



# Ransomware Defense Validated Design Guide

SAFE Design Guide

Security Domain: Threat Defense

September 2016

# Contents

Contents .....	2
Introduction.....	3
SAFE Introduction .....	4
Ransomware Overview.....	5
Ransomware Infection .....	6
Common vectors of infection into an organization.....	6
Ransomware Communications .....	8
Ransomware Kill Chain .....	9
Ransomware Defense.....	10
Best Practices .....	12
Things you can do .....	12
Recovery in the event that the worst has happened .....	12
Solution Architecture .....	13
Phase One—Validated Testing .....	14
Email Security .....	15
DNS Security.....	16
Anti-Malware Security.....	17
Threat Intelligence.....	18
Phase Two—Campus Reference Architecture .....	20
Advanced Web Security .....	20
Network Monitoring.....	21
Identity-based Segmentation .....	21
Infrastructure Segmentation and Intrusion Prevention .....	22
Architecture Summary.....	23
Implementation and Validation.....	24
Cisco Cloud Email Security .....	24
Cisco Umbrella DNS Security .....	33
Cisco Advanced Malware Protection for Endpoints (AMP) .....	40
Validation Testing .....	45
Summary .....	46
References .....	47
Appendix A .....	48
Lab Diagram .....	48

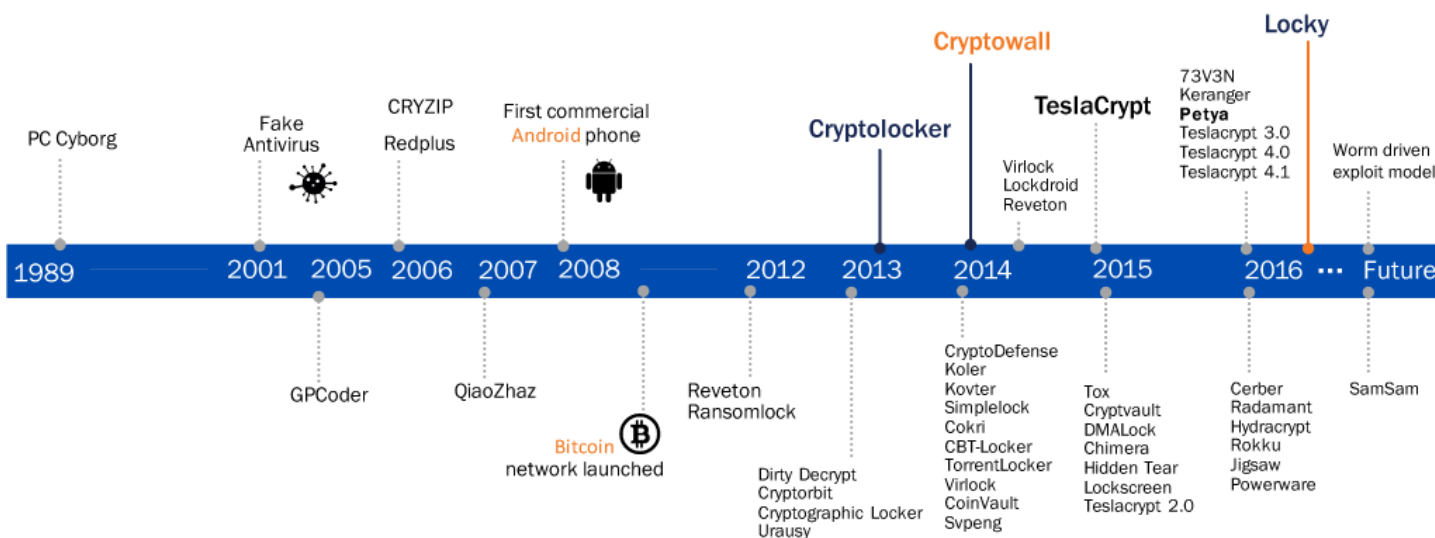
# Introduction

Ransomware is the most profitable type of malware in history. In the past, malware typically did not deny access to systems or destroy data. Attackers primarily tried to steal information and maintain long-term access to the systems and resources of their victims. Ransomware has changed the game from stealthy undetected access to extortion.

Every single business or person who pays to recover their files, makes this payment directly to the attackers. The relatively new emergence of anonymous currencies such as Bitcoin and Ripple gives attackers an easy way to profit with relatively low risk, making ransomware highly lucrative and funding the development of the next generation of ransomware. As a result, ransomware is evolving at an alarming rate, as shown in Figure 1. It is projected that future versions will propagate like worms, spreading throughout an organization in a coordinated manner and aggregating the ransom demand.

Figure 1—Evolution of Ransomware

## The Evolution of Ransomware Variants



Cyber-criminals collected \$209 million in the first three months of 2016 by extorting businesses and institutions to unlock computers. At that rate, ransomware is on pace to be a \$1 billion a year criminal industry this year. The Angler Exploit kit, which infects your system and deploys the ransomware, will be responsible for over \$60 million this year alone<sup>1</sup>.

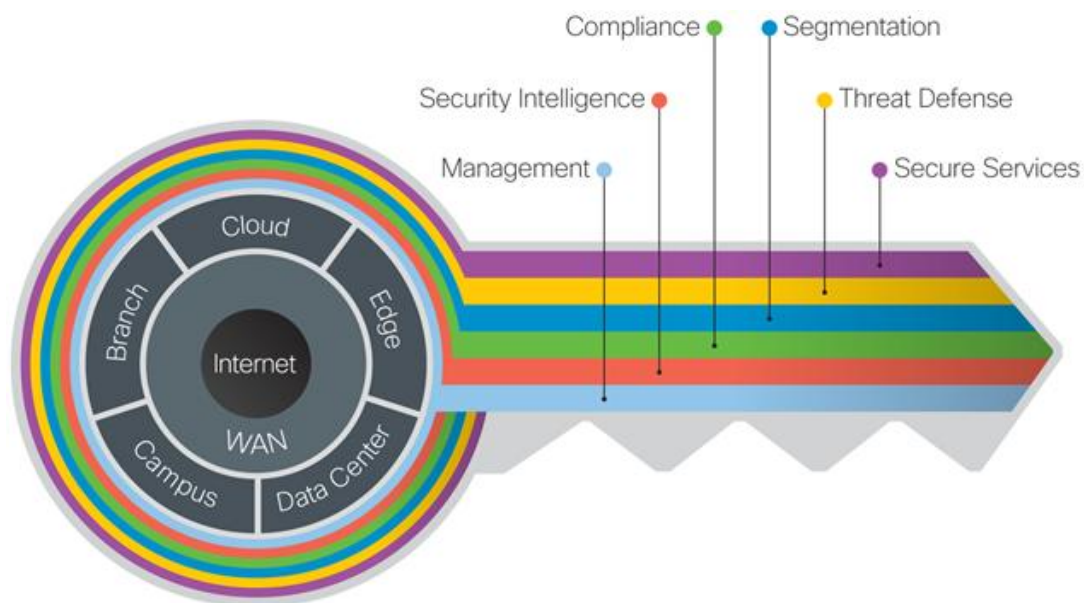
Cisco can help protect your business from the ransomware threat using a defense-in-depth architecture, protecting your users both inside and outside the network.

<sup>1</sup> Ransomware: Past, Present, and Future - <http://blog.talosintel.com/2016/04/ransomware.html>

# SAFE Introduction

SAFE simplifies complexity across the enterprise by implementing a model that focuses on the areas that an organization must secure. This model treats each area holistically, focusing on today's threats and the capabilities needed to secure each area against those threats, as shown in Figure 2. Cisco has deployed, tested, and validated these critical business challenges.

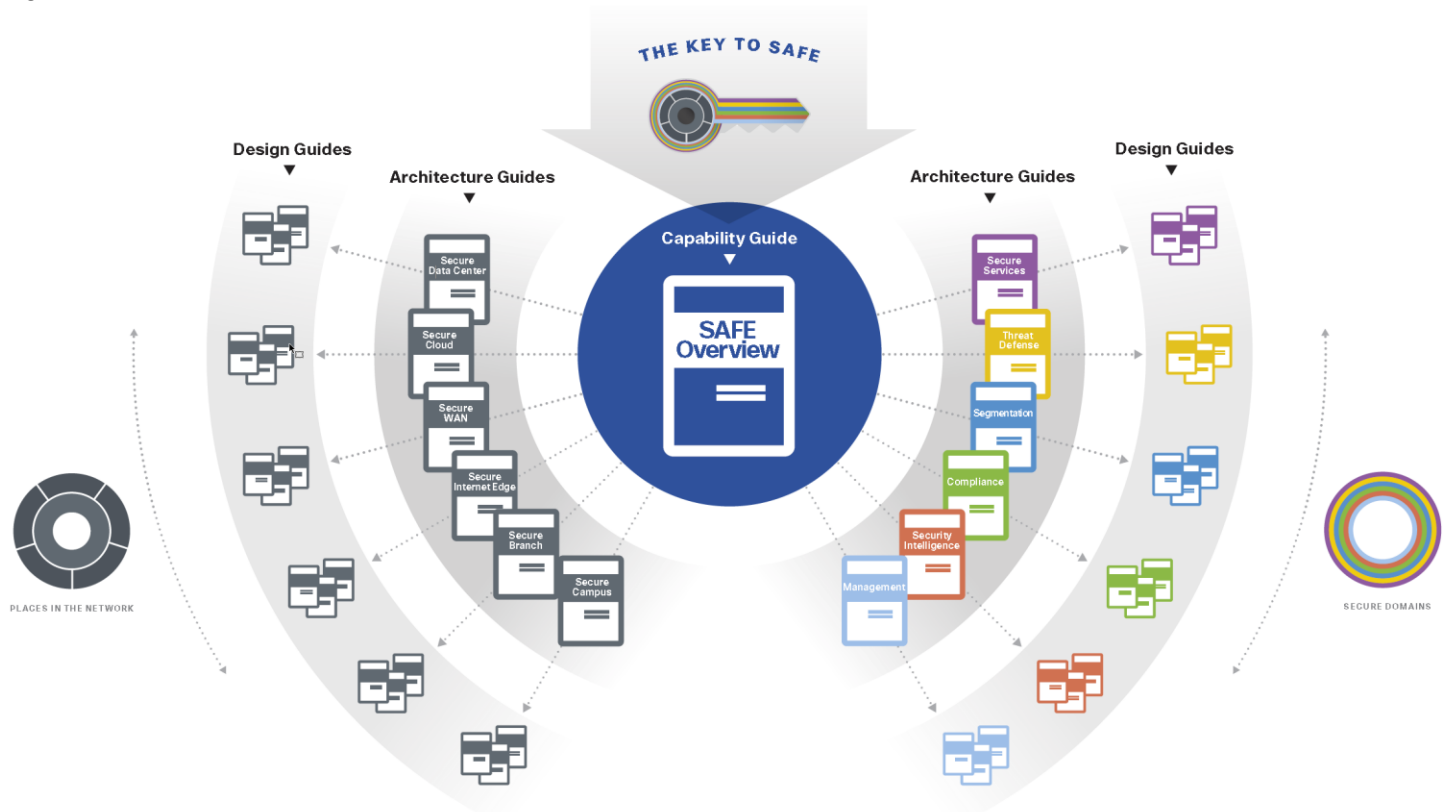
Figure 2—The SAFE Solution



*The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains.*

SAFE simplifies end-to-end security by using views of complexity depending on the audience needs, as shown in Figure 3. Ranging from business flows and their respective threats to the corresponding security capabilities, architectures, and designs, SAFE provides guidance that is holistic and understandable.

Figure 3—SAFE Guidance



More information about how Cisco SAFE simplifies security can be found here: [www.cisco.com/go/safe](http://www.cisco.com/go/safe)

This design guide addresses a specific use case of ransomware under the SAFE Threat Defense domain. The design validation for this solution use case includes Cloud services and offerings. Additionally, this guide includes a recommended architecture for the Campus PIN, which is still undergoing validation testing.

## Ransomware Overview

Businesses and individuals can be taken hostage by malware that locks up critical resources—ransomware. Ransomware uses traditional malware attack vectors such as phishing emails and exploit kits to deliver the ransomware to a desktop. Once established, it takes over systems and stored data, encrypting their contents, denying access, and holding them hostage until a ransom is paid. Ransomware uses well-established public/private key cryptography, so that the only way to recover the files is to either pay of the ransom or restore files from backups. Typically, if the ransom demand is paid, the attacker often, but not always, provides the decryption keys to restore access.

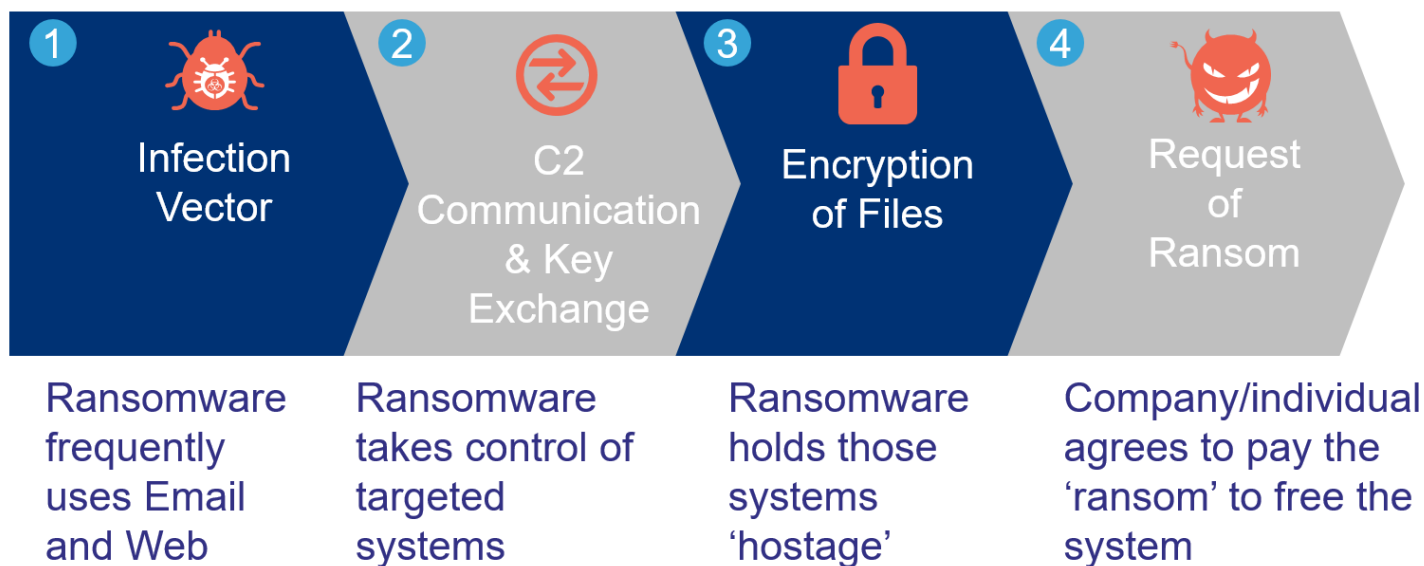
The denial of access to these critical resources can be catastrophic to businesses:

- Healthcare—Hospitals might lose the ability to provide patients with real-time care (admittance, surgeries, medications, and so on.)
- Public safety—Responders might not being able to respond to 911 or emergency calls
- Financial—Banking systems might go offline for trading or banking activities
- Retail—The inability to process payments so that customers are not able to make purchases

# Ransomware Infection

Figure 4—Typical Ransomware Infection Steps

## Typical Ransomware Infection steps



1. Ransomware is commonly delivered through mass phishing campaigns, malvertising, or targeted exploit kits.
2. After delivery, ransomware takes control of your system and may try to communicate back to its command and control infrastructure to create and transmit the public/private keys used to encrypt the files.
3. After the ransomware has the necessary keys, it identifies specific file types and directories to encrypt and avoids many system and program directories, ensuring stability for delivery of the ransom after it finishes running.
4. After encryption completes, a notification is left for the user with instructions on how to pay the ransom.

## Common vectors of infection into an organization

There are many ways an organization can be compromised by ransomware. The most common are email phishing attacks and web-hosted malvertising.

**Email**—Email is a one-to-many infection vector when used with distribution lists and mass mailings. It is common for a single user to manage multiple email accounts, both personal and corporate. Every account represents a security threat. For example, although IT organizations spend enormous time and effort to select mail security services such as Cisco Email Security Appliance or Cloud, it is very common for the users to check their personal email using public email services such as Hotmail and Gmail. These private email accounts are easily accessed through web portals that bypass these email security services. Accessing, downloading, and executing email attachments and phishing links from such accounts are a major concern.

**Web**—Malvertising ads are criminally-controlled advertisements that intentionally infect systems installing exploit kits or ransomware directly. These can be any ad on any site, and are often sites accessed on a daily basis. When a user clicks on the ad, they are taken to a site that then infects their

computer. Malvertisement networks comprise thousands of network domain names, creating a shared infrastructure that is constantly changing. These domain names can be random or semi-structured, but all have a relatively short lifespan and are replaced frequently. These domains host the exploit kits, tools and command and control services criminals use to infect, control, and disrupt systems. Almost all of these communications are encrypted.

There are multiple ways that users can interact with malvertising, such as simply visiting a site that serves ads, or clicking on a link in a page of search results or an e-mail<sup>2</sup>. Savvy web surfers often implement adblockers on their systems for protection, but this can impact a site's ad revenue, so there is a battle restricting content and requiring adblocks to be disabled. Although major sites can limit access to their sites based on the use of an adblocker, these publishers cannot guarantee that the ads served will not be malicious. These sites and services are prime targets for compromise and redirection.

Ransomware is aggressively evolving to adopt the most invasive features of other malware (for example, Nimda, Sasser, Code Red, SQL Slammer, Sality, Conficker), spreading into and infecting an entire enterprise network, encrypting all the data they can access for a larger lump-sum payout. To prepare for this future, a defense-in-depth architecture that includes deep network visibility will be critical in protecting the network.

---

<sup>2</sup> <http://blog.talosintel.com/2016/05/spin-to-win-malware.html>

## Ransomware Communications

Ransomware communications include command and control (C2) callback methods for obtaining encryption keys and payment messaging, as shown in Table 1.

Table 1 - Ransomware Communication Methods

NAME*	Encryption Key				Payment Msg
	DNS	IP	No C2	TOR	Payment
Locky	✓	✓			DNS
SamSam			✓		DNS (TOR)
TeslaCrypt	✓				DNS
CryptoWall	✓				DNS
TorrentLocker	✓				DNS
PadCrypt	✓				DNS (TOR)
CTB-Locker	✓			✓	DNS
FAKEBEN	✓				DNS (TOR)
PayCrypt	✓				DNS
KeyRanger	✓			✓	DNS

\*Top variants as of March 2016

After a system is successfully compromised, the exploit kit analyzes its environment (for example, OS, unpatched applications, and so on) to then retrieve and drop an effective ransomware variant. A callback is then made to the ransomware infrastructure to retrieve the keys needed to encrypt the system. Many of the most prevalent exploit kits and ransomware variants resolve a domain name to an IP address to initiate this callback.

Although some variants of ransomware behave differently—for example, SamSam uses a built-in encryption key that does not require a C2 callback, and other variants use Tor-based Onion Routing or IP-only callbacks that avoid DNS—there are many ways that the Ransomware Defense Solution can help.



## Ransomware Kill Chain

The first two steps of the infection process outlined above are most commonly broken down into seven stages of an attack, as shown in Figure 5. Not all attacks use every stage, but these are the most common.

Figure 5—Seven Stages of an Attack



The term “kill chain” refers to the ability to block an attack at any of these specific stages if the correct capabilities can be employed. Following is a brief description of these stages as they are commonly understood across the security industry by similar names<sup>3</sup>.

- RECON:** The attacker gathers information to help them create seemingly trustworthy places and messages to stage their malvertisements and phishing emails.
- STAGE:** Using information collected during RECON, the cybercriminals try to fool users into opening e-mails or clicking on links.
- LAUNCH:** The staging sites redirect from trustworthy-looking sites to sites that launch the exploit kits and/or other malicious content.
- EXPLOIT:** When a user is at the compromised site, their system is scanned for vulnerabilities that are then exploited to take control of the user's system.
- INSTALL:** Once an exploit has taken control, the final dropped file/tool is installed that will infect and encrypt the victim's system—the ransomware payload. This stage may also include additional executables to deliver other malware in the future.
- CALLBACK:** Once infected, the malware “calls home” to a command-and-control server (C2) where it retrieves keys to perform the encryption or receive additional instructions.
- PERSIST:** The files on the hard disk, mapped network drives, and USB devices are encrypted and a notice or splash screen pops up with instructions to pay the ransom to restore the original files. This notice persists, and at times deletes files, as a timer counts down to the expiration of being able to retrieve the unlock keys, putting extreme pressure on the user. Additionally, the exploit kit can persist and pivot to other more critical systems.

<sup>3</sup> [http://www.cisco.com/c/en/us/products/security/annual\\_security\\_report.html](http://www.cisco.com/c/en/us/products/security/annual_security_report.html)

## Ransomware Defense

The Ransomware Defense Solution creates a defense-in-depth architecture with Cisco Security best practices, products, and services to prevent, detect, and respond to ransomware attacks.







Cisco's Ransomware Defense Solution is not a silver bullet or a guarantee, but it does help to:



- Prevent ransomware from getting into the enterprise wherever possible
- Stop it at the system level before it gains command and control
- Detect when it is present in the network
- Work to contain it from expanding to additional systems and network areas
- Perform incident response to fix the vulnerabilities and areas that were attacked

This solution helps to keep operations running, reducing the fear of being taken hostage and losing control of your critical systems.

To defend against the ransomware kill chain, specific capabilities are necessary to build the appropriate layers of defense. Table 2 identifies the SAFE methodology capabilities (as represented by the blue icons) best suited for this defense.

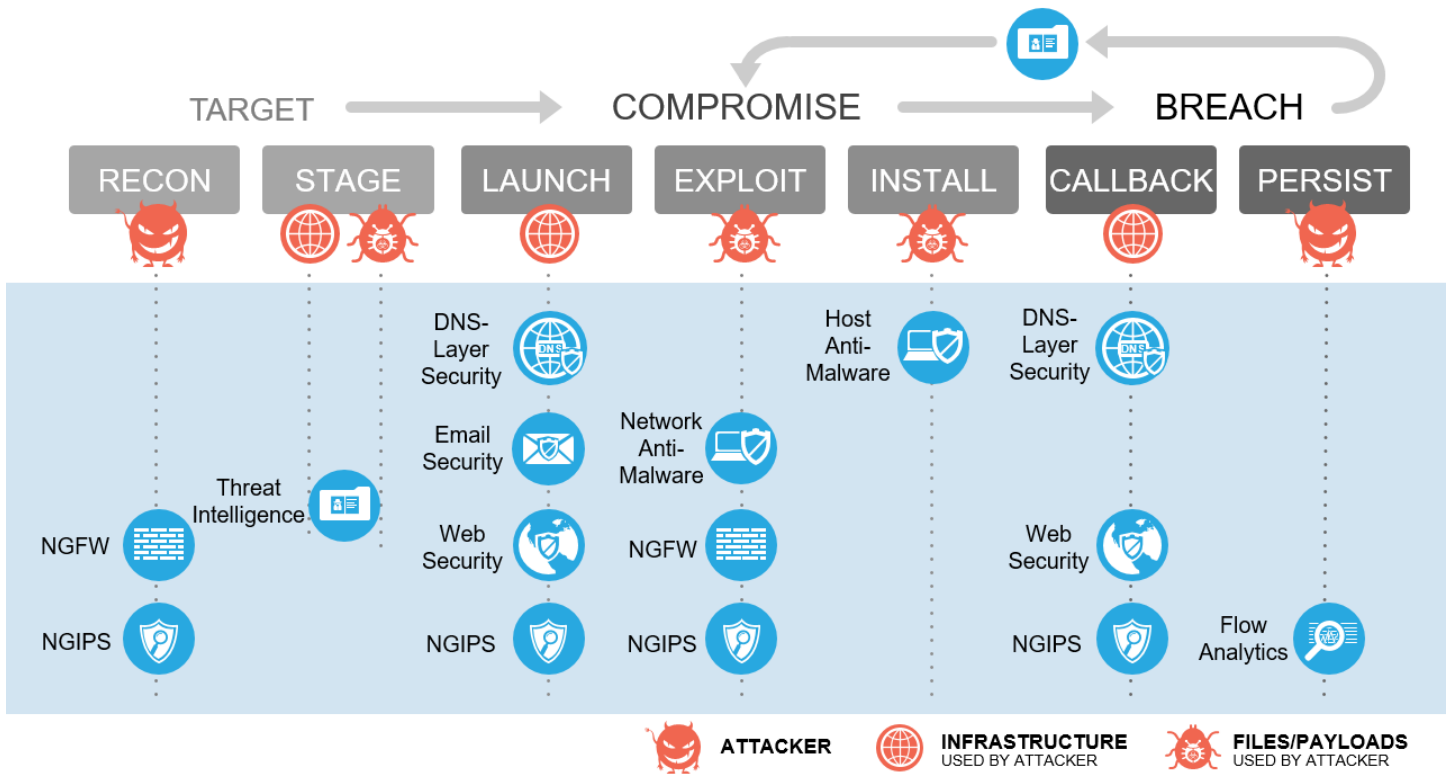
Table 2 - SAFE Capabilities to Defend against Ransomware Attacks

icon	Capability	Function
	Threat intelligence	Knowledge of existing ransomware and communication vectors, and learned knowledge in new threats
	E-mail security	Block ransomware attachments and links
	DNS Security	Block known malicious domains and break the C2 callback
	Client Security	Inspect files for ransomware and viruses, quarantine and remove
	Web Security	Block web communication to infected sites and files
	Identity-based Firewall Segmentation	Authenticate access, and separate traffic based on role and policy

	<p>Intrusion Prevention</p>	<p>Block attacks, exploitation, and intelligence gathering</p>
	<p>Network Monitoring</p>	<p>Monitor infrastructure communications using flow-based analytics; identify and alert on abnormal traffic flows</p>

Each of these capabilities are then deployed to combat and defend against the seven stages of an attack, as shown in Figure 6.

Figure 6—Breaking the Kill Chain with Security Capabilities



These capabilities work together to create several layers of defense, protecting the organization against the threat and spread of ransomware.

## Best Practices

### Things you can do

It is not enough to have a world class defense-in-depth architecture. You need to know what the critical priorities are for running your business, and whether they can be impacted if your systems are locked down.

- The most important action is to ensure you have good backups. If you do weekly backups, you should transition to daily; if you do daily, look to transition to hourly or real-time.
- Develop a good disaster recovery plan, and ensure that it is regularly tested and updated as the business grows and changes.
- Identify all of the people, processes, and tools necessary to handle a critical disruption or event. Perform drills to test these plans on a regular basis.
- Develop a comprehensive baseline of the applications, system images, information, and your normal running network performance. These give you visibility into changes on your network, enabling detection of the unusual.
- Standardized images of operating systems and desktops allow for easy re-imaging to recover infected infrastructure.

### Recovery in the event that the worst has happened

Backup recovery is your last line of defense, and avoids having to pay out a ransom to the attackers. Your ability to recover from this attack with minimal data loss and/or service interruption amounts to whether or not the system backups and/or disaster recovery sites were compromised as a part of the attacker methodology. Whether or not your backups were compromised depends on how well your backup systems and/or network and/or recovery sites were sufficiently segmented from your main network. Even if your organization does not use on-site backups at all, instead opting for cloud backup solutions (such as Amazon Glacier), if those cloud backup credentials are left in easily accessible locations, or if passwords are reused, the attacker could easily delete all backup instances, resulting in 100% data loss if there is no other backup solution in place. A secure, off-site, enterprise backup solution could easily be defeated through password reuse and/or poor password management.

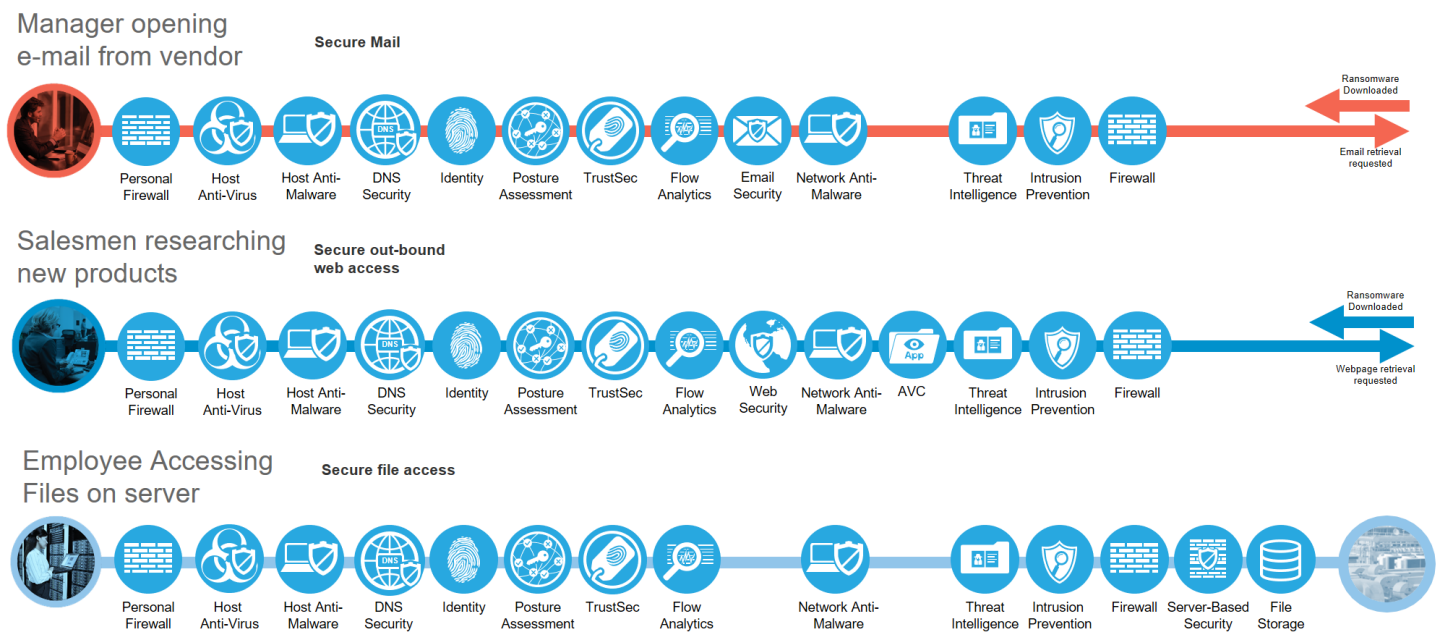
For enterprises using backup solutions, there are a wide variety of backup methodologies; the SANS reading room has a comprehensive document on tape rotation schemes that is very helpful. Typically, as a part of a tape rotation policy, a portion of the tapes are delivered to an off-site storage facility. This is for disaster recovery purposes; if there a catastrophic failure at the site hosting an organization's data, the tapes at the storage facility are still there to recover from at a backup facility. In a scenario in which local backups are deleted, removed, or otherwise made inaccessible by the attackers, off-site backups are often your only hope of restoring service without paying the ransom. Depending on how often your backups are sent off-site determines how much data (if any) would be inaccessible or lost.

# Solution Architecture

The first step in developing a defense-in-depth architecture is to take all of the capabilities that can break the ransomware kill chain and match them with the real-world business functions/flows as identified in the SAFE model. Specific to ransomware, these are web browsing and email usage, because these are the highest risk methods of infection. Also included as a third example are files on internal storage.

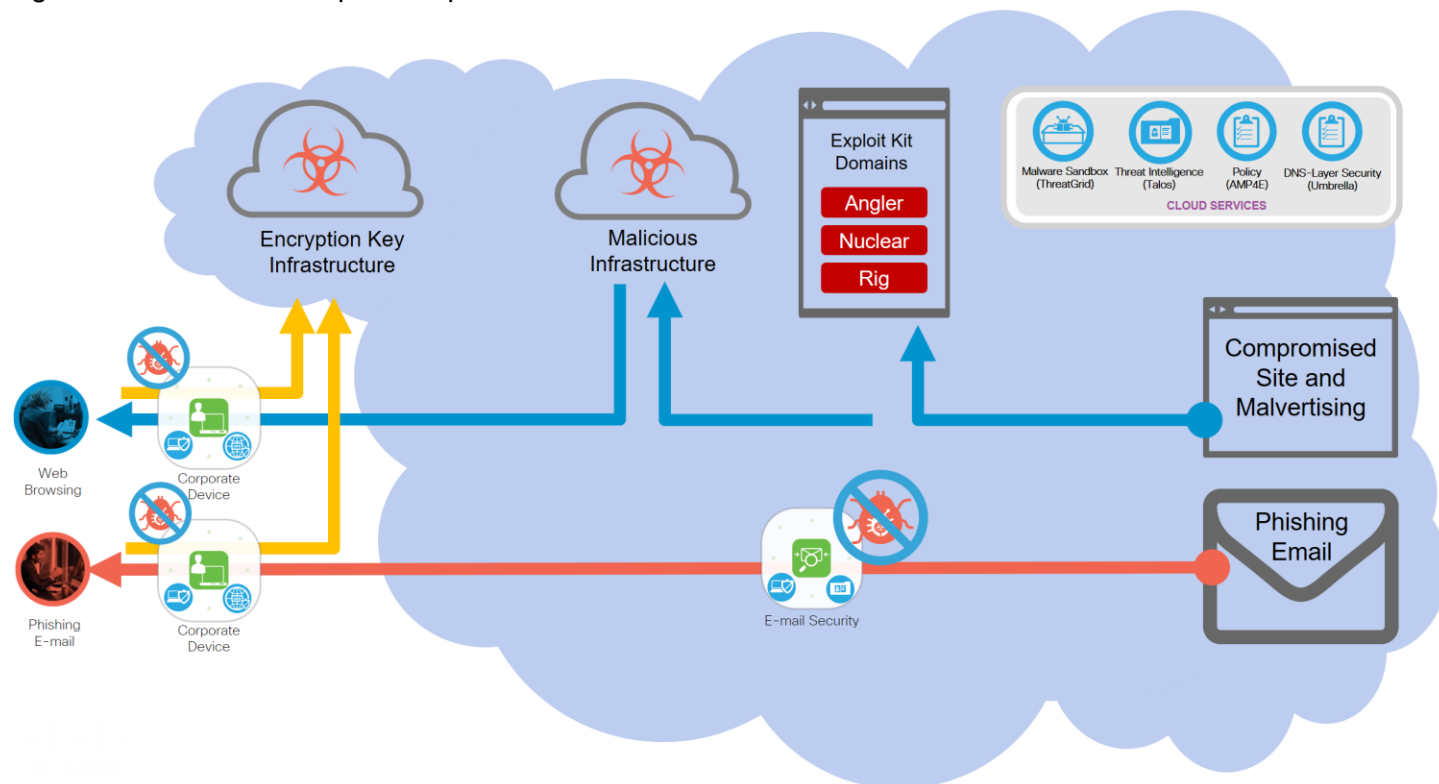
Each of these three business flows are shown in Figure 7, with the selected capabilities described above. Across an organization, these capabilities may be duplicated in several network domains. All duplicates have been removed, and the capabilities are not necessarily in any specific order. They are representations of the best ways to protect the flows from an end-to-end perspective.

Figure 7—SAFE Business Flows and Capabilities for Ransomware Defense



Because a comprehensive deployment of these capabilities can include significant costs and time to deploy, this solution has been divided into two phases. Phase one includes several capabilities that can be rapidly deployed with relatively low effort and achieve a great reduction in risk, as shown in Figure 8. Phase two adds the remaining capabilities, and is shown on a sample Campus network architecture in Figure 15..

Figure 8—Cloud and Endpoint Capabilities



## Phase One—Validated Testing

With the threat of ransomware attacks and infections looming, action must be taken to block it before becoming the next victim. The organization must augment existing security measures by implementing email, DNS, and anti-malware security capabilities. These are quick and easy to deploy cloud-enabled services that provide an immediate reduction in the risk of successful ransomware attacks.

Three steps to a quick and successful defense include;

1. Block the number one vector of infection—Filtering email attachments and URLs before they reach a single user.
2. Stop command and control (C2) communication and redirection to malicious sites—Add a layer of DNS security for on-net and off-net protection.
3. Enable malicious file protection (AMP) capabilities across all supporting infrastructure (hosts, network, email and web).

Deploying these capabilities is crucial, and should be prioritized by group; admins, executives, key servers, and then as broadly as possible.

Each of these offerings share the cloud-based services of Talos Threat intelligence, Threat Grid file analysis and Umbrella Security Graph.

## Email Security

Email security blocks a significant amount of ransomware attacks by pre-filtering all messages coming into (red arrow) an organization before ever reaching a real person that may open or click on it. Messages are evaluated through several policy enforcement inspection steps that must be enabled. These include content, virus checking, malware checking, and spoofing.

Malware checking is performed using the Advanced Malware Protection (AMP) integrated service. Known bad attachments (based on file hashes and other recognition abilities) can be stripped, but the best practice is to drop or quarantine the entire message. For unknown attachments, messages are held in quarantine while the attachments undergo file analysis in the Threat Grid file sandboxing service. Forwarding decisions are then chosen based on the severity of the analysis report returned. Proper CES integration with mail systems can allow retrospection to clean up infected e-mail before it is retrieved by other users. Figure 9 shows messages with attachments stripped.

NOTE: On rare occasions, malicious files can initially be classified as “safe” due to their ability to change behavior after analysis.

Figure 9—Email with Prepended Subject Notifications

All Unread		Search Current Mailbox (Ctrl+E)	Current Mailbox
FROM	SUBJECT	SIZE	
Date: Two Weeks Ago			
Matt Matt	Going to Cisco Live?	12 KB	
Hey Team, I hear that several of you are going to Cisco Live in Las Vegas! That is so awesome, I wish I could go. I have always wanted to go to Vegas and make some killer money at the card tables. I found this cool site that has a bunc...			
Chuck Robber	[SUSPICIOUS MESSAGE - This is a potential Phish] Here are the links to the work you must review	22 KB	
Well team, It seems like the attachment I sent is getting blocked. Here is a link to our dev site to check out the trainers we need to get evaluated ASAP! Dev Site < <a href="http://stage.secure-web.sco.cisco.com/1-ilq0G5TSREGuBDOIZtZQfvJk9QVpBa-RvWkgtCqR_XE...">http://stage.secure-web.sco.cisco.com/1-ilq0G5TSREGuBDOIZtZQfvJk9QVpBa-RvWkgtCqR_XE...</a> >			
Chuck Robber	[WARNING: MALWARE DETECTED - Attachment Dropped]Report Generator	9 KB	
Mail System Admini...	How is our service?	117 KB	
Hi Devnet team, Just wanted to check in and see how your e-mail is working. Please take this quick survey and let us know! Customer email survey < <a href="http://devnet.letmein.ml/email-survey.pdf.exe">http://devnet.letmein.ml/email-survey.pdf.exe</a> > @ Mail Administrator 2016...			

The email system also evaluates URLs to determine whether a message contains spam or phishing links, and take an appropriate action based on the URL’s reputation. For enhanced protection against ransomware, message modification and virus outbreak filters must also be enabled globally and added to the mail policies. Outbreak filters defend against emerging threats and blended attacks. They can issue rules on any combination of six parameters, including file type, file name, file size, and URLs in a message.

As Cisco’s Talos Threat Intelligence learns more about an outbreak, it can modify rules and release messages from quarantine accordingly. Outbreak filters can also rewrite URLs in suspicious messages. This recipient browsing activity can be tracked by enabling Web Interaction Tracking (WIT). When clicked, the new URLs redirect the recipient through the Cisco Web Security proxy. The website content is then actively scanned, and outbreak filters display a block screen to the user if the site contains malware or exploit kits that would drop ransomware. If the content is unknown, a decision option is presented as shown in Figure 10.



Figure 10—Decision Option from Web Interaction Tracking

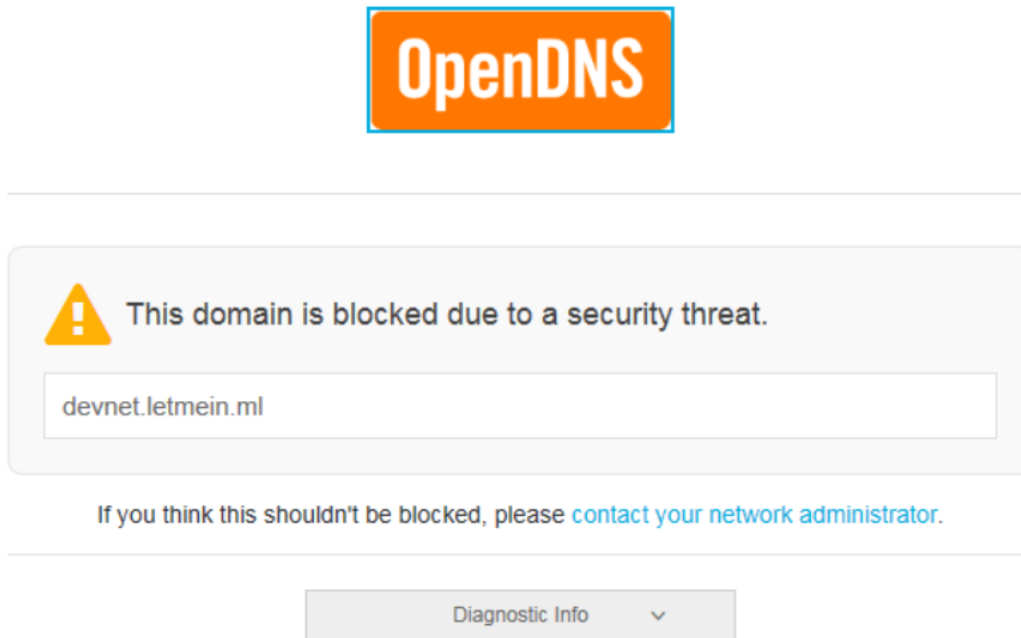


## DNS Security

DNS Security enforces security at the domain name resolution step of converting a name to an IP address to reach a server on the internet. Security at this DNS layer enables the ability to protect devices both on and off of an organization's network for all communication types, not just web sites. In the case of the initial launch where a URL would take a user to a seemingly trustworthy site, Umbrella would block the DNS request and replace it with a safe destination before the user's browser connects to the malicious site—whether the user clicked on a link or if there was a redirect from a compromised site, as shown in Figure 11.



Figure 11—DNS Block Page

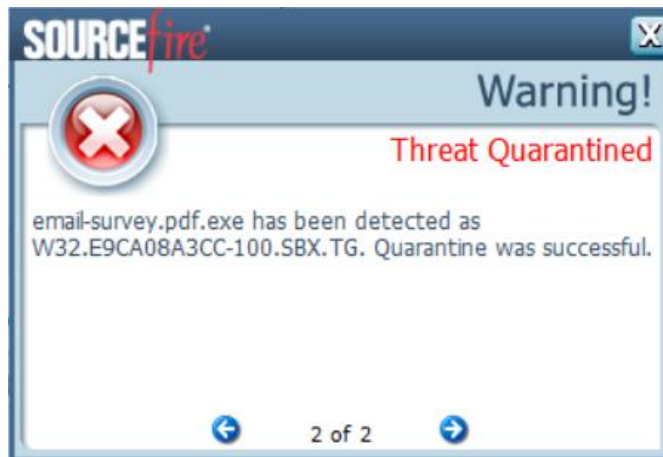


As shown in Figure 11, several different domain networks may exist for each of the kill-chain stages (blue arrows), with differing levels of threat intelligence gathered for each. A new domain that is only hours or minutes old may be used for the initial phishing site, whereas the subsequent malicious infrastructures may have days or weeks of known bad history. Each stage offers an opportunity for DNS Security to block the communication before the compromise occurs to protect the user from the infection. Additionally, Umbrella also stops C2 callbacks if an infection does occur (yellow arrows), no matter what port or protocol is used. This can stop the ransomware file drop or the C2 callback for encryption keys.

## Anti-Malware Security

Host-based anti-malware is the last line of defense, and often the only defense for communications encrypted end-to-end (password protected archives, https/sftp, chat file transfers, and so on). Cisco's Advanced Malware Protection (AMP) analyzes all files that reach the user's system. If the file is known to be malicious, it is quarantined immediately, as shown in Figure 12.

Figure 12—AMP Quarantine Notification

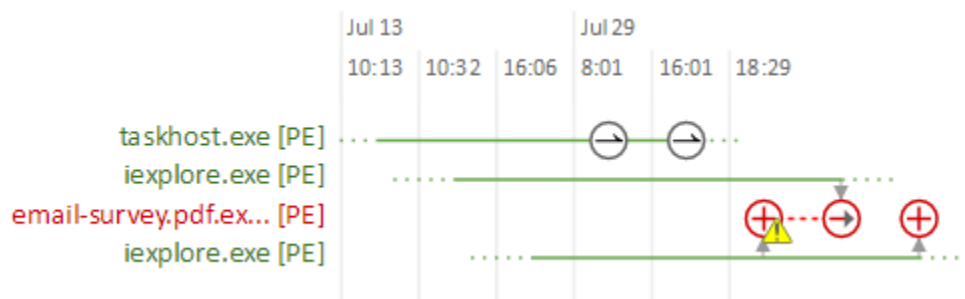


If the file is of low prevalence (files never seen before, and have no history), it is uploaded automatically to Threat Grid for analysis (additional configuration and licensing required), which provides retrospective security to detect malware that evaded initial inspection.

Using a combination of file signatures, file reputation, behavioral indicators, and sandboxing, AMP can stop the initial exploit kit from executing on a user's system and can also stop the execution of the dropped ransomware file and remove it.

Additionally, AMP continuously analyzes and records all file activity on a system, regardless of a file's disposition. If at a later date a file behaves suspiciously, AMP retrospectively detects it and sends an alert. AMP records a detailed history of malware's behavior over time, including where and how it entered the network, where else it traveled, and what it is doing. Based on a set policy, AMP can then automatically or manually contain and remediate the threat. Figure 13 shows how AMP tracks the actions of files on a system.

Figure 13—AMP Device Trajectory



## Threat Intelligence

Our Cisco Talos Group (Cisco Threat Intelligence Group) analyzes millions of malware samples and terabytes of data per day, and pushes that intelligence to AMP to provide 24/7 protection. Also, advanced sandboxing capabilities perform automated static and dynamic analysis of the unknown files against 500+ behavioral indicators to uncover stealthy threats.

Through the combination of both Talos and Threat Grid threat analysis engines, suspicious email attachments and files can be sandboxed, analyzed, and categorized as malware or ransomwares in as quickly as 20-30 minutes. However, low prevalence files may take a slightly longer time to analyze and identify, to minimize the chance of false positives on the analysis. Figure 14 shows an analysis report of a ransomware sample used in the solution validation testing.

Figure 14—File Analysis Report

**ThreatGRID**  
Malware Threat Intelligence Platform

Metadata Behavioral Indicators Network Activity Processes Artifacts Registry Activity File Activity

## Analysis Report

<b>ID</b>	28cbbee15b1ea4c884edd8470d8205f4	<b>Filename</b>	fpzryrf.exe
<b>OS</b>	7601.18798.amd64fre.win7sp1_gdr.150316-1654	<b>Magic Type</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>Started</b>	7/29/16 18:44:43	<b>Analyzed As</b>	exe
<b>Ended</b>	7/29/16 18:50:39	<b>SHA256</b>	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
<b>Duration</b>	0:05:56	<b>SHA1</b>	a2de85810fd5ebcf29dc5da5dd29ce03470772ad
<b>Sandbox</b>	phl-work-02 (pilot-d)	<b>MD5</b>	dd07d778edf8d581ffaadb1610aaa008

**Warnings**

- Executable Failed Integrity Check

## Behavioral Indicators

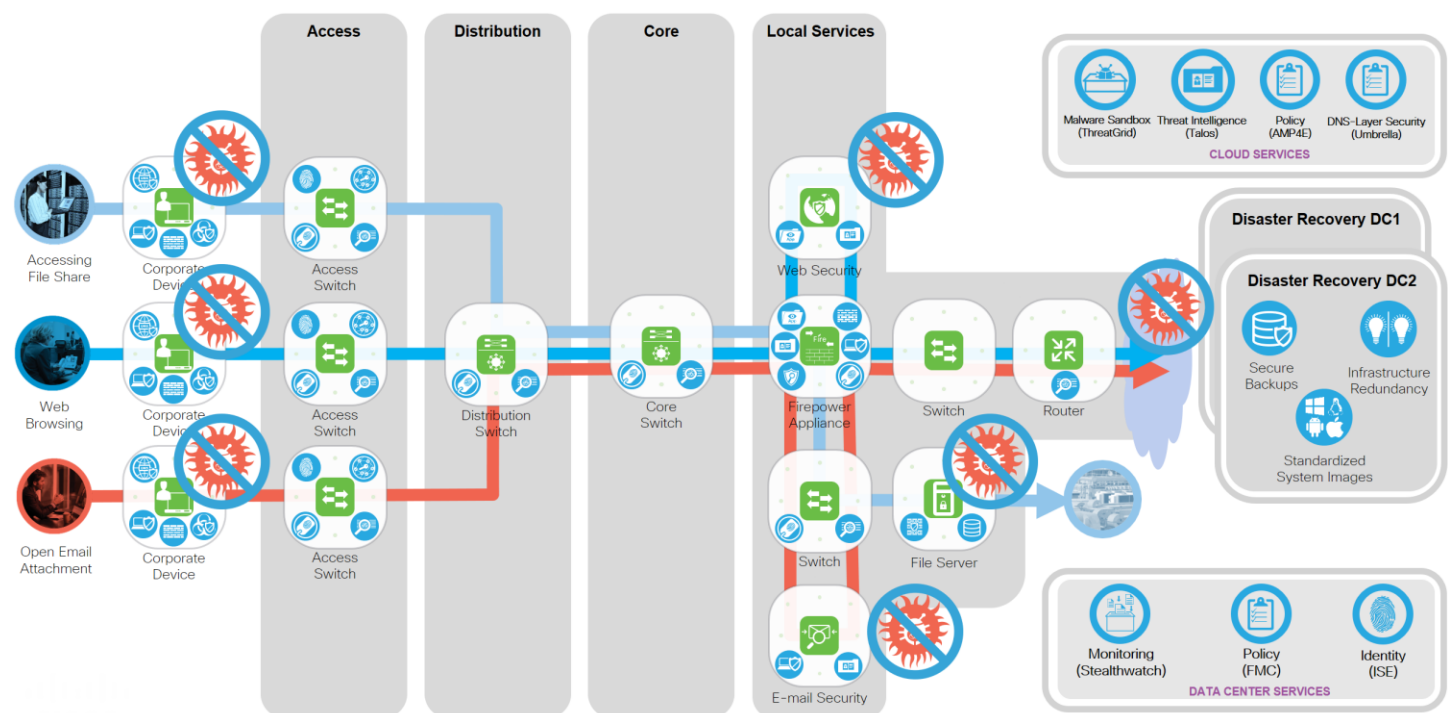
CTB Locker Detected	Severity: 100	Confidence: 100
Generic Ransomware Detected	Severity: 100	Confidence: 95
Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100
Process Modified a File in a System Directory	Severity: 90	Confidence: 100
Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80
Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
Decoy Document Detected	Severity: 70	Confidence: 100
Process Modified an Executable File	Severity: 60	Confidence: 100
Process Modified File in a User Directory	Severity: 70	Confidence: 80
Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80
Hook Procedure Detected in Executable	Severity: 35	Confidence: 40
Ransomware Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

Retrospective security intelligence for malware that evaded initial inspection, is shared via Talos Threat Intelligence to both email and host anti-malware services. All current and future instances of these malicious files are blocked or removed.

## Phase Two—Campus Reference Architecture

The Phase Two architecture builds upon the capabilities deployed in Phase One by implementing a fully segmented role-based infrastructure with network monitoring and enforcement capabilities throughout. Figure 15 shows a sample campus architecture using the SAFE Secure Campus PIN. Layers on the business use case flows of email, web, and file sharing that were used above. Each of the capabilities needed to protect these flows is applied to the appropriate system platforms (green squares) or shown as cloud services.

Figure 15—Phase Two Sample Campus Architecture



### Advanced Web Security

Through web filtering and web reputation scoring, Cisco's Web Security controls access to more than 50 million known websites by applying filters from a list of more than 75 content categories. These controls cover access to web pages, individual web parts, and micro-applications so employees can access sites needed for work; and apply a finer level of control and inspection for ransomware hosted within known and trusted domains such as social networking sites and other services. Features include:

- Cloud- and/or premises-based web security gateway to protect all users, regardless of location
- Scalable to accommodate from 100 to more than 10,000 users
- Web security, application control, management, and reporting fully integrated
- Powered by Talos Threat Intelligence for comprehensive zero-day threat protection

Outbreak intelligence runs webpage components in a highly secure virtual emulation to determine how each component behaves, and blocks any malware or ransomware.

The file reputation feature captures a fingerprint of each file as it traverses an organization's network. These fingerprints are sent to AMP's cloud-based intelligence network for a reputation verdict. After an attack, using file retrospection, you can track a file's disposition over time after it enters your environment. If it is found to be malware, you can discover where the file entered and where it is currently located to mitigate future intrusions. Additionally, Cisco's Cognitive Threat Analytics (CTA) integrated feature helps reduce threat identification time by actively identifying the symptoms of a malware infection through behavioral analysis, anomaly detection, and machine learning.

## Network Monitoring

Cisco Stealthwatch provides visibility and security intelligence across an entire organization before, during, and after an attack. It continuously monitors the network and provides real-time threat detection and Incident response forensics if a ransomware outbreak occurs.

Stealthwatch turns the network into a sensor, ingesting and analyzing NetFlow data from infrastructure and workstations, creating a baseline of the normal communication of an organization and its users. From this baseline, it is then much easier to identify when sophisticated attackers infiltrate the network trying to analyze and deploy ransomware. It can identify malware, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), and insider threats. It monitors both north-south and east-west (lateral) movements to detect the widest range of attacks.

Stealthwatch works in tandem with the Cisco Identity Services Engine and Cisco TrustSec technology. Through this integration you can identify users and systems, and appropriately segment critical network assets based on system behavior automatically.

## Identity-based Segmentation

To best defend against the spread of ransomware, users should be allowed access only to the resources and system file shares they need to perform their duties. A system infected with ransomware tries to search the network for other file share drives and vulnerable systems to encrypt or infect them using the credentials of the current system user.

Cisco TrustSec with Cisco Identity Services Engine (ISE) is used to segment your network and enforce role-based access control. With Cisco TrustSec technology, you can control access to network segments and resources based on context, user, device, and location according to a specific security policy.

With Security Group Tags (SGT) enforcement, an infected user system with maintenance contractor credentials is blocked from accessing finance data, regardless of network topology or whether this contractor was using wired or wireless access to the network.

Through integration with Stealthwatch, if an infected system is identified based on abnormal behavior on the network, the Identity Services Engine can institute a change of authorization based on this learned behavior and apply a different SGT policy to quarantine them and immediately protect the rest of the network.

## Infrastructure Segmentation and Intrusion Prevention

### Segmentation with NGFW

The Cisco Firepower Next-Generation Firewall (NGFW) is a fully integrated, threat-focused next-gen firewall with unified management. It delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint, each providing additional or alternate layers of defense against the threat of ransomware.

Each of these capabilities working in concert serves to thwart network reconnaissance when your organization is targeted for a ransomware attack. Blocking communication between various network resources serves to segment your infrastructure to the permitted users, systems, and protocols needed for business communications, and block those used to infiltrate, exploit, exfiltrate data or retrieve encryption keys as well as persist in your network.

Firepower NGFW enables comprehensive policy management that controls access, stops attacks, defends against malware, and provides integrated tools to track, contain, and recover from attacks that do get through.

### Management with Firepower Management Center

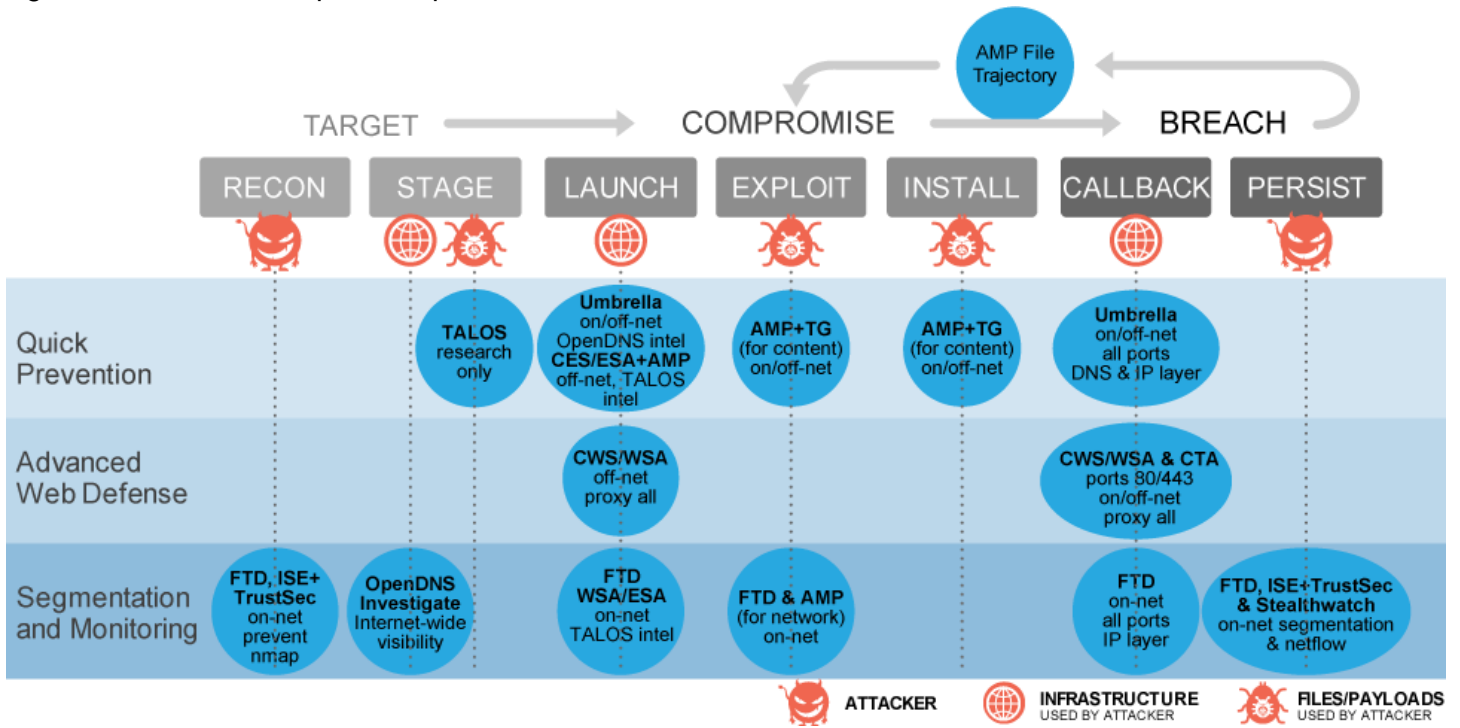
This is your administrative nerve center for network security management. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection on the Firepower platforms. It enables easy transitions from managing a firewall to controlling applications to investigating and remediating ransomware outbreaks.

With the Cisco Firepower Management Center and Stealthwatch behavior analysis, you can share security intelligence and automate threat containment through ISE.

# Architecture Summary

Each of the products identified in the phases above fulfill the capability requirements necessary to defend against an attack across the kill chain, as shown in Figure 16.

Figure 16—Products Replace Capabilities in the Kill Chain



## Implementation and Validation

The products listed in Table 3 were implemented for the validation testing of the Ransomware Defense Solution. Each of the product sections describes how they were customized after a typical installation to best defend against ransomware.

Table 3—Solution Products validated

Product	Description	Platform	Version
Cloud Email Security	E-mail security with AMP	Cloud	v10.0.0-071
Umbrella Roaming and Network-based DNS Protection	DNS Security for roaming users outside the organization. Network DNS for all internal devices and systems	Cloud / Roaming client	v2.0.189
Advanced Malware Protection (AMP)	Host anti-malware protection for endpoints	Cloud / Client endpoint	v4.4.2.10200

### Cisco Cloud Email Security

The following steps outline how to configure email security to best defend against ransomware and other advanced persistent threats (APT) after the Cloud Email Security service is up and functioning normally and fully integrated into your mail process flows. For a new CES installation, the Default Policy should be similar to Figure 17 below.

Step 1 Select Mail Policies > Incoming Mail Policies.

Figure 17—Default Policy for New Deployment

Policies								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver Mailbox Auto Remediation: Disabled ...	Not Available	Disabled	Retention Time: Virus: 1 day	

Within the incoming Mail Policies, we edit the Default Policy elements of Advanced Malware Protection, Content Filters and Outbreak Filters.

Advanced Malware Protection.

Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:

- Obtaining the reputation of known files
- Analyzing behavior of certain files that are not yet known to the reputation service



- Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network

These features are available only for incoming messages. Files attached to outgoing messages are not evaluated.

Step 1 Click the link in the Advanced Malware Protection column of the Default Policy to modify it.

Figure 18—Advanced Malware Protection in Default Policy

### Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	<input type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> No
<b>Message Scanning</b>	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
<b>Unscannable Attachments:</b>	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[WARNING: ATTACHMENT UNSCANNED]"/>
	▸ Advanced <i>Optional settings for custom header.</i>
<b>Messages with Malware Attachments:</b>	
Action Applied to Message:	Drop Message ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[WARNING: MALWARE DETECTED - Attachm"/>
	▸ Advanced <i>Optional settings for custom header.</i>
<b>Messages with File Analysis Pending:</b>	
Action Applied to Message:	Quarantine ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[WARNING: ATTACHMENT(S) MAY CONTAIN"/>
	▸ Advanced <i>Optional settings for custom header.</i>
<input checked="" type="checkbox"/> <b>Enable Mailbox Auto Remediation (MAR)</b>	
<i>Mailbox Auto Remediation Actions apply only if Mailbox Settings are configured. See System Administration &gt; Mailbox Settings .</i>	
Action to be taken on message(s) in user's mailbox:	<input type="radio"/> Forward to: <input type="text"/> <input checked="" type="radio"/> Delete <input type="radio"/> Forward to: <input type="text"/> and Delete

Cancel

Submit

It is a best practice to prepend the email message subject with an informative warning based on the status of the messages attachments.

**Step 2** Configure the Modified Message Subject for both Unscannable Attachments and File Analysis Pending results.

Messages with malware attachments may have the attachments stripped, delivered with a warning, or dropped altogether. The most common practice is to drop the entire message.

**Step 3** Configure the Action Applied to Message > Drop Message.

Messages with File Analysis Pending can be either delivered or quarantined. The best practice is to quarantine these email messages until a result is received by the analysis engine. If the attachment is malicious, it will follow the Attachments setting. If the result returned is unknown, the message will be delivered and the Message Subject prepended with a warning.

**Step 4** Configure the Action Applied to Message > Quarantine.

By enabling Mailbox Auto Remediation (MAR), messages already delivered to a user's mailbox can be deleted if the threat verdict later changes to malicious.

**Step 5** Configure MAR by ticking Enable, and set the action to Delete.

**Step 6** When finished with these changes, click Submit.

File Reputation and Analysis Service implements the AMP engine for inspecting messages as enabled by the policy above. File Analysis is enabled by default for new implementations and inspects Windows and DOS executables, but you should also select additional file types for analysis.

**Step 7** Select Security Services > File Reputation and Analysis.

**Step 8** Select Edit Global Settings

Figure 19—File Analysis Settings

### Edit File Reputation and Analysis Settings

Advanced Malware Protection	
<i>Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.</i>	
File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: (?)	<input checked="" type="checkbox"/> Enable File Analysis
File Types:	<input checked="" type="checkbox"/> Adobe Portable Document Format (PDF) <input checked="" type="checkbox"/> Microsoft Office 2007+ (Open XML) <input checked="" type="checkbox"/> Microsoft Office 97-2004 (OLE) <input checked="" type="checkbox"/> Microsoft Windows / DOS Executable <input checked="" type="checkbox"/> Other potentially malicious file types
▶ Advanced Settings for File Reputation	<i>Advanced settings for File Reputation</i>
▶ Advanced Settings for File Analysis	<i>Advanced settings for File Analysis</i>

Cancel

Submit

**Step 9** Enable additional file types as shown in Figure 19 above. Click Submit.

## Content Filtering

Some ransomware and exploit kits are attached to messages as scripts and are not inspected by file analysis. These scripts can run locally on the system if opened and bypass security in web browsers.

As a best practice, Cisco recommends using content filtering to remove the following types of script attachments:

- .js
- .wsf
- .vbs

Create a new incoming content filter to drop messages with these attachments.

Step 10      Select Mail Policies >Incoming Content Filters >Add Filter.

Step 11      Enter a descriptive name and description.  
Name: BlockScriptAttachments  
Description: Save people from Ransomware by blocking script attachments: .js or .wsf or .vbs

Step 12      Click Add Condition > Attachment File Info > Filename contains .js.

Figure 20—New Content Filter Condition

The screenshot shows a window titled "Edit Condition" with a close button in the top right corner. On the left is a vertical list of filter categories, with "Attachment File Info" selected and highlighted. The main area of the window is titled "Attachment File Info" and contains a "Help" link in the top right. Below the title is a descriptive paragraph: "Does the message contain an attachment of a filetype matching a specific filename or pattern based on its fingerprint (similar to a UNIX file command)? Does the declared MIME type of an attachment match, or does the IronPort Image Analysis engine find a suspect or inappropriate image? Is the attachment corrupt?". There are five radio button options: "Filename:" (selected), "Filename contains term in content dictionary:", "File type is:", "MIME type is:", and "Image Analysis Verdict:". The "Filename:" option has a dropdown menu set to "Ends With" and a text input field containing ".js\$". The "Image Analysis Verdict:" option has a descriptive note: "This condition is currently unavailable because the service is not enabled. See Security Services > IronPort Image Analysis." At the bottom of the main area is a note: "(\*) accepts regular expression". At the bottom of the dialog box are "Cancel" and "OK" buttons.

**Edit Condition**

Message Body or Attachment  
Message Body  
URL Category  
URL Reputation  
Message Size  
Message Language  
Attachment Content  
**Attachment File Info**  
Attachment Protection  
Subject Header  
Other Header  
Envelope Sender  
Envelope Recipient  
Receiving Listener  
Remote IP/Hostname  
Reputation Score  
DKIM Authentication  
Forged Email Detection  
SPF Verification  
S/MIME Gateway Message  
S/MIME Gateway Verified  
Duplicate Boundaries Verification

### Attachment File Info [Help](#)

Does the message contain an attachment of a filetype matching a specific filename or pattern based on its fingerprint (similar to a UNIX file command)? Does the declared MIME type of an attachment match, or does the IronPort Image Analysis engine find a suspect or inappropriate image? Is the attachment corrupt?

**Filename:**  
Ends With | .js\$ \*

**Filename contains term in content dictionary:**  
*No content dictionaries are defined. See Mail Policies > Dictionaries.*

**File type is:**  
Is | Compressed

**MIME type is:**  
Is |

**Image Analysis Verdict:**  
*This condition is currently unavailable because the service is not enabled. See Security Services > IronPort Image Analysis.*

**Attachment is Corrupt**

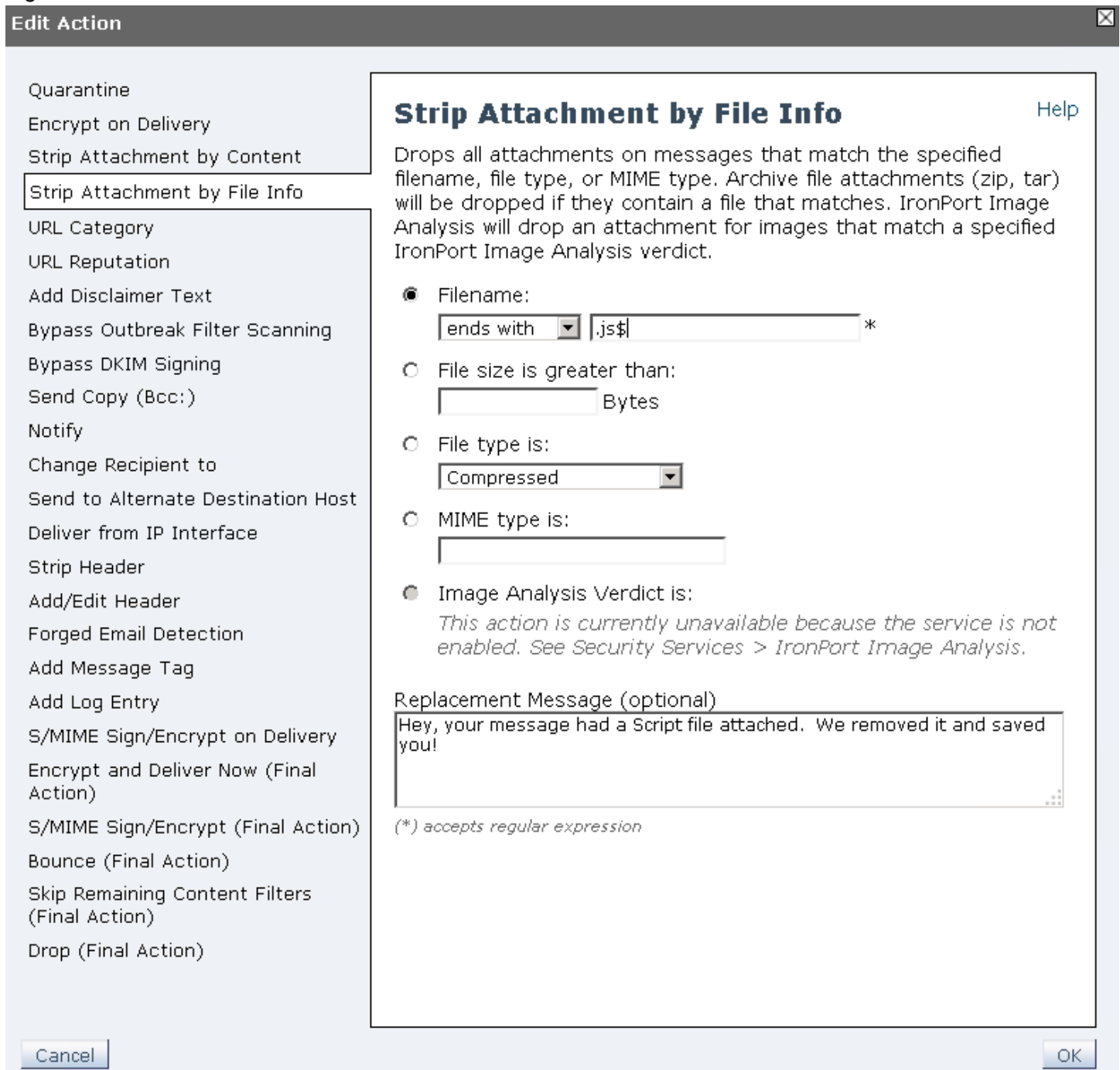
(\*) accepts regular expression

Cancel OK

Step 13 Click OK.

Step 14 Click Add Action > Strip Attachment by File Info > Filename contains .js.

Figure 21—New Content Filter Action



Step 15 Click OK.

Repeat Steps 12-15 for .wsf and .vbs file types as well. Your final filter should include all six, as shown in Figure 22.

Figure 22—Content Filter that Removes Script Files  
**Edit Incoming Content Filter**

Content Filter Settings			
Name:	BlockScriptAttachments		
Currently Used by Policies:	Default Policy		
Description:	Save people from Ransomware by blocking script attachments: .js or .wsf or .vbs		

Conditions			
Add Condition...		Apply rule: If one or more conditions match	
Order	Condition	Rule	Delete
1	Attachment File Info	attachment-filename == ".js\$"	
2	▲ Attachment File Info	attachment-filename == ".wsf\$"	
3	▲ Attachment File Info	attachment-filename == ".vbs\$"	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Strip Attachment by File Info	drop-attachments-by-name(".js\$", "Hey, your message had a Script file attached. We removed it and saved you!")	
2	▲ Strip Attachment by File Info	drop-attachments-by-name(".wsf\$", "Hey, your message had a Script file attached. We removed it and saved you!")	
3	▲ Strip Attachment by File Info	drop-attachments-by-name(".vbs\$", "Hey, your message had a Script file attached. We removed it and saved you!")	

Cancel Submit

Step 16 Click Submit when finished.

Enable the new Content Filter in the Default Policy

Step 17 Select Mail Policies > Incoming Mail Policies > Disabled in the Content Filter column of the Default Policy to modify it.

Step 18 Select Enable Content Filters in the dropdown, check the enable column for the newly created filter.

Figure 23—Enable Content Filtering and Filter  
**Mail Policies: Content Filters**

Content Filtering for: Default Policy			
Enable Content Filters (Customize settings)			

Content Filters			
Order	Filter Name	Description	Enable
1	BlockScriptAttachments	Save people from Ransomware by blocking script attachments: .js or .wsf or .vbs	<input checked="" type="checkbox"/>

Cancel Submit

Step 19 Click Submit when finished.

## Outbreak Filters

Outbreak Filters protects your network from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur. Cisco gathers data on outbreaks as they spread and updates the threat intelligence services in real-time to prevent these messages from reaching your users.

For new installations, the Outbreak Filter is enabled by default, but it is a best practice to also enable Message Modification, which enables URL rewriting on messages. This feature informs users to use caution when opening specific messages.

Step 20 Select Mail Policies > Incoming Mail Policies > Retention Time in the Outbreak Filter column of the Default Policy to modify it.

Figure 24—Outbreak Filter Message Notification

### Mail Policies: Outbreak Filters

Outbreak Filtering for: Default Policy	
Enable Outbreak Filtering (Customize settings) ▼	
Outbreak Filter Settings	
Quarantine Threat Level: ?	3 ▼
Maximum Quarantine Retention:	Viral Attachments: 1 Days ▼ Other Threats: 4 Hours ▼ <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured
Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3 ▼
Message Subject:	Prepend ▼ [SUSPICIOUS MESSAGE - This is a potential \$threat_category] <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>
Include the X-IronPort-Outbreak-Status headers:	<input checked="" type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
Bypass Domain Scanning ?	<input type="text"/> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>
Threat Disclaimer:	None ▼ <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies &gt; Text Resources &gt; Disclaimers</small>

Cancel

Submit

Step 21 When finished enabling message modification, click Submit.

## Web Interaction Tracking

Web Interaction Tracking allows administrators to track the end users who click on URLs rewritten by Cisco Email Security. Allowing tracking of messages with malicious links, including who clicked on the link and the results of their actions.

By default, Web Interaction Tracking is disabled. To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking.

Step 22 Select Security Services > Outbreak Filters > Edit Global Settings

Figure 25—Web Interaction Tracking for Outbreaks

### Edit Outbreak Filters Settings

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> <b>Enable Outbreak Filters</b>	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	<input type="text" value="512K"/> Maximum <i>Add a trailing K or M to indicate units.</i>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> Receive Emailed Alerts
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> Enable Web Interaction Tracking

Cancel Submit

Step 23 Check the Email Alerts and Web Interaction Tracking check boxes. Then click Submit.

To also track URLs due to policy rewrites, you must also enable Web Interaction Tracking in the URL filtering settings.

Step 24 Select Security Services > URL Filtering > Enable.

Figure 26—Web Interaction Tracking for URL Filter

### URL Filtering

URL Filtering Overview	
<input checked="" type="checkbox"/> <b>Enable URL Category and Reputation Filters</b>	
Use a URL whitelist: (?)	<input type="text" value="None"/>
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> Enable Web Interaction Tracking

Cancel Submit

Step 25 Check the Enable URL Category and Reputation Filters and Enable Web Interaction Tracking checkboxes, and then click Submit.

When finished with all changes, you need to commit the changes for these new settings to take effect.

Step 26 Click the yellow Commit Changes button in the upper right corner, leave an appropriate comment, then click Commit Changes to submit them.



## Cisco Umbrella DNS Security

The Umbrella Roaming Client protects laptops regardless of where they are in the world or how they connect to the Internet. The client works by securely redirecting DNS queries bound for the Internet to the Umbrella Secure Cloud Gateway via one of the OpenDNS Global Network data centers distributed worldwide so that your policies are enforced as you choose and security is applied, preventing your computers from becoming compromised.

Several scenarios include computers accessing the Internet through 3g/4g wireless carrier networks, untrusted networks via Wi-Fi hotspots (for example, airport, café, hotel, home), and within office environments behind trusted network gateways or Umbrella-protected networks.

There are no additional configuration steps needed to defend against ransomware. The procedure for downloading and installing the roaming clients can be found here:

<http://info.umbrella.com/rs/opensns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf>

### Cisco Umbrella Roaming

The Cisco Umbrella Roaming Only offering uses a simplified policy that blocks critical security threats, as shown in Figure 27.

Figure 27—Cisco Umbrella Roaming Computers Policy

The screenshot shows the configuration interface for a Cisco Umbrella policy. It is divided into two main panels: 'Policy' on the left and 'Security Settings' on the right.

**Policy Panel:**

- Security Settings:** Malware, Phishing Attacks, Suspicious Response, Botnet, Drive-by Downloads/Exploits, Dynamic DNS, Mobile Threats, and High-Risk Sites and Locations will be blocked. (EDIT)
- Allow Domains:** No domains whitelisted. (EDIT)
- Block Page Appearance:** (Preview block page) (EDIT)
- ADVANCED SETTINGS:**
  - Log All Requests
  - Log Only Security Events (Log and report on only those requests that match a security filter, with no reporting on other requests.)
  - Don't Log Any Requests (Note: No reporting will be available in this mode.)

**Security Settings Panel:**

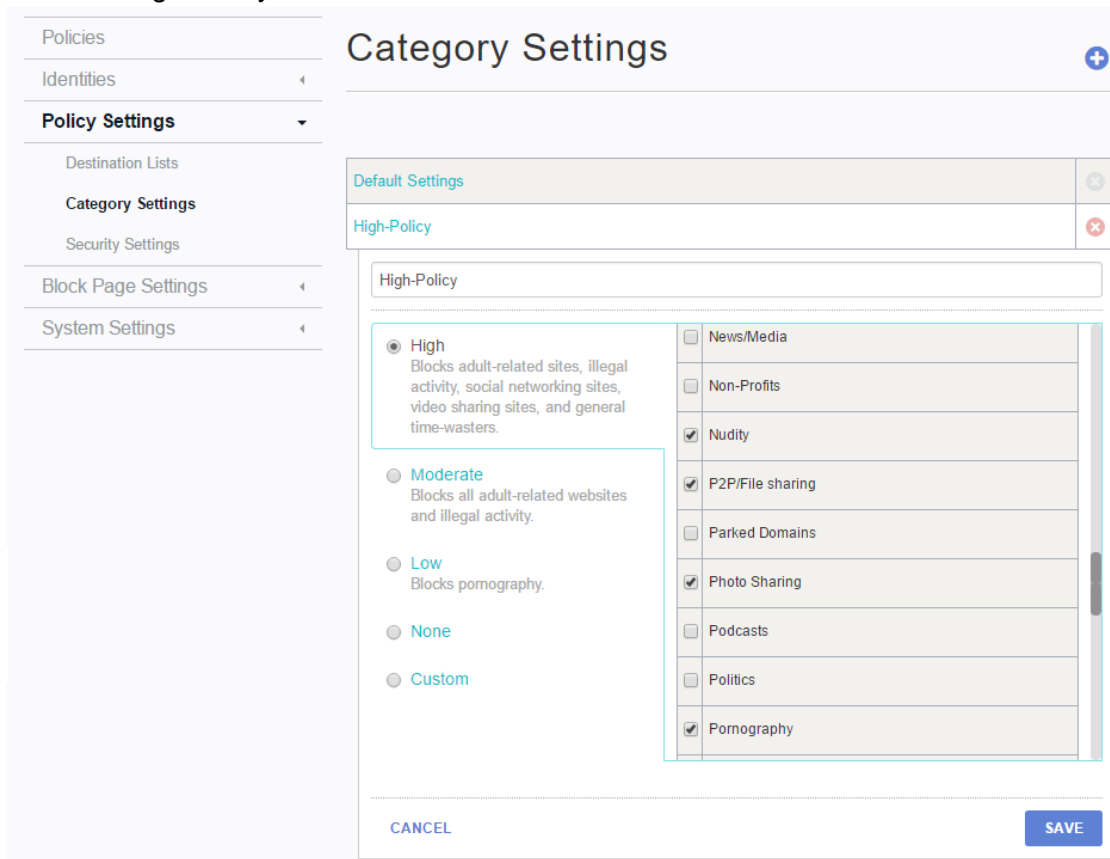
The default security settings are chosen to maximize protection while minimizing false positives. Selecting additional categories may increase false positives, while deselecting default categories will increase your threat exposure.

- PREVENT**
  - Malware (Malicious software including drop servers and compromised websites.)
  - Drive-by Downloads/Exploits (Websites and files that are designed to run code without user intervention.)
  - Dynamic DNS (Block sites that are hosting dynamic DNS content.)
  - Mobile Threats (Threats specific to phones, tablets, or other roaming devices.)
  - Suspicious Response (Public DNS entries that resolve to your internal network space, a tactic of DNS rebinding attacks.)
- CONTAIN**
  - Botnet (Prevent compromised devices from communicating with hackers' command and control servers.)
  - Phishing Attacks (Fraudulent websites that aim to trick users into handing over personal or financial information.)
- ADVANCED THREATS**
  - High-Risk Sites and Locations (Domains identified by some of our statistical models.)

### Cisco Umbrella

The complete Cisco Umbrella offering can protect network, roaming and mobile devices. It includes a more comprehensive set of policies options, including restricting access to other categories of content, which may also reduce the risk of being directed to domains where ransomware may be hosted (such as Gambling, P2P/File sharing, Hate/Discrimination). Several pre-configured policies are available in addition to creating a custom policy. Figure 28 shows the High-Policy that was used in our validation testing.

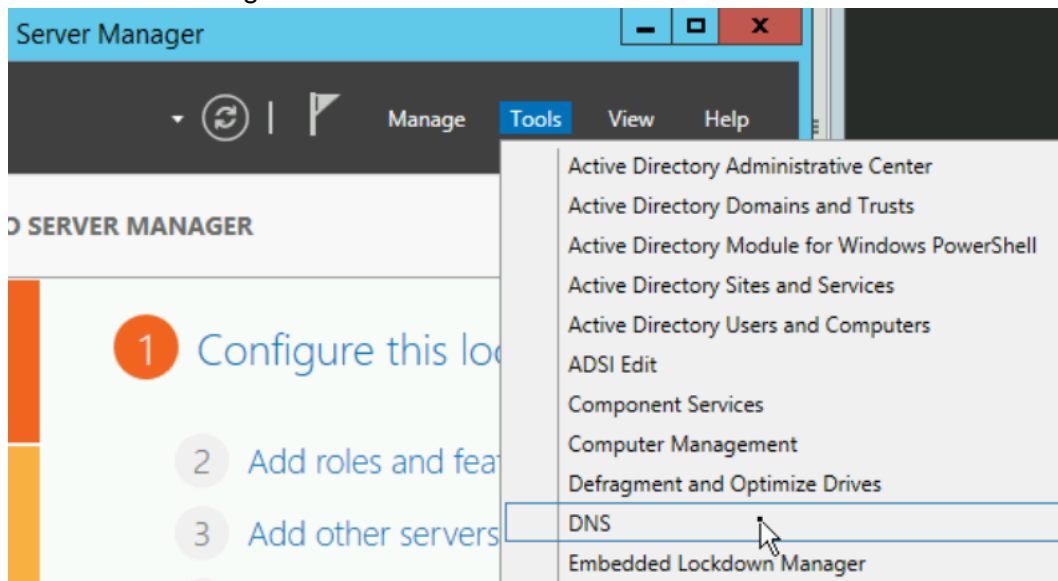
Figure 28—Umbrella High-Policy



For organizations that implement their own internal network DNS servers, Umbrella can be easily enabled for the entire network. Configure your DNS server to use the Umbrella servers as forwarders instead of performing their own Root lookups for external domains. This eliminates the need to deploy the Umbrella client on any internal network system, making for a simple clientless implementation that protects everything on the network. The following steps outline how to configure Windows DNS forwarding to use Umbrella as we did for part of our validation testing.

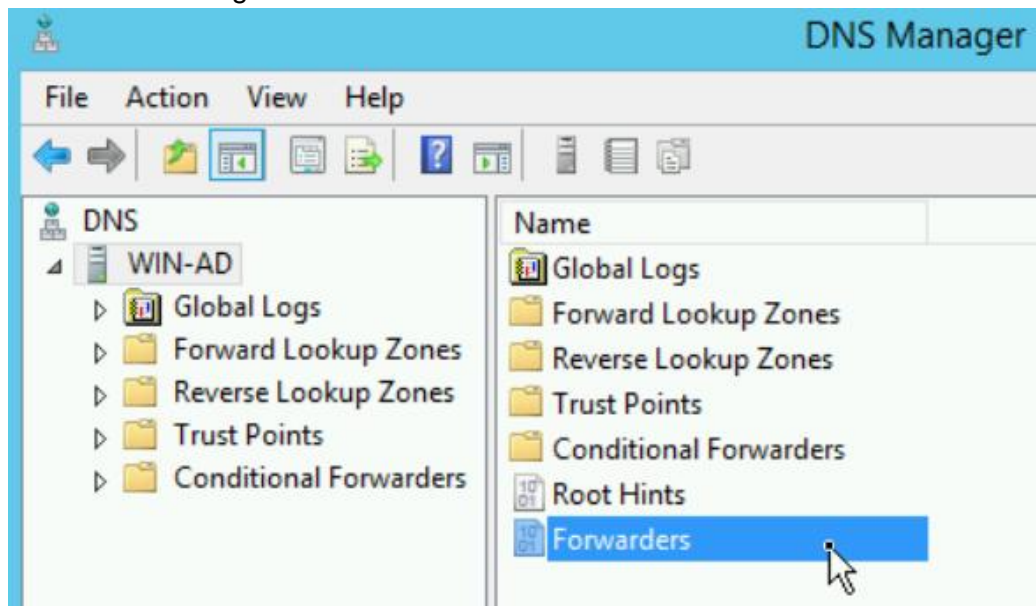
Step 1 Open Windows DNS manager under Server Tools.

Figure 29—Windows DNS Manager



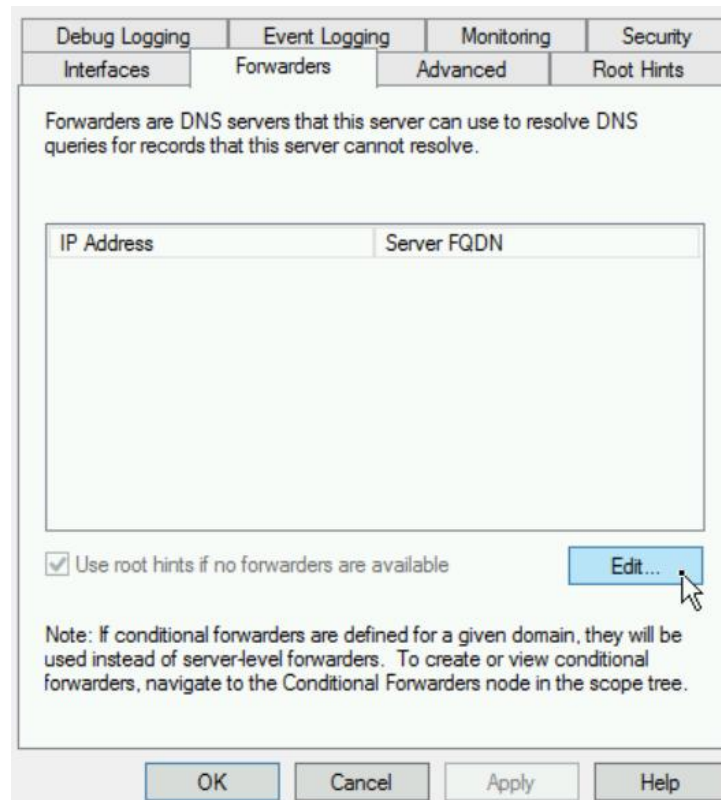
Step 2 Choose the server to edit, then select Forwarders.

Figure 30—Windows DNS Manager Forwarders



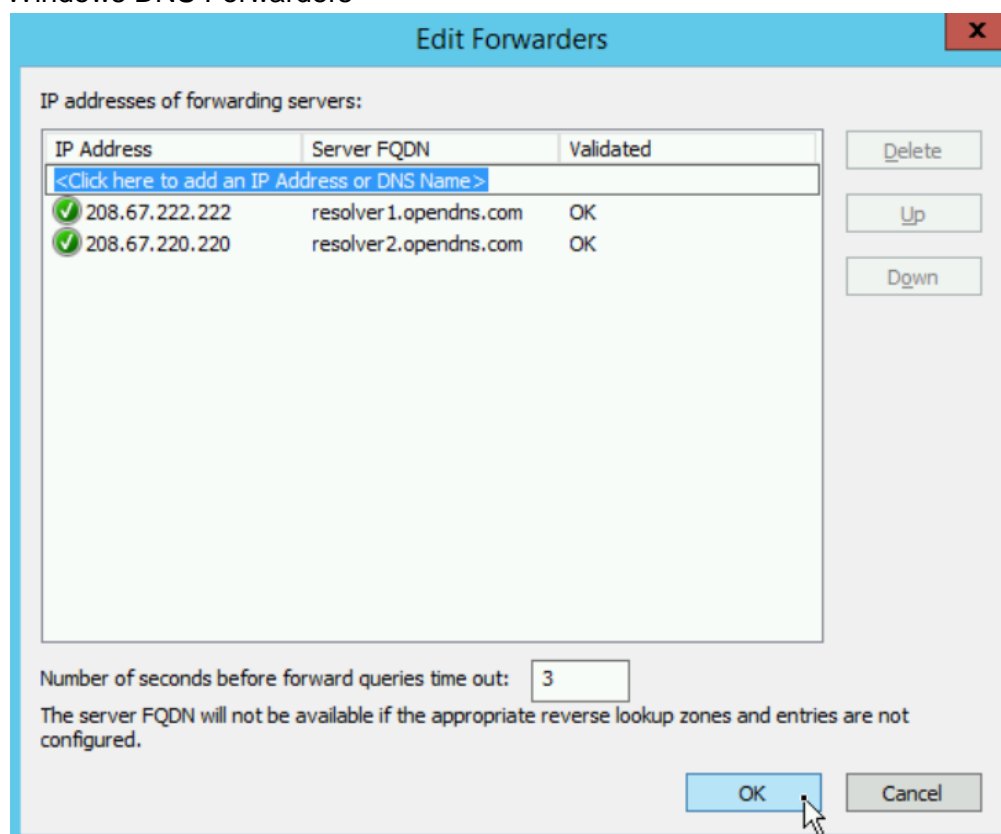
Step 3 Click Edit.

Figure 31—Edit Windows DNS Forwarders



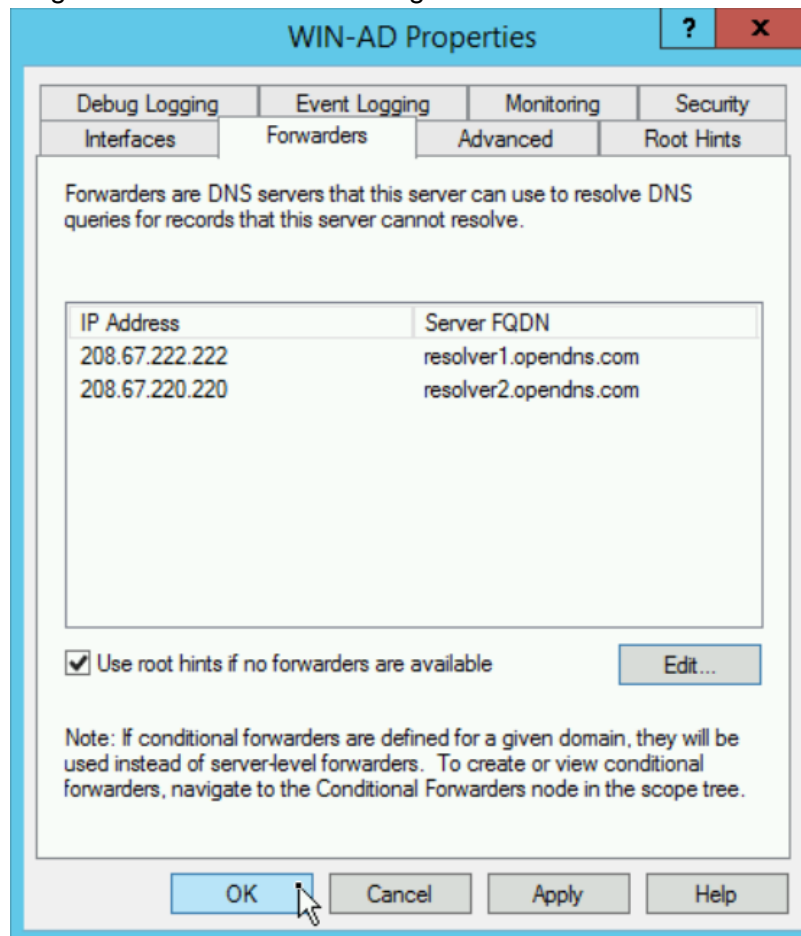
Step 4 Enter the addresses for the Umbrella DNS servers; 208.67.220.220, 208.67.222.222 and then Click OK.

Figure 32—Add Windows DNS Forwarders



Step 5 Click OK to commit the changes and close the configuration window.

Figure 33—Complete Changes to Windows DNS Manager

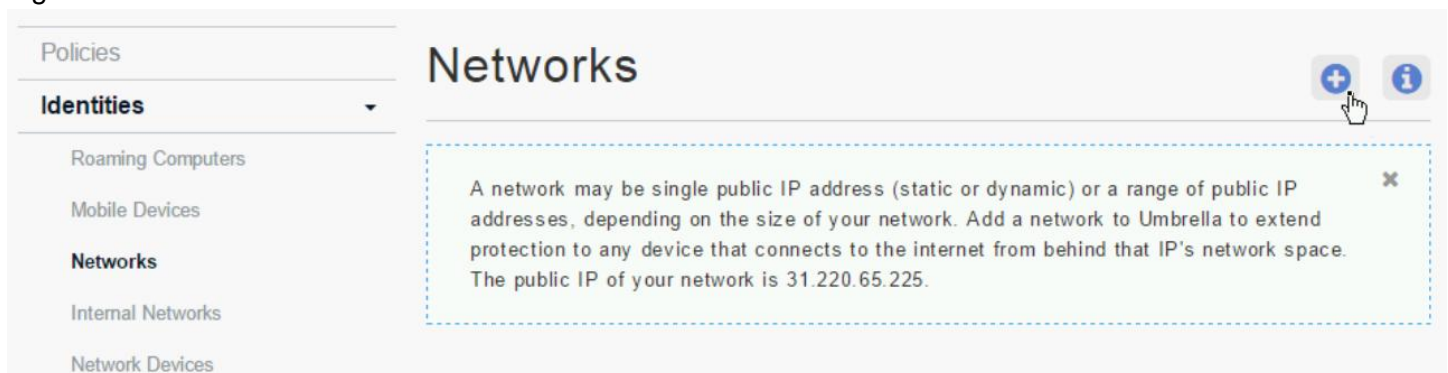


Add the public IP address that your DNS server uses to the network identities in Umbrella.

Step 6 Select Configuration > Identities > Networks.

Step 7 Click the “plus” icon to add a new network.

Figure 34—Add Umbrella DNS Network



**Step 8** Enter the public IP address of the network along with the subnet mask, usually a /32 subnet, and choose a descriptive name. Then click Save.

Figure 35—Configure New Network

The screenshot displays the 'Networks' configuration page. On the left, a sidebar lists navigation options: Policies, Identities (expanded to show Roaming Computers, Mobile Devices, and Networks), Internal Networks, Network Devices, Policy Settings, Block Page Settings, and System Settings. The main content area is titled 'Networks' and features a search bar labeled 'Search the Networks...'. Below the search bar is a form for adding a new network. The form includes a 'Network Name' field containing 'My DNS Server Public IP', an 'IP Address' field with '31.220.65.225' and a dropdown menu set to '32 (1 IP)', and a 'Dynamic' checkbox with a 'Learn More' link. There is also a checkbox for 'Enable a daily stats email to:' followed by an 'Email' input field. At the bottom of the form, there are 'CANCEL' and 'SAVE' buttons.

Now all systems that use the internal network DNS server are protected, and all activity reporting can be attributed to requests from the internal DNS server.

The Activity report shows all DNS lookup actions, and clearly designates what destination domains were blocked and the category that destination belonged to. Figure 36 shows the results of the blocked domain when trying to download ransomware or access other category blocked sites. Identity information includes the Umbrella Roaming Client system and lookups from the internal DNS server.

## Figure 36—Umbrella Blocked Domain Lookups

### Activity Search



Activity Search - All Identities - All Destinations - All IPs - All Responses - Last 24 hours (UTC-07:00 [Change time zone](#)) - All Categories - All Security Categories

Date	Time		Destination	Record	Category	Identity	External IP	Internal IP
Jul. 29, 2016	3:31:28 PM	✔	ssl.google-analytics.com	A	Search Engines	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM	✔	js-agent.newrelic.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:28 PM	✔	bam.nr-data.net	A	Software/Technology	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:26 PM	✘	devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM	✔	www.cisco.com	A	Software/Technology, Bu...	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:25 PM	✘	devnet.letmein.ml	A	Malware	Devnet-7	31.220.65.225	N/A
Jul. 29, 2016	3:31:06 PM	✔	c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:04 PM	✘	devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM	✔	www.cisco.com	A	Software/Technology, Bu...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:31:03 PM	✘	devnet.letmein.ml	A	Malware	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:24 PM	✘	whitehouse.com	A	Parked Domains, Nudity...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:14 PM	✔	c.global-ssl.fastly.net	A		My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:30:12 PM	✘	pornhouse.com	A	Pornography, Sexuality	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM	✔	clients1.google.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:53 PM	✔	bam.nr-data.net	A	Software/Technology	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:50 PM	✘	www.box.net	A	File Storage, Business S...	My DNS Server ...	31.220.65.225	N/A
Jul. 29, 2016	3:29:44 PM	✔	ssl.google-analytics.com	A	Search Engines	My DNS Server ...	31.220.65.225	N/A

## Cisco Advanced Malware Protection for Endpoints (AMP)

AMP is a cloud-based “software-as-a-service” solution. Once your account is set up, you configure a policy, then deploy AMP’s lightweight connector on your endpoints. Supported endpoints include connectors for Windows, Mac, Linux, and Android systems. If your organization has high-privacy restrictions, an alternative deployment option includes an on-premises, air-gapped AMP Private Cloud Virtual Appliance, which is outside the scope of this solution validation.

The first time you log into the FireAMP console, you will be presented with the first-use wizard. This wizard can walk you through some of the steps to quickly configure your FireAMP environment by creating exclusions for antivirus products, setting up proxies, configuring a policy, and creating groups. These steps are covered in the Quick Start Guide<sup>4</sup> and not duplicated here.

The following additional configuration steps are needed to provide the best protection possible against ransomware. Several settings are performed in the policy used by your system groups, others in the AMP account settings. First, edit the policy settings; enable Execute Mode (blocks files from being run until they have been scanned) and increase the maximum scan and archive file size limits as appropriate to fit your organization. Of the 1600+ ransomware samples we collected for solution validation, 103 of them were larger than the default 5MB Maximum Scan File Size in the Protect Policy (the largest was 51MB).

NOTE: Larger file sizes for scanning will increase WAN utilization to the Internet, and may affect other communications. For large organizations, an onsite scanning appliance may be a preferred option.

Step 1            After logging in to the AMP Console, select Management > Policies.

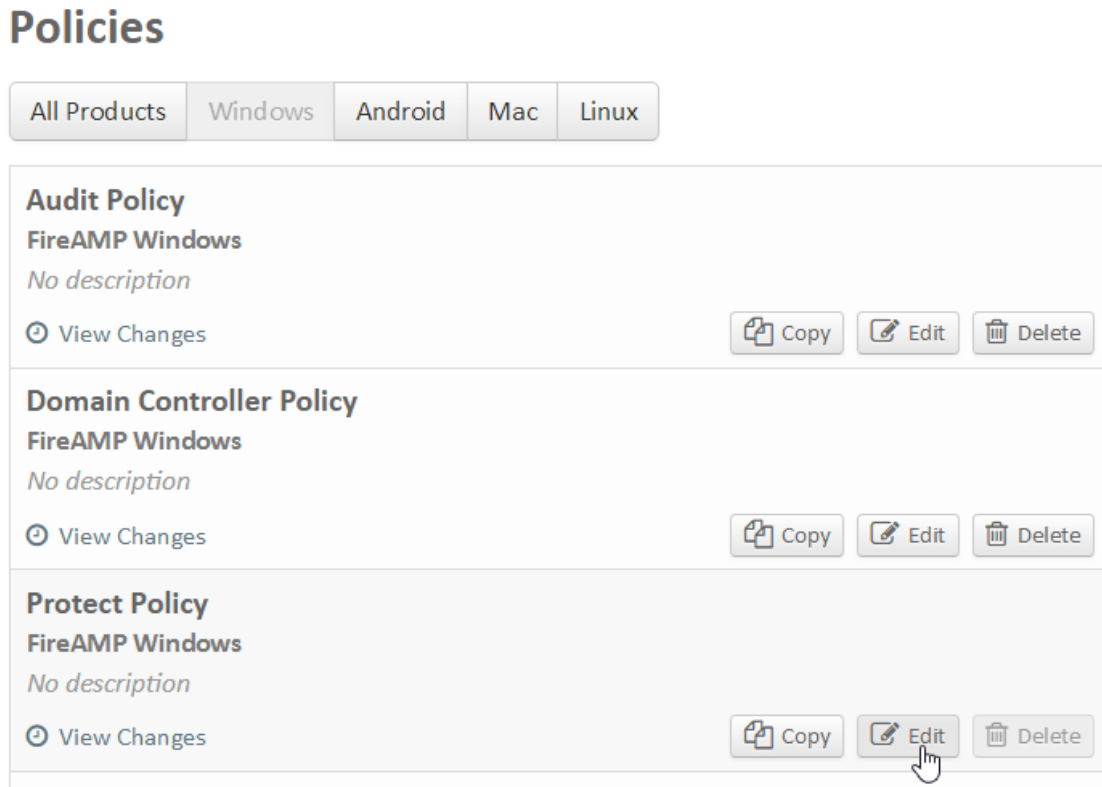
---

<sup>4</sup> <https://docs.amp.cisco.com/FireAMPQuickStartGuide.pdf>



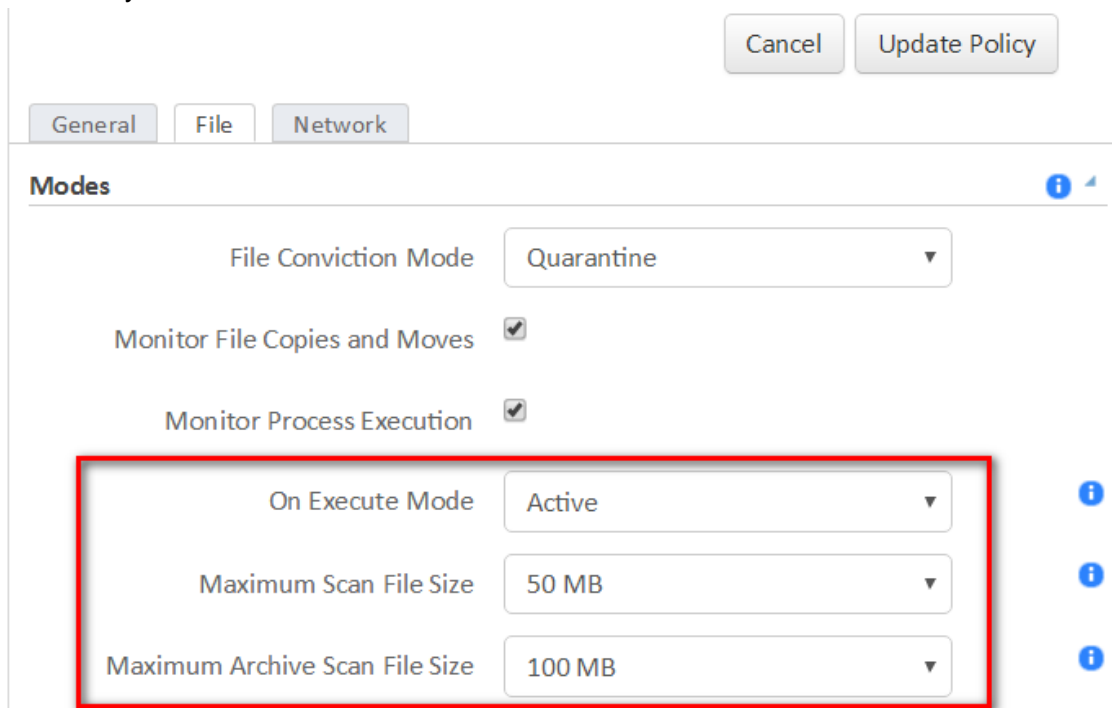
Step 2 Select the appropriate Protect Policy you are deploying to your endpoints and click Edit.

Figure 37—AMP Protect Policy



Step 3 Change to the File tab of the policy, set Execute Mode Active, and set Max file sizes.

Figure 38—Edit Policy File Attributes



Device Flow Correlation (DFC) can stop ransomware callback communications at the source and is especially useful for remote endpoints outside the corporate network.

Step 4 Select the Network Tab, set DFC Action to Blocking, and check Terminate and Quarantine.

Figure 39—Edit Policy Network Attributes

The screenshot shows the 'Edit Policy Network Attributes' window. At the top right are 'Cancel' and 'Update Policy' buttons. Below are tabs for 'General', 'File', and 'Network'. The 'Network' tab is active, showing the 'Device Flow Correlation (DFC)' section. It includes a title bar with an information icon and a close icon. The settings are: 'Enable DFC' with a checked checkbox; 'Detection Action' set to 'Blocking' in a dropdown menu; 'Terminate and Quarantine' with a checked checkbox; and 'Data Source' set to 'Custom and Sourcefire' in a dropdown menu. Information icons are present next to the 'Detection Action' and 'Terminate and Quarantine' settings. A red box highlights the 'Detection Action' and 'Terminate and Quarantine' settings.

**WARNING!** Before enabling this feature make sure you have whitelisted any applications allowed in your environment, particularly any proprietary or custom software.

Step 5 Click Update Policy when finished.

The Cisco AMP Threat Grid API allows you to automatically submit files for analysis. Before configuring Auto analysis, all users must have two-factor authentication enabled for their accounts to ensure the highest level of privacy is maintained as all analyzed files are accessible by the administrative users configured in the console. Once Two-Step Verification is enabled on your accounts, you can then edit the accounts business settings to enable the file repository, API key, and submission settings.

Step 6 Select Accounts > Business > Edit.

**Step 7** Under Features, enable “Request and store files from endpoints”, set your Threat Grid API key if you have a separate account, slide the “Daily submissions for Automatic Analysis” to the desired level, and select the VM image that best matches the majority of your endpoints. Then click Update Submission Settings.

Figure 40—AMP Account Business Settings

The screenshot displays the AMP Account Business Settings interface. At the top, there are two buttons: a grey "Cancel" button and a green "Update" button. Below this is a section titled "Features". It contains two rows of settings. The first row has the text "Request and store files from endpoints" on the left, a grey "Disable..." button in the middle, and a lock icon on the right with the text "Requires Two Step Verification". The second row has "3rd Party API Access" on the left, a "Configure API Credentials" link in the middle, and a question mark icon on the right with the text "View API Documentation". Below the "Features" section is a heading "Cisco AMP Threat Grid API". Underneath this heading is a form with an "API key" label, a question mark icon, a text input field containing "\*\*\*\*\*hjp6dm", a green "Save" button, and a grey "Use Default Key" button. Below the API key section is another form with a "Daily submissions for Automatic Analysis" label, a slider control set to "80% (200 of 250)", a "VM image for analysis" label, a dropdown menu showing "Windows 7x64", and a green "Update Submission Settings" button.

**Step 8** When finished, click Update at the top to update your account settings.

Now enable automatic analysis to send low prevalence executable files from specific groups to File Analysis.

**Step 9** Select Analysis > Prevalence > Configure Automatic Analysis.

Step 10 Select the system groups you want to enable Automatic Analysis for, and click Apply.

Figure 41—Enable AMP Automatic Analysis

## ← Automatic Analysis Configuration

This enables automatic analysis for Low Prevalence Executables per group.

The screenshot shows a configuration window titled "Automatic Analysis Configuration". At the top, it states "This enables automatic analysis for Low Prevalence Executables per group." Below this is a dropdown menu showing "1 selected" with a downward arrow. To the right of the dropdown is a green "Apply" button. The dropdown menu is open, displaying a list of system groups with checkboxes: "Audit" (unchecked), "Domain Controller" (unchecked), "Protect" (checked), "Server" (unchecked), and "Triage" (unchecked). The "Protect" option is highlighted in blue. A mouse cursor is pointing at the "Protect" option, and a tooltip labeled "Protect" is visible next to it.

Once you have configured Automatic Analysis, low prevalence executable files are submitted every four hours. FireAMP requests the file from the FireAMP Connector that observed it if it is available. Once the file has been retrieved, it is submitted to File Analysis. You can then view the results of the analysis from the File Analysis page. If the file is not retrieved for a period of time, you can check the file fetch status in the File Repository.

## Validation Testing

Solution validation testing for the first phase of the design was accomplished by creating a representative enterprise network of Windows servers and client workstations with full internet connectivity. The testing implemented Cisco's Cloud Email Security, DNS Security with Umbrella, and AMP for endpoints products.

Before testing the samples of ransomware, servers and workstations were deployed and joined to an Active Directory domain. File shares were configured from the workstations to file servers, and mapped to a drive letter. Microsoft Exchange was deployed for the email server, and email accounts were created for users unique to each workstation deployed. Various software packages were installed on the systems to best represent several typical generations of infrastructure deployments and upkeep as specified in Table 4.

Table 4 - Test System Software Installations

Test system software installations versions:							
	XPsp3x86	Win7sp1x64 Enterprise	Win10x64 Enterprise	2008R2 LOW-FS	2012R2 HIGH-FS	2012R2 AD	2012R2 Exchange
Java	Jre-6u45	Jre-7u80	Jre-8u91				
MS Office	2007	2013	2016				
Firefox	5	20	47				
MS IE	8	10	11	8	11	11	11
Acrobat Reader	10	11	DC				
Adobe Flash	12	18	21				
MS .net	2	3.5	4.5	3.5	3.5+4.5		3.5+4.5
MS Silverlight	3	4	5.1				
C++	9.0.3	9.0.3	9.0.3				
Host FW	Off	Off	Off	Off	Off	Off	Off
DNS to AD	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Join AD	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Static IP and GW	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Twenty-one families of ransomware samples were run on these systems to establish a baseline of what ransomware would infect each system build, whether administrative user right were needed, and how quickly the encryption completed for local and network shares. None of the working ransomware samples needed to perform a DNS lookup before encrypting the system. It is believed that this is because the known samples used have had their C2 domains already shut down or moved, so those samples did not function on the baseline systems, and were removed from further testing.

As all test samples were obtained from the Threat Grid File analysis repository, they were immediately recognized by AMP when the files were SHA-256 hashed by the connector and checked. To create unique versions of the ransomware for testing, a re-hashing utility was used that modified the executable files and inserted innocuous spaces or annotations, changing the resulting file hash without affecting the operation ability of the ransomware samples. This allowed testing of automatic file analysis features for low prevalence files in all products.

## Summary

Ransomware is a problem that will continue to grow and impact more organizations. If infection attacks are successful, they create a significantly negative business impact on an organization.

This solution accomplishes the goal of keeping your organization up and running, with the peace of mind that there is only a small chance of losing control of your critical systems and being held hostage.

The period of time from a new malicious campaign starting to Threat Intelligence-based protection is 30min-4hr with the Cisco Ransomware Solution, which is significantly better than the industry average of 100 days<sup>5</sup>.

Cisco Ransomware Defense focuses on prevention where possible, quick detection, and rapid containment to reduce the impact of a ransomware attack if one gets through your defenses.

For more information on Cisco Ransomware Defense solutions and products, please visit [www.cisco.com/go/ransomware](http://www.cisco.com/go/ransomware).

---

<sup>5</sup> [http://www.cisco.com/c/m/en\\_us/offers/sc04/2016-annual-security-report/index.html?KeyCode=001031927](http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html?KeyCode=001031927)

# References

Cisco SAFE Simplifies Security:

[www.cisco.com/go/safe](http://www.cisco.com/go/safe)

Cisco Cloud Email Security:

[http://www.cisco.com/web/products/security/cloud\\_email/index.html](http://www.cisco.com/web/products/security/cloud_email/index.html)

Cisco Email Security:

<http://www.cisco.com/c/en/us/products/security/email-security/index.html>

Cisco Email URL content filtering best practices:

<http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html>IG-teocv

Cisco DNS Security:

<https://www.opendns.com/enterprise-security/threat-enforcement/>

Cisco Umbrella Roaming Client Installation:

<http://info.umbrella.com/rs/opendns/images/TD-Umbrella-Mobility-Roaming-Client-Guide.pdf>

DNS Best Practices:

<http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html>

Setting up DNS Forwarding for Windows Server 2012 and 2012 R2:

<https://support.opendns.com/entries/47071344-Windows-Server-2012-and-2012-R2>

Cisco Advanced Malware Protection for Endpoints:

<http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html>

Cisco Advanced Malware Protection:

<http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html>

Cisco Talos - Comprehensive Threat Intelligence:

<http://www.cisco.com/c/en/us/products/security/talos.html>

Cisco ThreatGrid:

<http://www.cisco.com/c/en/us/solutions/enterprise-networks/amp-threat-grid/index.html>

Cisco Web Security:

<http://www.cisco.com/c/en/us/products/security/web-security/index.html>

Network as a Sensor:

<http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-sensor.html>

Cisco Stealthwatch:

<http://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>

Cisco Identity Services Engine with TrustSec (Network as an Enforcer):

<http://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/net-enforcer.html>

Cisco Rapid Threat Containment Solution:

<http://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html>

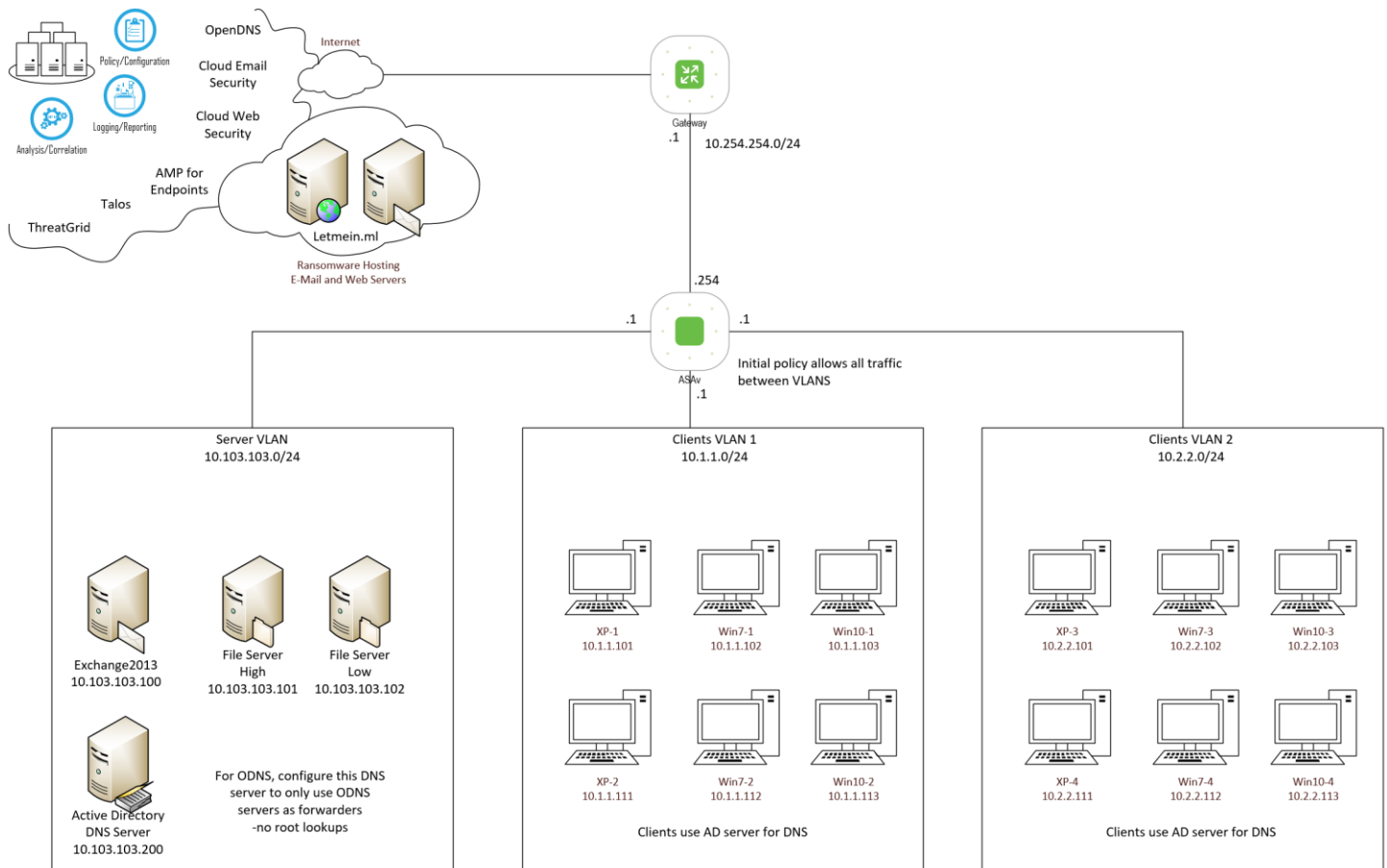
Cisco Firepower Management Center:

<http://www.cisco.com/c/en/us/products/security/firesight-management-center/index.html>

# Appendix A

## Lab Diagram

Figure 42—Lab Diagram





For more information on SAFE, see [www.cisco.com/go/SAFE](http://www.cisco.com/go/SAFE).



---

Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV Amsterdam,  
The Netherlands

---

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

---

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. (1110R)