# Cisco Ransomware Defense: Keep ransomware at bay

What if you could stay safer from ransomware, however it may attempt to get into your network? Cisco shares threat information across all points of attack to bring a more unified solution to your problem.

## Overview

Files and information are the lifeblood of an organization. Keeping this information—and your organization's productivity—intact and secure is nonnegotiable.

But in comes ransomware—malicious software, or malware—that locks up the information on an organization's computers like documents, financial records, customer data. It will not release these files until the user pays a fee, or ransom, to unlock these files and get them back. Without the appropriate defenses, ransomware can inflict enough damage to reduce an organization to operating with pen and paper.

Ransomware is commonly delivered through exploit kits, malvertising (infected ads on a website that can deliver malware), phishing (fraudulent emails masquerading as trustworthy), or spam campaigns. The actual infection can begin when someone clicks on a link or an attachment in a phishing email. Infections can subsequently spread laterally through an organization by exploiting unpatched vulnerabilities with worm-like efficiency.

Cisco® Ransomware Defense reduces the risk of ransomware infections with an layered, architectural approach from the endpoint to the network, email, and the web. We deliver integrated defenses so they work together to provide ultimate visibility with ultimate responsiveness against ransomware.

## Benefits

- **Reduce the risk of ransomware** so you can keep focused on running your business
- **Get immediate protection** with security that can block threats before they attempt to take root
- **Gain exceptional visibility and responsiveness** from the DNS layer to the network to the endpoint
- **Prevent malware from spreading laterally** with strong network segmentation
- **Block more, faster with Talos threat intelligence** across all threat vectors

© 2017 Cisco and/or its affiliates. All rights reserved.

## A fast-growing, powerful threat

This is the year of ransomware. And it is proving to be seriously profitable. Ransomware has quickly become the most lucrative type of malware ever seen.

The FBI has said ransomware is on the way to becoming a $1 billion annual market. Cisco Talos research shows that a single ransomware campaign can generate up to $60 million annually.

Attackers have the funds and the desire to continue innovating ransomware strands that will become far more virulent. We believe that ransomware will become more capable of self-propagating, with the aim of locking up vast swaths of corporate networks. That would effectively knock corporate IT functionality back to the 1970s.

Current responses to ransomware tend to revolve around single point products. We must consider bringing a more architectural approach to bear given the various vectors that ransomware targets.

This solution overview addresses the various vectors and methods that attackers use. Defenders must:

- Secure both email and the web
- Block access to malicious infrastructure on the Internet
- Stop any ransomware files that make it all the way to an endpoint
- Block the command-and-control callbacks used
- Prevent lateral movement of ransomware should an infection occur

© 2017 Cisco and/or its affiliates. All rights reserved.

## What you buy

Cisco Ransomware Defense brings together all the necessary pieces of the Cisco security architecture to address the ransomware challenge. You can choose all the pieces or select ones that fulfill an immediate security need.

Ransomware Defense comprises:

- **Cisco Umbrella,** which blocks threats at the network layer, far away from your network
- **Cisco Advanced Malware Protection (AMP) for Endpoints,** which blocks malicious ransomware files from running on endpoints
- **Cisco Email Security,** which stops phishing and spam messages seeking to deliver ransomware

Advanced Malware Protection can be immediately added to email security products through an easy license for static and dynamic analysis (sandboxing) of unknown attachments that traverse the Cisco Email Security gateway.

With Ransomware Defense, you can use your network as an enforcer to contain the spread of ransomware. It will not be able to propagate as easily on the network in the worst-case scenario of an infection. Cisco Security Services can provide immediate triage in the case of an outbreak. They also streamline deployments and help ensure that the solution is configured to provide the greatest possible effectiveness in your environment.

## Key capabilities

- Block ransomware from getting into the network or being downloaded onto laptops
- Contain ransomware in worst-case scenarios should it enter the network
- Shared threat intelligence across all products for a unified, concerted defense

**“We have covered a great risk in the web attack vector of ransomware and greatly improved our user experience in regards to Internet connectivity.”**

**Jason Hancock, Global Senior Network Engineer, Octapharma**

## Next steps

Keep your business focused on what it does best by contacting your Cisco sales representative for more information on Cisco Ransomware Defense. Visit our webpage at: https://www.cisco.com/go/ransomware.

## Security Services help you fight ransomware

The Cisco Security Services Incident Response team can provide both incident response readiness services and reactive incident response in the case of ransomware outbreaks.

Additionally, Cisco Security Integration Services address solution-level architectural challenges. Our team has deep expertise in delivering integrated security solutions to speed the adoption of needed security technology, such as AMP, with little disruption.

More broadly, organizations must also ensure they have appropriate data backup technology and policies in place to hedge against the impacts of a ransomware infestation.

## Cisco Capital

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

## The Cisco advantage

Ransomware will find a way into your organization through any means necessary. Phishing emails, compromised web banners, spam—many vectors need to be protected. Only Cisco brings a security architecture to bear in confronting the ransomware challenge. Point products alone lack the ability to share visibility and threat intelligence across multiple products and threat vectors. Cisco Ransomware Defense is backed by our industry-leading Talos Research Group, which shares ransomware behaviors and details across web, email, and endpoint products. With Talos, threats seen in email can be subsequently blocked from web connections and endpoint transfers, and vice-versa. This ‘see it once, block it everywhere’ capability reduces time to detect, protects users wherever they are, and just may be what keeps your company name out of tomorrow’s headlines.

© 2017 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: https://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. (1110R)

C22-737492-02 10/17