

# The Race Against Ransomware

## A Proven Road To Better Security

### Ransomware

#### A roadblock that's here to stay

While new types of attacks like cryptomining have entered the race, ransomware is still a huge obstacle for businesses. Learn how Cisco customers are staying ahead of today's threats.

*"We reduced time to detect threats by more than a month with Cisco Email Security."*

— Muscogee County School District<sup>1</sup>

The hype surrounding large-scale ransomware attacks such as NotPetya, which the White House called "the most destructive and costly cyberattack in history," has died down a bit.<sup>2</sup> However, today's ransomware reality is still very daunting.

EVERY  
**14**  
SECONDS

By the end of 2019, businesses will **fall victim to ransomware** every 14 seconds.<sup>3</sup>

Welcome to the City of Aspen, Colorado<sup>4</sup>  
Population: 6,658

*"We have seen a reduction in malware infections from several a week to practically zero [with Cisco Umbrella]."*

**\$11.5**  
BILLION

\$11.5 billion global ransomware damages predicted annually by 2019<sup>5</sup>

### Security speed bumps: What's slowing us down?

The massive growth of Internet-connected devices, explosion of attack methods, and shortage of qualified security professionals have all contributed to the rise of ransomware.

Some of the world's largest and most prestigious **organizations have been stopped in their tracks** due to ransomware in recent years.

**69%**  
of organizations **don't believe** their anti-virus solutions provide adequate protection.<sup>6</sup>

**40%**

**Over 40%** of companies have sensitive **files that are unprotected** and open to every employee.<sup>4</sup>

### Driving forward: Where do we go now?

Today's sophisticated cyberattacks require a thorough, layered security approach. There is no one technology that will eliminate ransomware roadblocks.

At the same time, throwing a multitude of disjointed solutions at the problem will not clear the path either.

Organizations need to think of security more holistically and adopt solutions that complement each other and work together to steer attackers and malware off course. Cisco offers a multi-pronged approach to Ransomware Defense to put your security into overdrive.

*"Cisco AMP for Endpoints has enabled us to detect malware and ransomware that other anti-virus products we previously used had missed."*

— Nichel International<sup>7</sup>

*"Cisco AMP for Endpoints increased endpoint visibility by 90 percent, detected 90 percent more threats, and reduced incident response time to less than a day."*

— Saudi Arabia National Guard<sup>8</sup>

### Cisco paves the way

In the race against ransomware, having the best cars and drivers is vital. However, accidents can still happen, so it's good to also have the best responders in your pit crew.

*"We have had zero malware infections since the implementation of Cisco Umbrella three years ago."*

— Mid-Sized Financial Services Company<sup>9</sup>

### Cisco Ransomware Defense



#### Cisco AMP

Discover, contain, and remove advanced malware, zero-day attacks, and persistent threats.



#### Cisco Email Security

Stop phishing, ransomware, and spam from compromising your environment by blocking malicious communications.



#### Cisco Umbrella

Obtain a first line of defense against threats on the Internet, whether users are on or off the corporate network.



### Test Drive Cisco Ransomware Defense

Start Here



© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

1. TechValidate, <https://www.techvalidate.com/vendor-research/cisco>. 2. The White House, Statement from the Press Secretary, February 2018. 3. Cybersecurity Ventures, "Global Ransomware Damage Costs Predicted To Hit \$11.5 Billion By 2019," November 2017. 4. TechRepublic, "Report: 41% of companies have 1,000+ sensitive files open to every employee," April 2018. 5. Ponemon Institute, The 2017 State of Endpoint Security Risk, November 2017.