Cisco Ransomware Defense: Keep Ransomware at Bay

What if you could stay safer from ransomware, however it may attempt to get in? Only Cisco gives you the security products and architecture to do so.

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 a individual's or an organization's computer like documents, photos and music. 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 phishing emails. Infections can also happen when users surf to sites with malicious ads that automatically infect computers.

Enter Cisco® Ransomware Defense. It reduces the risk of ransomware infections with a layered approach, from the DNS layer to the endpoint to the network, email, and the web. We deliver integrated defenses with an architectural approach that combines ultimate visibility with ultimate responsiveness against ransomware.

Benefits

- **Reduce risk of ransomware** so you can keep focused on running your business
- **Get immediate protection** with security that can block threats before they can attempt to take root
- **Gain unmatched visibility and responsiveness** from an architectural approach from the DNS layer to the network to the endpoint
- **Prevent malware from spreading laterally** with strong network segmentation
- **Get industry-leading Talos threat research** and intelligence on ransomware

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 it is on way to becoming a $1 billion annual market. Cisco Talos research shows that a single ransomware campaign can generate up to $60 million annually. Ransomware is gaining so much attention it is has been featured on broadcast TV shows.

Attackers have the funds and 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 it targets to gain infections.

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 and prevent easily lateral movement of ransomware should an infection occur.

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 DNS 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, both cloud and on premises, which stops phishing and spam messages seeking to deliver ransomware
- Advanced Malware Protection can be immediately added to email security products via an easy license for static and dynamic analysis (sandboxing) of unknown attachments that traverse the Cisco email security gateway
- Cisco Firepower™ next-generation firewall (NGFW), which blocks command-and-control traffic and any malicious files traversing the network
- Cisco ISE via the Cisco network dynamically segments your network, so ransomware cannot spread laterally

With Ransomware Defense, organizations can use their network as an enforcer to contain the spread of ransomware. It will not be able 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 incident response after an outbreak. They also streamline deployments of AMP, NGFW, and other solution products.

Key Capabilities

- Block ransomware from getting into the network or downloading onto laptops
- Contain ransomware in worst case scenarios should it enter the network

Security Services Help 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. It streamlines the deployment of solution technologies like AMP for Endpoints and Cisco Firepower NGFW. Our team has deep expertise in delivering integrated security solutions to speed the adoption of needed security technology with little disruption.

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

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

– Octapharma

Cisco Capital

Financing to Help You Achieve Your Objectives

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 will not suffice. Our solution is backed by our industry-leading Talos Research Group, which has carried out extensive threat research on ransomware, powering our effective layered protection. We will block ransomware and even fight it if it slips through the cracks and gets into your network—which may well be an unfortunate reality.

C22-737492-01 08/16