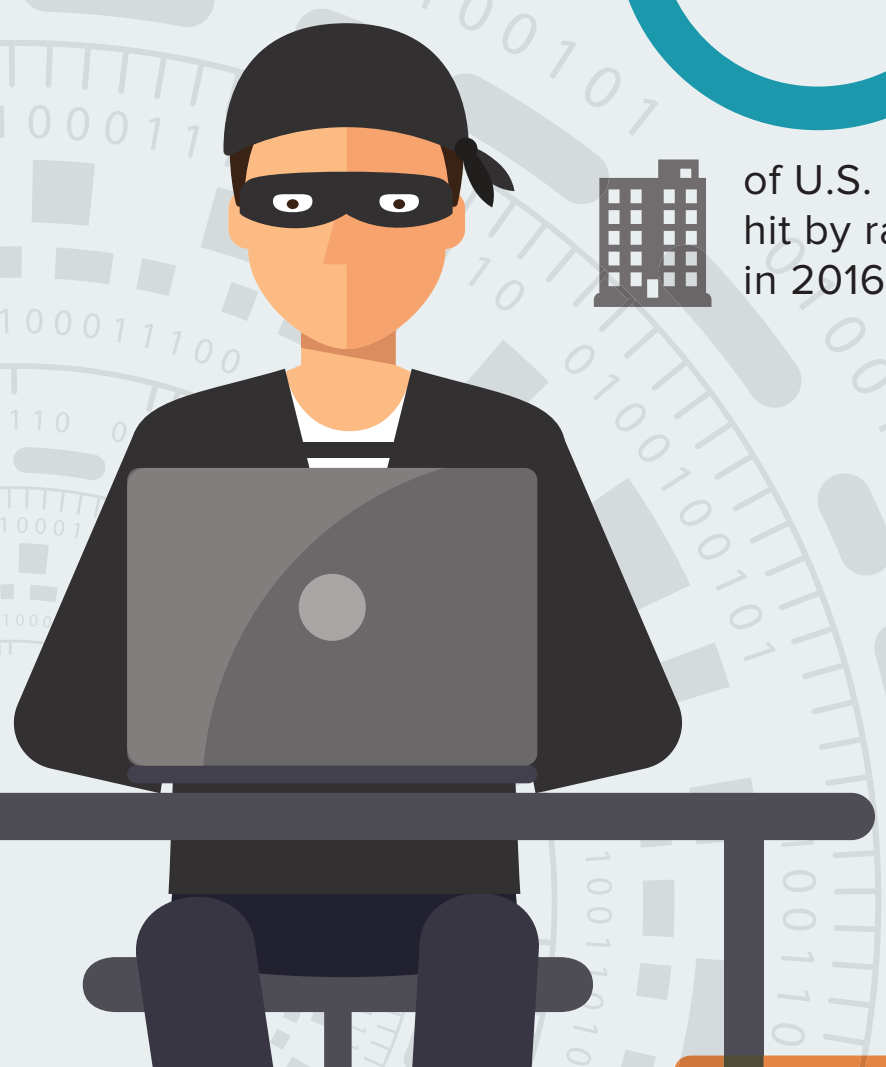
10 ESSENTIALS FOR STOPPING RANSOMWARE

A RISING THREAT



40% of U.S. enterprises hit by ransomware in 2016[1]

60% of malware is ransomware[2]

91% of malware uses DNS to carry out attacks[3]

$1 BILLION payout to ransomware criminals in 2016[5]

#1 delivery vehicle for ransomware: **PHISHING EMAIL ATTACHMENTS**[4]

6,000% increase in ransomware-infected emails in 2017 vs. 2016[6]

IT'S NOT ALWAYS ABOUT THE MONEY

Some ransomware is not designed primarily to make you pay up, but instead to disrupt operations or wipe data from computer systems.

STOP RANSOMWARE WITH THESE 10 ESSENTIALS

START WITH THE BASICS

1. WATCH YOUR BACK
Always backup your essential data.

2. STAY CURRENT
Prioritize and apply the latest security updates and patches.

3. SEGMENT FOR SAFETY
Limit spread of ransomware with network segmentation.

4. GET THE WORD OUT
Train employees in safe email and Microsoft macros best practices.

INTEGRATE AND IMPLEMENT PROACTIVE MEASURES

5. IMPLEMENT DNS RESPONSE POLICY ZONE (RPZ)
enforcement to prevent data exfiltration and block DNS communications with malicious sites and command and control servers.

6. MONITOR DNS REQUESTS
to identify suspicious DNS activity and to detect "kill switch" domains that can be used to disable some types of ransomware attacks (e.g., by redirecting requests to internal "sinkholes").

7. IMPROVE VISIBILITY AND DISCOVERY
with tools that can detect unauthorized or compromised devices and virtual machines anywhere on your network so you can automatically block their access and ensure compliance.

8. USE DATA FROM DNS, DHCP, AND IP ADDRESS MANAGEMENT
to gain valuable insights that help you see ransomware attacks in context so you can better understand risk and prioritize remediation.

9. HARNESS THREAT INTELLIGENCE
consolidated, curated, and updated—to detect, prioritize, and anticipate evolving threats.

10. INTEGRATE SECURITY RESPONSE
to accelerate remediation by sharing threat data, malicious events, and context across entire security ecosystem including endpoint security, NAC, SIEM and other technologies.

Sources: 1. 2016 Malwarebytes Survey Report 2. Malwarebytes Research 3. Cisco 2016 Annual Security Report 4. 2016 IBM Security Study 5. FBI Figures 6. 2016 IBM Security Study