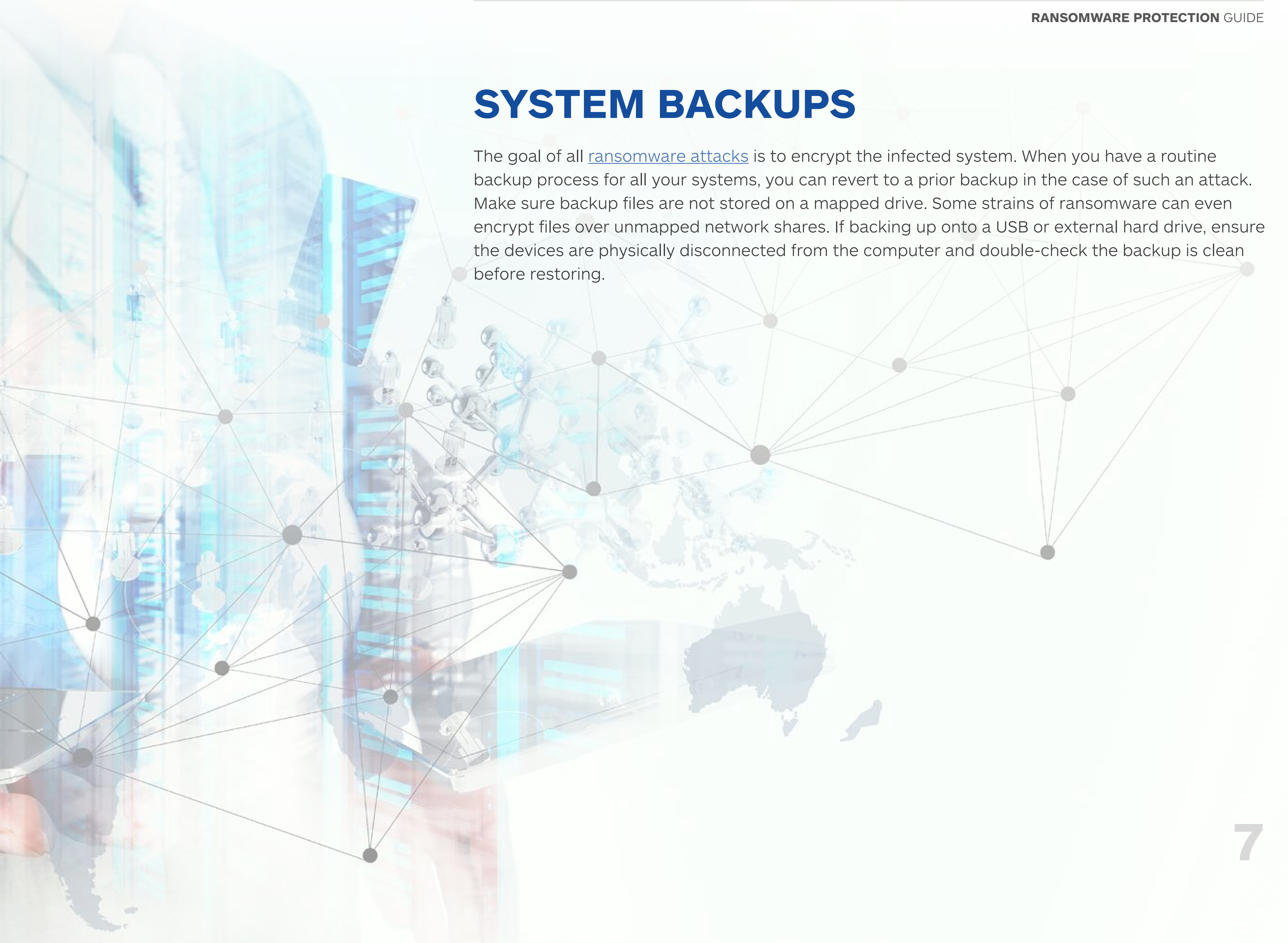
Prioritize new vulnerabilities based on your systems exposure, exploit availability, and existence of active threats in the wild.

APPLY

Non-critical updates on non-critical systems should be applied during scheduled maintenance windows. Emergency updates should be applied as soon as possible after you have confirmed the patch is stable.

SYSTEM BACKUPS

The goal of all ransomware attacks is to encrypt the infected system. When you have a routine backup process for all your systems, you can revert to a prior backup in the case of such an attack. Make sure backup files are not stored on a mapped drive. Some strains of ransomware can even encrypt files over unmapped network shares. If backing up onto a USB or external hard drive, ensure the devices are physically disconnected from the computer and double-check the backup is clean before restoring.



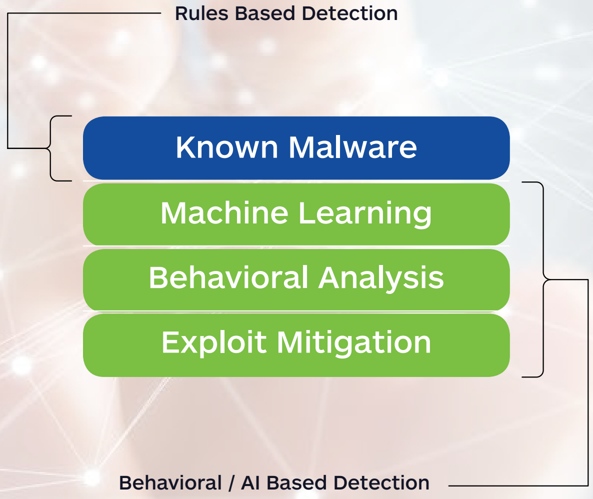
ADOPT MULTI-LAYERED ENDPOINT SECURITY

Enterprises need strong endpoint security that protects them at all stages of the ransomware attack chain. Adopt a solution with multiple protection layers for the best practice approach to detect and block ransomware attacks before they happen.

The first layer blocks known malware quickly and with low overhead. This is done with matching and rules-based technologies. Despite some claims that signatures are ineffective, they have their place in a multi-layer process. This is a lightweight method to protect against known malware without resorting to more resource-intensive techniques.

Next are dynamic layers that detect unknown and zero-day threats. Each have their strengths, yet none should be considered a perfect, "silver bullet" approach on their own. A solution with the combination of these dynamic layers provides comprehensive threat coverage across multiple vectors for both known and unknown threats.

For the best protection, we recommend your endpoint security includes the following layers:



Rules Based Detection

Known Malware

Machine Learning

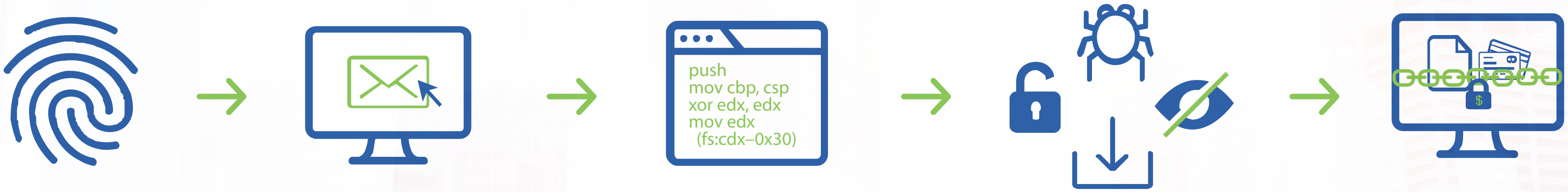
Behavioral Analysis

Exploit Mitigation

Behavioral / AI Based Detection

ABOUT MALWAREBYTES ENDPOINT PROTECTION

Malwarebytes makes it easy for your security and risk management leaders to achieve effective endpoint protection. The Malwarebytes solution combines a blend of **seven distinct and complementary technologies** to deliver leading endpoint security with simplified management and minimal end-user impact. This creates an interlocking web of matching and signature-less technologies that work together to not only block ransomware execution but also its deployment on the endpoint.



Profiling

1 Application hardening reduces the vulnerability surface, making the computer more resilient, and proactively detects fingerprinting attempts by advanced attacks.

Delivery

2 Web protection protects users by preventing access to malicious websites, ad networks, scammer networks, and "bad neighborhoods."

Exploitation

3 Exploit mitigations proactively detect and block attempts to abuse vulnerabilities and remotely execute code on the machine, which is one of the main infection vectors today.

4 Application behavior ensures that installed applications behave correctly and prevents them from being abused to infect the machine.

Payload Execution

5 Anomaly detection machine learning proactively identifies viruses and malware based on anomalies from known good files.

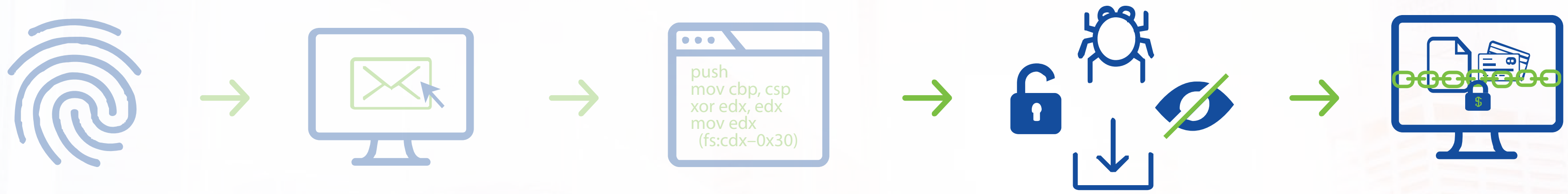
6 Payload analysis is composed of heuristic and behavioral rules to identify entire families of known and relevant malware.

Malicious Behavior

7 Ransomware mitigation is a behavior monitoring technology that detects and blocks ransomware from encrypting users' files.

MALWAREBYTES PROTECTION AGAINST WANNACRY

Malwarebytes Endpoint Security's signature-less, heuristic, and behavioral technologies fight ransomware at every stage of the attack chain. Let's look at this in action against the WannaCry ransomware.



Profiling

Application Hardening

Delivery

Web Protection

Exploitation

Exploit Mitigations

Application Behavior

Payload Execution

Payload Analysis

Anomaly Detection

(Updated after initial detection by Ransomware Mitigation)

Malicious Behavior

Ransomware Mitigation

(Zero-hour protection)

Payload Analysis

Immediately after the initial detection, the Malwarebytes Threat Intelligence Team updated the Payload Analysis layer to detect the attack earlier in the infection.

Malicious Behavior Detection

At the zero hour, the Ransomware Mitigation layer detected WannaCry and stopped the encryption of any files.

Malwarebytes

WHY MALWAREBYTES?

Malwarebytes makes it easy for your security and risk management leaders to achieve effective endpoint protection. Our solution combines a blend of distinct and complementary technologies to deliver leading endpoint security with simplified management and minimal enduser impact. This creates an interlocking web of rules-based and behavior/AI-based technologies that work together to not only block malware execution but also its deployment on the endpoint.

At Malwarebytes, we have a strong history as the go-to vendor for endpoint malware remediation. Our expertise in endpoint incident response provides thorough remediation and generates the world's most informed threat intelligence telemetry of data on zero-day malware.

TAKE YOUR FIRST STEP IN PROACTIVE PREVENTION AGAINST RANSOMWARE.

For more information about
Malwarebytes Endpoint Protection visit:
malwarebytes.com/business