LEARNING MADE EASY

# Ransomware Defense Checklist

The rise of ransomware has quickly become an extremely lucrative criminal enterprise, as targeted organizations often pay the ransom to get their data back quickly. But every single organization that pays to recover its files is directly funding the development of the next generation of ransomware. As a result, ransomware continues to evolve, with more sophisticated variants and more specific targeted attacks. Recent research from Cybersecurity Ventures predicts ransomware attacks will cost the global economy $6 trillion annually by 2021!

Ransomware must be prevented when possible, detected when it attempts to breach a network, and contained to limit potential damage when it infects systems and endpoints. Ransomware defense calls for a new best-of-breed security approach that spans the organization from the network edge, to the domain name system (DNS) layer, all the way to the data center and across endpoint devices, no matter where they're being used.

## What Is Ransomware?

Ransomware is malicious software (malware) used in a cyberattack to encrypt the victim's data with an encryption key that is known only to the attacker, thereby rendering the data unusable until a ransom payment (usually cryptocurrency, such as Bitcoin) is made by the victim.

- Ransom amounts are typically high, but usually not exorbitant, to get victims to simply pay the ransom as quickly as possible, instead of contacting law enforcement and potentially incurring far greater costs due to the loss of their data and negative publicity.
- Ransomware is commonly delivered through exploit kits, waterhole attacks (in which one or more websites that an organization frequently visits is infected with malware), malvertising (malicious advertising), or email phishing campaigns.
- Ransomware typically identifies user files and data through some sort of an embedded file extension list. Files that match one of the listed file extensions are then encrypted. The ransomware then typically leaves instructions for the victim on how to pay the ransom.

**Use this checklist to prepare your organization to effectively defend against ransomware threats:**

## Best Practices to Reduce Ransomware Risks

**Before an attack: discover, enforce, harden**

- [ ] Conduct regular security awareness and training for your end users. This training should be engaging and contain the latest information on security threats and tactics.
- [ ] Perform ongoing risk assessments to identify any security weaknesses and vulnerabilities in your organization, and address any threat exposures to reduce risk.

**During an attack: detect, block, and defend**

- [ ] Communicate timely and accurate information to all stakeholders.
- [ ] Share incident response data and intelligence throughout the security architecture.

**After an attack: scope, contain, and remediate**

- [ ] Resume normal business operations, including restoring backups and reimaging systems, as necessary.
- [ ] Collect and preserve evidence for law enforcement and auditing purposes.
- [ ] Analyze forensic data to predict and prevent future attacks, for example, by identifying related domains and malware with the associated IP addresses, file hashes, and domains.
- [ ] Perform root cause analysis, identifying lessons learned, and redeploying security assets, as necessary.

## Building the New Best-of-Breed Security Architecture

To safeguard businesses against ransomware and other modern threats, a new best-of-breed security architecture leverages an integrated, portfolio-based approach that is simple, open, and automated, rather than traditional point products. This new architecture consists of the following components:

- [ ] **Next-generation firewalls (NGFWs) and next-generation intrusion prevention systems (NGIPSs)** with visibility into intrusion events, with data enrichment from other security products
- [ ] **Threat intelligence** from industry-leading sources and cloud-based product data, with the ability to collect and prioritize high-urgency incident data for further investigation and response
- [ ] **Domain name system (DNS) layer security** to extend protection beyond the organization's firewalls
- [ ] **Secure web gateway** to protect across all ports and protocols
- [ ] **Cloud access security broker (CASB)** to protect against risky, unauthorized cloud apps
- [ ] **Highly granular, software-defined network segmentation** with role-based policy enforcement regardless of location, device, or IP address
- [ ] **Email, web, and endpoint security** to expand visibility and correlate threats
- [ ] **Advanced malware protection** with sandboxing capabilities from the network to the endpoint
- [ ] **Automated platform integrations**, along with centralized visibility and management, to tie components together and make life easier for your security operations team

## Deploying Cisco Ransomware Defense

Cisco Ransomware Defense offers an integrated approach that provides protection from ransomware and is backed by unmatched threat intelligence from Cisco Talos. Cisco's unified security architecture brings together complementary security products including DNS-layer, web, email, endpoint, and network security.

- [ ] **DNS-layer security:** Cisco Umbrella stops ransomware attacks (and other cyberattacks) before they start, by blocking Internet connections to malicious sites serving up ransomware.
- [ ] **Malware protection:** Cisco Advanced Malware Protection (AMP) for Endpoints delivers a complete framework of detection capabilities and big data analytics to continuously analyze files and traffic in order to identify and retrospectively block advanced malware threats at the first sign of malicious behavior.
- [ ] **Email security:** Cisco Email Security with AMP blocks spam, phishing emails, malicious attachments, and suspicious URLs, which are important attack vectors for ransomware.
- [ ] **Network protection:** Cisco Firepower threat-focused next-generation firewalls (NGFWs) deliver an integrated threat defense across the entire attack continuum — before, during, and after an attack — with unparalleled visibility and embedded Cisco TrustSec technology that delivers dynamic software-defined network segmentation.
- [ ] **Incident response:** Cisco Security Advisory Services include deployment services for Cisco Ransomware Defense solutions including Firepower and AMP, as well as incident response.

TIP

**It may seem like there are a lot of tools in this list. The good news is, you don't have to log into each one and manage them separately! Cisco Threat Response automates integrations across many Cisco security products and aggregates their intelligence sources into an integrated platform.**


**Discover how to:**

- **Reduce risk of ransomware**
- **Get immediate protection against attacks**
- **Prevent malware from spreading laterally**

To find out how to keep your business protected, we recommend *Ransomware Defense for Dummies - Cisco 2nd Special Edition.*

**READ THE EBOOK**

CISCO

dummies
A Wiley Brand



Wiley part no.: 978-1-119-68281-3