Cloud Multicloud Portfolio:

Cloud Protect

Design and Deployment Guide for Cisco SAFE

June 2018
# Contents

**Executive summary** .................................................................................................................................................. 3  
Cisco Multicloud Portfolio: overview .......................................................................................................................... 3  
Cloud Protect: overview .............................................................................................................................................. 4  
Cloud Protect: use cases ............................................................................................................................................ 4  
Cloud Protect: benefits ............................................................................................................................................... 4  
**Technology overview** ........................................................................................................................................... 5  
Cisco SAFE................................................................................................................................................................. 5  
Cisco Umbrella........................................................................................................................................................... 6  
Cisco Umbrella roaming client ..................................................................................................................................... 6  
Advanced Malware Protection (AMP) for Endpoints ..................................................................................................... 7  
Cisco Talos Group and Cisco Threat Intelligence Group ............................................................................................. 8  
**Solution design** ....................................................................................................................................................... 10  
**Validated deployment steps** .................................................................................................................................. 13  
Configuring Windows DNS forwarding ..................................................................................................................... 15  
Enable protection against malicious files ................................................................................................................... 18  
**Appendix: product list and validation testing details** ................................................................................................. 22  
**Additional resources** .................................................................................................................................................. 23
Executive summary

Cisco® SAFE is a part of the Cloud Protect component of the Cisco Multicloud Portfolio for simplifying multicloud adoption and management. This guide will lead you through the process of deploying Cisco SAFE to provide an architectural approach to multicloud environments that includes a security reference model and a method for aligning your business requirements and security capabilities.

This guide documents how Cisco SAFE secures users’ devices connecting to the Internet (cloud), both on and off the network. This includes blocking malicious files at initial entry by inspection and using a sandbox to further inspect unknown files for advanced protection. The audience for this document includes, but is not limited to, security analysts, security administrators, and computer security professionals who want to secure their organization’s data flows and applications.

Cisco Multicloud Portfolio: overview

In a multicloud world, growing complexity is driving a cloud gap between what your customers require and what your people, processes, and tools can support. With the Cisco Multicloud Portfolio, we make it simple: simple to connect, simple to protect, and simple to consume.

The Cisco Multicloud Portfolio is a set of essential products, software, and services supported with simplified ordering and design deployment guides to help you when it comes to multicloud adoption. The Cisco Multicloud Portfolio consists of four component portfolios (Figure 1):

- **Cloud Advisory**: Helps you design, plan, accelerate, and remove risk from your multicloud migration.
- **Cloud Connect**: Securely extends your private networks into public clouds and helps make sure of the appropriate application experience.
- **Cloud Protect**: Protects your multicloud identities, direct-to-cloud connectivity, data, and applications, including Software as a Service (SaaS), and detects infrastructure and application threats on-premises and in public clouds.
- **Cloud Consume**: Helps you deploy, monitor, and optimize applications in multicloud and container environments.

Figure 1. Cisco Multicloud Portfolio: Cloud Advisory, Cloud Connect, Cloud Protect, and Cloud Consume
Cloud Protect: overview
Cloud Protect consists of essential products to protect your multicloud identities, direct-to-cloud connectivity, data, and applications, including SaaS, and detects infrastructure and application threats on premises and in public clouds:

- Cisco Umbrella™
- AMP for Endpoints
- Cisco Meraki™ Systems Manager
- Cloudlock
- Tetration Cloud
- Stealthwatch Cloud

For detailed use cases, see the section about Cloud Protect on the portfolio's solution page at https://www.cisco.com/go/multicloud.

Cloud Protect: use cases
Cloud Protect delivers value in the following use cases:

- Secure users connecting to the Internet (cloud), including users from data centers/main offices, branches (no Multiprotocol Label Switching [MPLS]), roaming places (off VPN), and direct-to-cloud users. Includes protection for ransomware, command and control callbacks, phishing attacks, and inappropriate web use.
- Secure users’ devices connecting to the Internet (cloud), both on and off the network. Includes blocking malicious files at initial entry by inspection and using a sandbox to further inspect unknown files for advanced protection.
- Enable endpoint protection by making sure that the right security services are installed and configured, by permitting only sanctioned apps to access the cloud and by constantly evaluating and dynamically taking corrective action based on changes to endpoint posture.
- Secure cloud applications and data. Includes detecting data leakages through sanctioned SaaS applications, as well as protecting sensitive data and users from malicious or compromised applications.
- Discover, map, baseline, and protect applications for workloads on the cloud, hybrid, and on the premises. Includes planning application migrations, identifying deviations in application behavior, and applying security policies for enforcing fine-grain application micro-segmentation.
- Efficiently identify threat activity and monitor user and device behavior across the public cloud and on-premises network. Use high-value, low-noise alerts to detect unusual, risky, and malicious behavior across your IT infrastructure, from the public cloud to headquarters to the branch network.

Cloud Protect: benefits
Cloud Protect benefits include:

- Secure cloud identities, data, and apps/SaaS.
- Provide secure cloud access for users on and off the network.
- Enable easy pluggable protection of mobile devices accessing apps (for example, Apple iOS devices).
- Protect workloads on public cloud Infrastructure-as-a-Service (IaaS) providers with security policy enforcement.
- Enable compliance in the cloud.
• Lower risk by providing increased visibility and control.
• Provide ~5% to 10% lower cost through simplified deployment.
• Reduce remediation time for >30% of organizations by >90%.
• Reduce malware infections for ~40% of organizations by >90%.
• Protect on-premises and cloud environments with a single vendor.
• Provide increased visibility tied into automated threat defense.
• Dynamically react to changes in endpoint posture by controlling apps, users, and services that access cloud data via laptops and mobile devices.

Technology overview
The cloud is a whole new frontier for hackers. They understand that cloud systems are mission-critical for many organizations, and they are exploring its potential as an attack vector in earnest. They also recognize that they can infiltrate connected systems faster by targeting cloud systems.

In the Cisco 2017 Annual Cybersecurity Report, we examined the risk of connected third-party cloud applications introduced into the enterprise by employees. The number of unique connected cloud apps per organization has increased dramatically since 2014. The average enterprise today has more than 1000 unique apps in its environment and more than 20,000 different installations of those apps. These apps touch the corporate infrastructure and can communicate freely with the corporate cloud and SaaS platforms as soon as users grant access through Open Authorization (OAuth).

The majority of cloud security risk stems from loss of control, lack of trust, shared access, and shadow IT. Cisco has observed an increase in hacker activity targeting cloud systems, with attacks ranging in sophistication. In January 2017, our researchers caught hackers hunting for valid breached corporate identities. Using brute-force attacks, the hackers were creating a library of verified corporate user credentials (usernames and passwords), potentially using known lists of compromised accounts on the web. They were attempting to login to multiple corporate cloud deployments using servers on 20 highly suspicious IPs.

Cisco SAFE
As your data flows from an increasing number of devices to your data center or private or public cloud, you must understand where your data is flowing to protect it. Cisco recommends using an architectural approach that helps you visualize the transit of the data.

Cisco SAFE uses security best practices that have been tested and verified to provide an architectural approach that includes a security reference model and a method to align your business requirements and security capabilities. The model incorporates security best practices and architectural designs. These validated designs provide guidance that is complete with configuration steps that make sure of effective, secure deployments for your organization. Cisco Validated Designs (CVDs) for SAFE can be found at https://www.cisco.com/go/safe.

Cisco SAFE simplifies network security by providing solution guidance using places in the network (PINs). This deployment guide provides a recommended threat defense architecture for the cloud PIN (see Figure 2).
Cisco Umbrella
Cisco Umbrella is a cloud security platform that provides Secure Internet Gateway (SIG) capabilities by blocking its connections to malicious destinations (for example, command and control) and files at the Domain Name System (DNS), IP, and HTTP/HTTPS layers. Because it is built into the foundation of the Internet, Cisco Umbrella delivers complete visibility into Internet activity across all locations, devices, and users. By analyzing and learning from this activity, Cisco Umbrella automatically uncovers attacker infrastructure staged for current and emerging threats. It can also proactively block requests before a connection is established. In this way, it can stop attacks earlier, identify already infected devices faster, and prevent data exfiltration. Cisco Umbrella provides an effective solution that is open, automated, and simple to use.

The complete Cisco Umbrella offering can protect network, roaming, and mobile devices. It includes a more comprehensive set of policy options, including restricting access to other categories of content, which might also reduce the risk of being directed to domains where ransomware might be hosted (for example, gambling, P2P/file sharing, or hate/discrimination). Several preconfigured policies are available in addition to creating a custom policy.

Cisco Umbrella roaming client
The Cisco Umbrella roaming client is a very lightweight DNS client that runs on your Windows or Mac OS X computers. It allows Cisco Umbrella security and policy-based protection, including intelligent proxy, to be enforced no matter to which network you are connected. Whether you’re at the office, a hotel, or a coffee shop or using a mobile hotspot, the Cisco Umbrella roaming client will be enforcing policies set by you in the Cisco Umbrella dashboard.

The Cisco Umbrella roaming client can be deployed directly on the endpoint or using the AnyConnect® roaming client. For more information, refer to the appropriate deployment guide.
Advanced Malware Protection (AMP) for Endpoints

Host-based antimalware 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 Advanced Malware Protection (AMP) analyzes all files that reach user systems. If a file is known to be malicious, it is quarantined immediately (see Figure 3).

**Figure 3.** Cisco AMP analyzes and quarantines all files known to be malicious

If a file is of low prevalence (for example, files never seen before and that have no history), it is uploaded automatically to ThreatGRID® for analysis (additional configuration and licensing required). This approach 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 an initial exploit kit from executing on a user's system. It can also stop execution of a 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 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 (see Figure 4).

**Figure 4.** AMP can automatically or manually contain and remediate threats based on policies
Cisco Talos Group and Cisco Threat Intelligence Group

The Cisco Talos Group (Cisco Threat Intelligence Group) analyzes millions of malware samples and terabytes of data per day. It then pushes this intelligence to AMP, providing 24/7 protection. Advanced sandboxing capabilities also enable it to perform automated static and dynamic analysis of unknown files against 500+ behavioral indicators to uncover stealthy threats.

Through the combination of both Talos and ThreatGRID threat analysis engines, suspicious email attachments and files can be sandboxed, analyzed, and categorized as malware or ransomware in as quickly as 20 to 30 minutes. However, low-prevalence files might take slightly more time to analyze and identify so as to minimize the chance of false positives.

Retrospective security intelligence for malware that evaded initial inspection is shared using Talos Threat Intelligence to both email and host antimalware services. All current and future instances of these malicious files are blocked or removed. Figure 5 shows an analysis report of a ransomware sample used in the solution validation testing.
Figure 5. Ransomware sample used in the solution validation testing as it appears in an analysis report
Solution design

To protect data accessed in the cloud, specific capabilities are necessary to build the appropriate layers of defense. The first step in developing a defense-in-depth architecture is to match all of the security capabilities that can thwart threats with real-world business functions and data flows used in the enterprise cloud environment. Table 1 identifies the SAFE methodology capabilities best suited for this defense.

Table 1. SAFE methodology capabilities and how they function

<table>
<thead>
<tr>
<th>Icon</th>
<th>Capability</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secure Internet gateway</td>
<td>Block connections to malicious destinations (for example, command and control) and files at the DNS, IP, and HTTP/S layers</td>
</tr>
<tr>
<td></td>
<td>Threat intelligence</td>
<td>Provide knowledge about existing ransomware and communication vectors and learned knowledge in new threats</td>
</tr>
<tr>
<td></td>
<td>Email security</td>
<td>Block ransomware attachments and links</td>
</tr>
<tr>
<td></td>
<td>Client security</td>
<td>Inspect files for ransomware and viruses and then quarantine and remove</td>
</tr>
<tr>
<td></td>
<td>Web security</td>
<td>Block web communication to infected sites and files</td>
</tr>
<tr>
<td></td>
<td>Identity-based firewall segmentation</td>
<td>Authenticate access and separate traffic based on role and policy</td>
</tr>
<tr>
<td></td>
<td>Intrusion prevention</td>
<td>Block attacks, exploitation, and intelligence gathering</td>
</tr>
<tr>
<td></td>
<td>Network monitoring</td>
<td>Monitor infrastructure communications using flow-based analytics, then identify and alert on abnormal traffic flows</td>
</tr>
</tbody>
</table>

In our testing and validation, each of these capabilities was deployed to combat and defend against the known seven stages of a cyberattack (see Figure 6). These capabilities work together to create multiple layers of defense, protecting the cloud assets of the organization.
Figure 6. How SAFE capabilities work together to create multiple layers of defense that protect the cloud assets of an organization.

There are layers specific to protecting endpoints such as mobile devices, securing direct-to-cloud users, and securing other devices. These devices send outbound data or telemetry, employees and partners require secure remote access, and employees and partners need secure web access to data or applications in the cloud.

Layers specific to a cloud infrastructure include web browsing and cloud application usage across a wide variety of devices, because these have the highest risk methods of infection. Also included are files saved on internal storage. Each of these three business flows is shown in Figure 7 with the selected capabilities described earlier. Across an organization, these capabilities might be duplicated in several PINs. All duplicates have been removed, and the capabilities are not necessarily in any specific order. They are just representations of the best ways to protect the flows from an end-to-end perspective.
Figure 7. SAFE capabilities as applied to three different business flows

Note that several different domain networks might exist for each of the kill chain stages (blue arrows), with differing levels of threat intelligence gathered for each. A new domain may be used for the initial phishing site, which is only hours or minutes old, whereas the subsequent malicious infrastructures might have days or weeks of known bad history. Each stage offers an opportunity for DNS security to block this communication before a compromise occurs to protect the user from infection. Additionally, Cisco Umbrella also stops command and control callbacks if an infection does occur, no matter what port or protocol is used. See Figure 8. In this figure, kill chain stages are marked in blue, and yellow arrows indicate when an infection occurs.

Figure 8. Each stage offers an opportunity for DNS security to block a malicious communication before a compromise occurs to protect the user from infection

Each of the products identified earlier provides the capabilities necessary to defend against an attack across the kill chain (see Figure 9).
To protect the organization in a cloud environment, it is important to augment existing security measures by implementing DNS and antimalware security capabilities. This guide is focused on design and deployment of these two capabilities. These are quick and easy-to-deploy cloud-enabled services that provide an immediate reduction in the risk of attacks.

The two steps to a quick and successful defense include:

- Stop command and control communication and redirection of malicious sites by adding a layer of DNS security (Cisco Umbrella) for on-net and off-net protection.
- 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 first, then executives, key servers, and finally as broadly as possible.

Each of these offerings shares the cloud-based services of Talos Threat Intelligence, ThreatGRID file analysis, and Cisco Umbrella Threat Intelligence.

**Validated deployment steps**

A SIG provides safe access to the Internet anywhere users go, even when they are off the VPN. Before you connect to any destination, a SIG acts as your secure on ramp to the Internet and provides the first line of defense and inspection. Regardless of where users are located or to what they are trying to connect, traffic goes through the SIG first. After the traffic gets to the SIG cloud platform, different types of inspection and policy enforcement can be applied.

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 protects devices both on and off of an organization’s network for all communication types, not just websites. In the case of the initial launch, where a URL would take a user to a
seemingly trustworthy site, Cisco Umbrella provides DNS security as part of its offering and blocks the DNS request. It then replaces the request with a safe destination before the user’s browser connects to the malicious site (see Figure 10). This step occurs whether the user clicked a link or if there was a redirect from a compromised site.

**Figure 10.** Cisco Umbrella enforces security by blocking and then replacing DNS requests with a safe destination before a user’s browser can connect to a malicious site

![Image of Cisco Umbrella enforcement](image)

Figure 11 shows the high web filtering policy that was used in our validation testing.

**Figure 11.** High web filtering policy

![Image of high web filtering policy](image)
For organizations that implement their own internal network DNS servers, Cisco Umbrella can easily be enabled for the entire network. You can do this enabling by configuring your DNS server to use the Cisco Umbrella servers as forwarders instead of performing their own root lookups for external domains. This approach eliminates the need to deploy the Cisco Umbrella client on any internal network system, making for a simple clientless implementation that protects everything on the network.

**Configuring Windows DNS forwarding**

The following steps outline how to configure Windows DNS forwarding to use Cisco Umbrella as we did for part of our validation testing.

**Step 1.** Open Windows DNS manager under Server Tools (see Figure 12).

**Figure 12.** Windows DNS manager can be opened from the Server Tools tab

**Step 2.** Choose the server to edit, then select Forwarders (see Figure 13).

**Figure 13.** Choose the server to edit, then select Forwarders
Step 3. Click Edit (see Figure 14).

Figure 14. Edit forwarders for the appropriate server

Step 4. Enter the addresses for the Cisco Umbrella DNS servers. Use 208.67.220.220 and 208.67.222.222, then click OK (see Figure 15).

Figure 15. Enter the Cisco Umbrella DNS server addresses
Step 5. Click OK to commit the changes and close the configuration window (see Figure 16).

Figure 16. Commit the changes you’ve made by clicking OK

Next, add the public IP address that your DNS server uses to the network identities in Cisco Umbrella.


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

Step 8. Enter the public IP address of the network along with the subnet mask, usually a /32 subnet. Choose a descriptive name, then click Save (see Figure 17).

Figure 17. Enter the public IP address for the network
You have completed configuration of Windows DNS forwarding.

Now that all systems that use the internal network DNS server are protected, all activity reporting can be attributed to requests from the internal DNS server. For example, this activity report shows all DNS lookup actions, as well as clearly designates which destination domains were blocked and the category to which that destination belonged. It also shows the results of a blocked domain when trying to download ransomware or access other category-blocked sites (see Figure 18).

**Figure 18.** This activity report shows all DNS lookup actions and designates which domains were blocked.

Enable protection against malicious files

AMP is a cloud-based SaaS solution. After your account is set up, you configure a policy and 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 design and deployment guide.

The first time you log in to the FireAMP console, you are presented with the first-use wizard. This wizard can help you quickly configure your FireAMP environment by creating exclusions for antivirus products, setting up proxies, configuring policies, and creating groups. These steps are covered in the QuickStart Guide¹ and not duplicated here.

The following additional configuration steps are needed to provide the best protection for a cloud environment. Several settings are performed in the policy used by your system groups, others in the AMP account settings.

¹ [https://docs.amp.cisco.com/FireAMPQuickStartGuide.pdf](https://docs.amp.cisco.com/FireAMPQuickStartGuide.pdf)
First, edit the policy settings. Start by enabling execute mode, which blocks files from being run until they have been scanned. Then increase the maximum scan and archive file size limits as appropriate to fit your organization. Of the 1600+ ransomware samples we collected for this solution validation, 103 were larger than the default 5-MB maximum scan file size in the protect policy (the largest was 51 MB).

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

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

**Step 2.** Select the appropriate protect policy you are deploying to your endpoints and click Edit (see Figure 19).

**Figure 19.** Select a protect policy to deploy to endpoints

![Policies](image)

**Step 3.** Change to the File tab of the policy. Then set on execute mode to Active. Next, set your maximum file size (see Figure 20).

![Policy Options](image)
Figure 20. Set the maximum file size

![Figure 20](image)

Note that Device Flow Correlation (DFC) can stop ransomware callback communications at the source. This fact makes it especially useful for remote endpoints outside the corporate network.

**Step 4.** Select the Network tab. Then set DFC action to Blocking. Next check Terminate and Quarantine (see Figure 21).

**Reader Tip**

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

Figure 21. Set the DFC action to block with the option to terminate and quarantine

![Figure 21](image)
Step 5. Click Update Policy when finished.

The Cisco AMP ThreatGRID API allows you to automatically submit files for analysis. Before configuring auto analysis, all users must have two-factor authentication enabled for their accounts. This enablement is to make sure that the highest level of privacy is maintained as all analyzed files are accessible by the administrative users configured in the console.

After two-step verification is enabled on your accounts, you can edit the accounts' business settings to enable the file repository, API key, and submission settings.


Step 7. Under Features, enable Request and store files from endpoints. Then set your ThreatGRID API key if you have a separate account. Next, slide daily submissions for automatic analysis to the desired level. Then select the VM image that best matches the majority of your endpoints. Click Update Submission Settings (see Figure 22).

Figure 22. Set the ThreatGRID API key, select the desired level for daily submissions for automatic analysis, and then match the appropriate VM image

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 10. Select the system groups for which you want to enable automatic analysis and click Apply (see Figure 23).
Figure 23. Select the system groups for which you want to enable automatic analysis

![Automatic Analysis Configuration](image)

You have completed the process for malicious file protection.

After 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. After 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.

**Appendix: product list and validation testing details**

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. Testing was implemented with Cisco Umbrella using AMP for endpoint products.

Before samples of malicious threats were tested, servers and workstations were deployed and joined to an Active Directory domain. File shares were configured from the workstations to file servers and then 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 later. (See Table 2.)

**Table 2. Test system software installation versions**

<table>
<thead>
<tr>
<th></th>
<th>XPsp3x86</th>
<th>Win7sp1x64 Enterprise</th>
<th>Win10x64 Enterprise</th>
<th>2008R2 LOW-FS</th>
<th>2012R2 HIGH-FS</th>
<th>2012R2 AD</th>
<th>2012R2 Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>Jre-6u45</td>
<td>Jre-7u80</td>
<td>Jre-8u91</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Office</td>
<td>2007</td>
<td>2013</td>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox</td>
<td>5</td>
<td>20</td>
<td>47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS IE</td>
<td>8</td>
<td>10</td>
<td>11</td>
<td>8</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Acrobat Reader</td>
<td>10</td>
<td>11</td>
<td>Data center</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adobe Flash</td>
<td>12</td>
<td>18</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS .net</td>
<td>2</td>
<td>3.5</td>
<td>4.5</td>
<td>3.5</td>
<td>3.5+4.5</td>
<td>3.5+4.5</td>
<td></td>
</tr>
<tr>
<td>MS Silverlight</td>
<td>3</td>
<td>4</td>
<td>5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C++</td>
<td>9.0.3</td>
<td>9.0.3</td>
<td>9.0.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host FW</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
Twenty-one families of threat samples were run on these systems to establish a baseline of which threats would infect each system build, whether administrative user rights were needed, and how quickly the encryption completed for local and network shares.

None of the working samples needed to perform a DNS lookup before encrypting the system. It is believed that this fact is because the known samples used had had their command and control domains already shut down or moved. Because these samples did not function on the baseline systems, they were removed from further testing.

Because all test samples were obtained from the ThreatGRID 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 threats for testing, a rehashing utility that modified the executable files and inserted innocuous spaces or annotations was used, changing the resulting file hash without affecting the operation ability of the ransomware samples. This approach allowed testing of automatic file analysis features for low-prevalence files in all products.

**Additional resources**

If you have further questions, refer to the following additional resources:

- Cisco Umbrella: [https://www.cisco.com/go/umbrella](https://www.cisco.com/go/umbrella)
- Cisco Umbrella Roaming Client Deployment Guide: [https://docs.umbrella.com/product/umbrella/1-introduction-1/](https://docs.umbrella.com/product/umbrella/1-introduction-1/)


For a complete list of all of our design and deployment guides for the Cisco Multicloud Portfolio, including Cloud Protect, visit [https://www.cisco.com/go/clouddesignguides](https://www.cisco.com/go/clouddesignguides).

About Cisco design and deployment guides
Cisco Design and Deployment Guides consists of systems and/or solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit: [https://www.cisco.com/go/designzone](https://www.cisco.com/go/designzone).

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networks, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.