

THE SOLUTION PROVIDER'S GUIDE TO FIGHTING RANSOMWARE

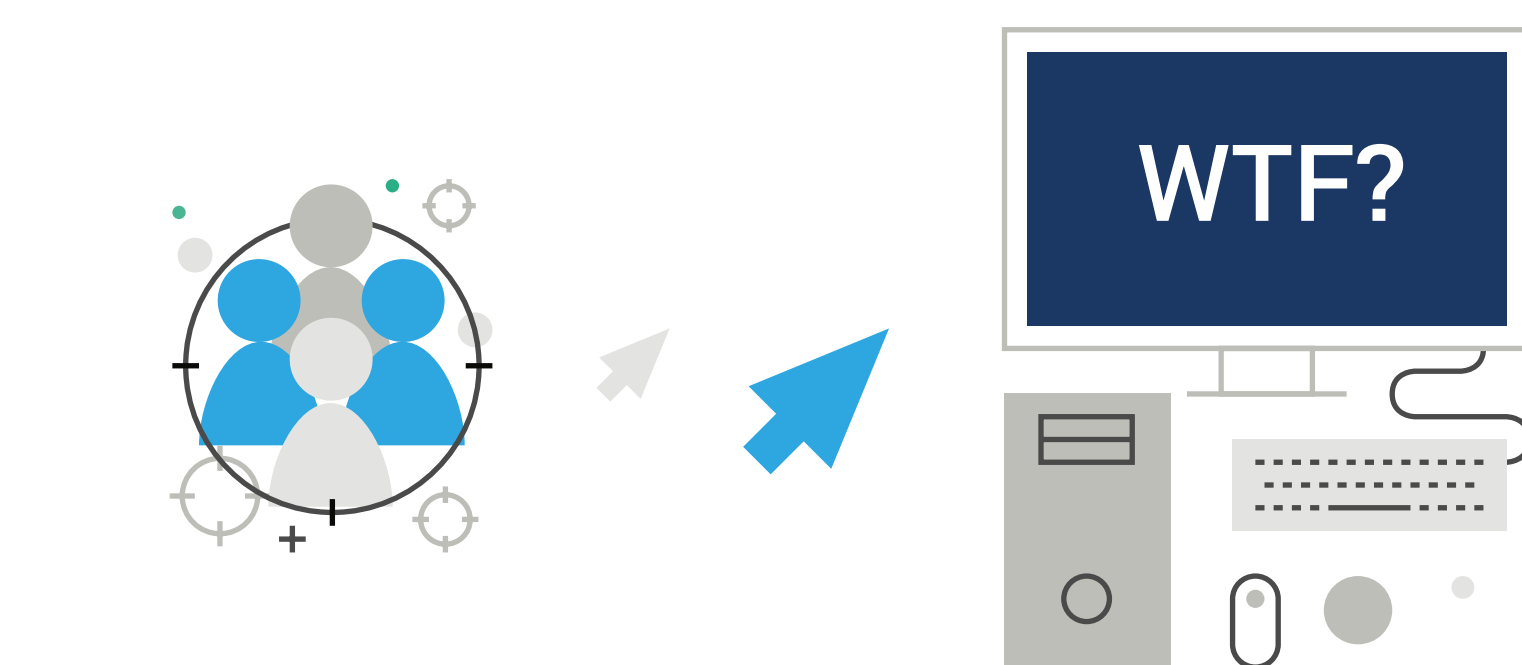
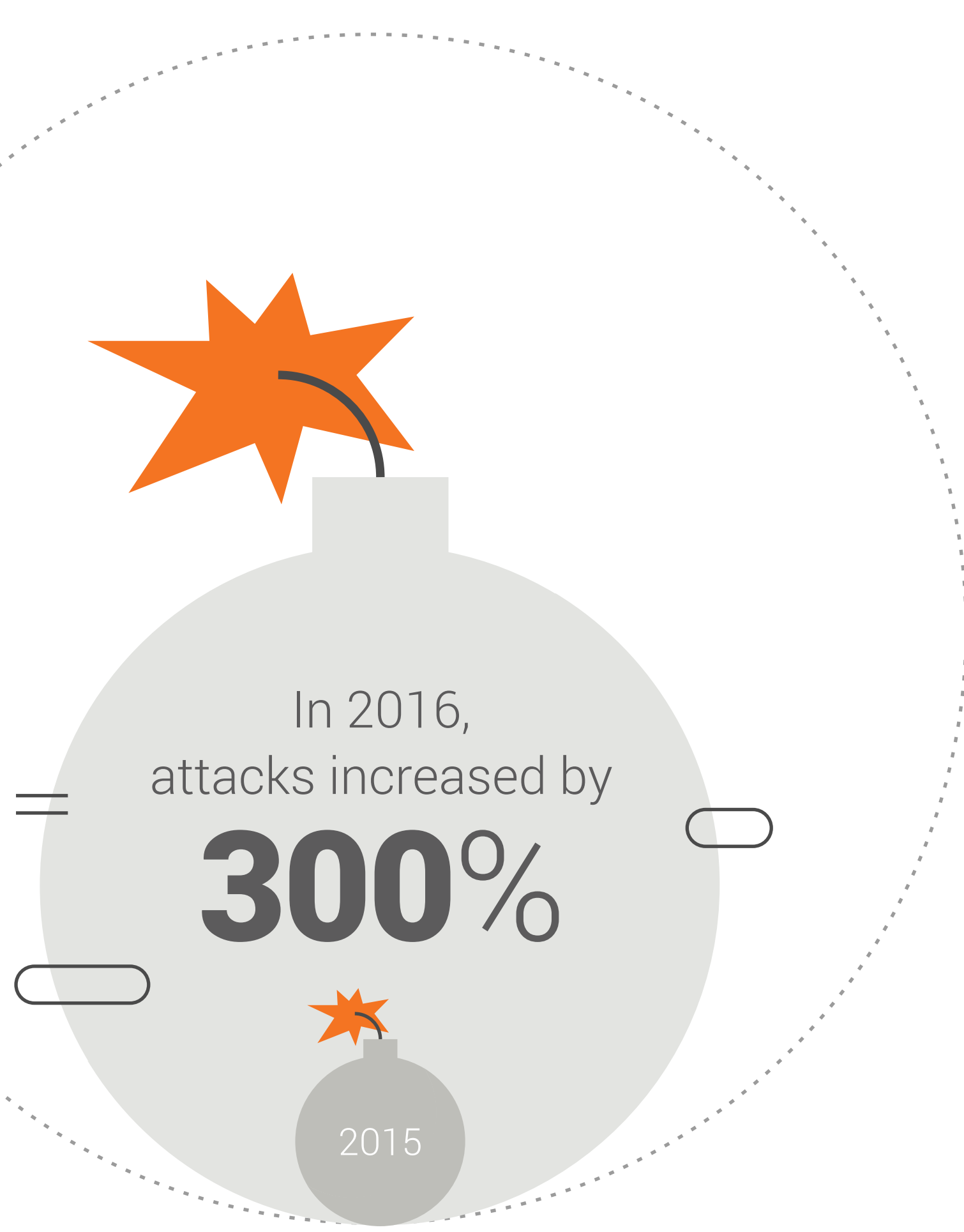


Hundreds of thousands

of ransomware attacks take place every single day. Everyone is a target. No one is immune.

Ransomware has become an epidemic and is now **one of the top concerns of cybersecurity professionals** due to the frequency of attacks and the risk of losing critical organization assets, including financial records, standard operating and even required day-to-day documents.

Most ransomware infections start when a user clicks an infected attachment or visits a compromised website. Unwittingly, the user unleashes the malware into his or her computer and if it isn't blocked, it often spreads to the entire network.

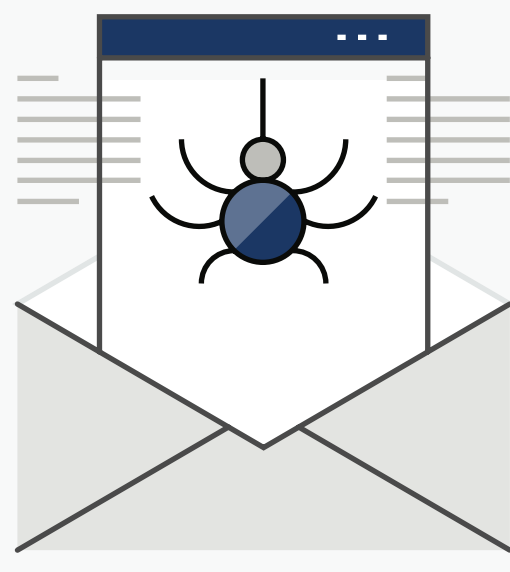


The FBI estimates that victims dished out at least **\$1 BILLION** in ransom payments in 2016.

An average of **\$4 MILLION per company**, according to the Ponemon Institute



And Juniper Research estimates the overall cost of cyberattacks will reach **\$2 TRILLION by 2019**.



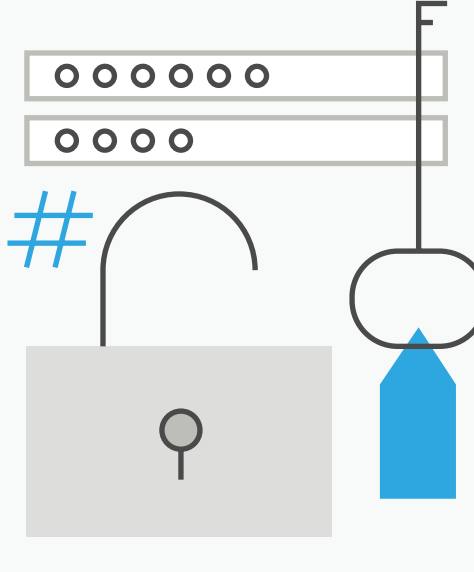
50%

of partners tell us ransomware is the **#1 concern of their clients**.



28%

of partners say clients **don't know they are at risk** of ransomware.



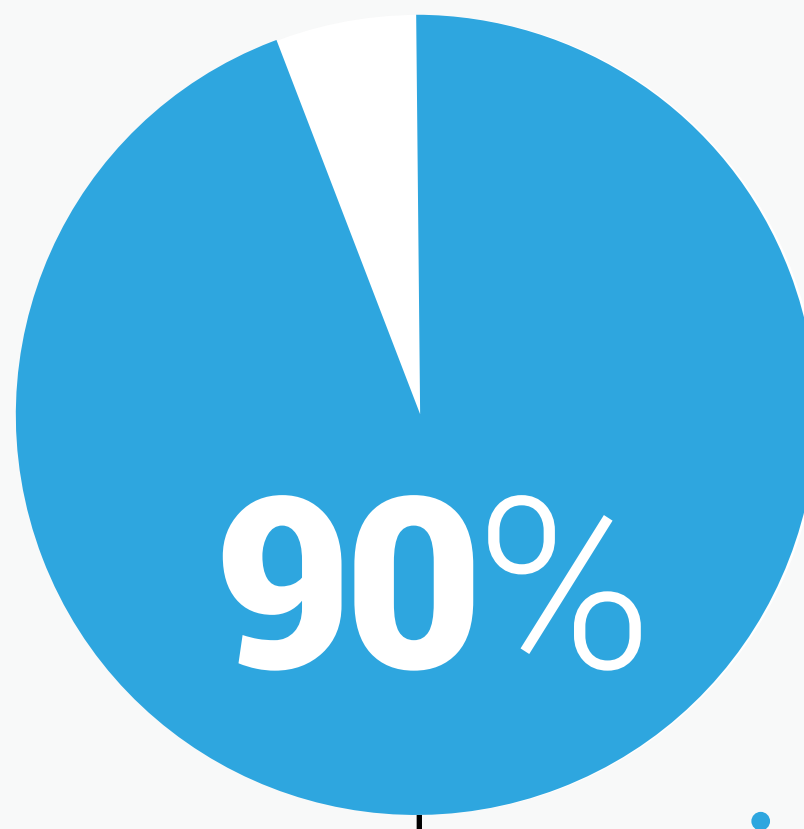
41%

of partners say not being able to guarantee protection is **their top roadblock** to selling ransomware prevention.

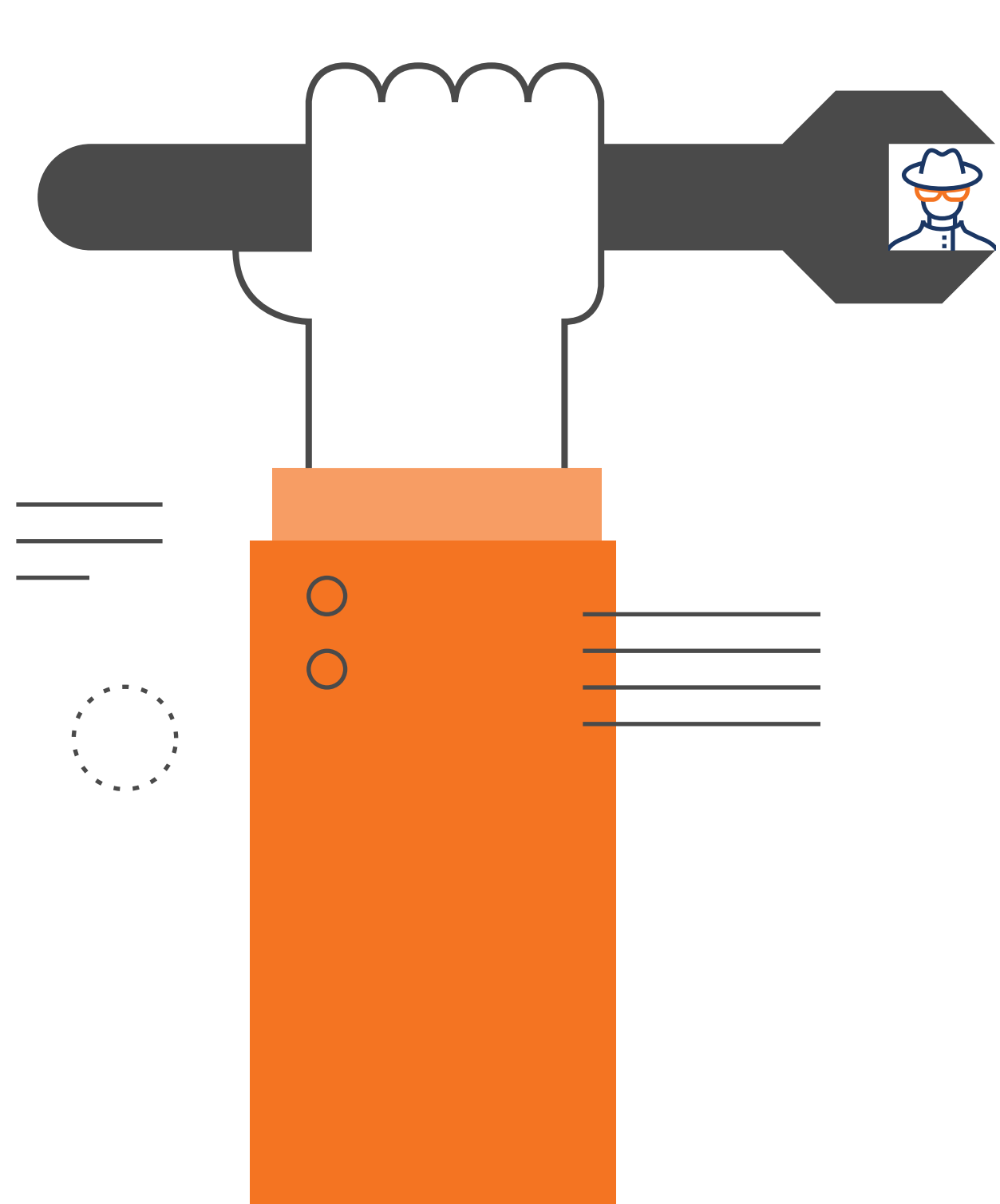


40%

of partners say accurate information on how solutions can prevent ransomware would **make selling solutions easier**.



of ransomware attacks result from phishing



To maintain a grip on the ransomware threat, solution providers must keep up with developments. New, more devious variants keep emerging as older ones fade into the sunset. Ransomware authors constantly think up new tricks to deliver variants to unsuspecting users and in some cases, they've gotten particularly creative with their demands.

Education is critical to protecting businesses from phishing attacks that can lead to ransomware infections. Solution providers should work with clients to understand, identify and avoid the risks by developing and implementing a user awareness and training program.

In addition to keeping up with threat developments and educating users, solution providers also must deliver the tools that help deter ransomware attacks. This should start with an assessment of each client's vulnerability level.

Endpoint security is essential in the fight against ransomware.

Tools should cover more than the basics of scanning for known viruses. Businesses need an advanced solution with built-in intelligence to identify known malware and phishing threats, as well as zero-day threats and any suspicious code that could turn out to be a new malware variant.

Protection should include the following:

- » Strong, advanced endpoint protection with machine learning and other sophisticated technologies to prevent unknown threats
- » Intelligent anti-phishing defense
- » Firewalls and web filters that block access to IP addresses known to be malicious
- » Email filters that block suspicious files and URLs from addresses known to be malicious
- » Patch management for all operating systems, applications and firmware
- » Behavior analysis to detect zero-day threats
- » Identity management to limit user access to only the resources they need
- » Data backup and recovery, preferably with frequent incremental backups



311 Park Place Blvd, Suite #300, Clearwater, FL 33759
Telephone and Email inquiries



VIPRE offers superior ransomware protection by preventing many of these threats before they can infect PCs. Using the top-rated VIPRE antivirus engine that consistently scores a 100% blocking rate, zero false positives, VIPRE provides a strong defense against phishing attacks, malicious URLs, Zero-day exploits and other online threats used to spread ransomware. Its Advanced Active Protection capabilities add an additional, sophisticated layer of ransomware defense by using cloud-based security services and behavioral analysis to prevent these pervasive threats.

Learn more by downloading our eBook:

<https://vipre.com/partners/partner-ransomware-ebook.pdf>

