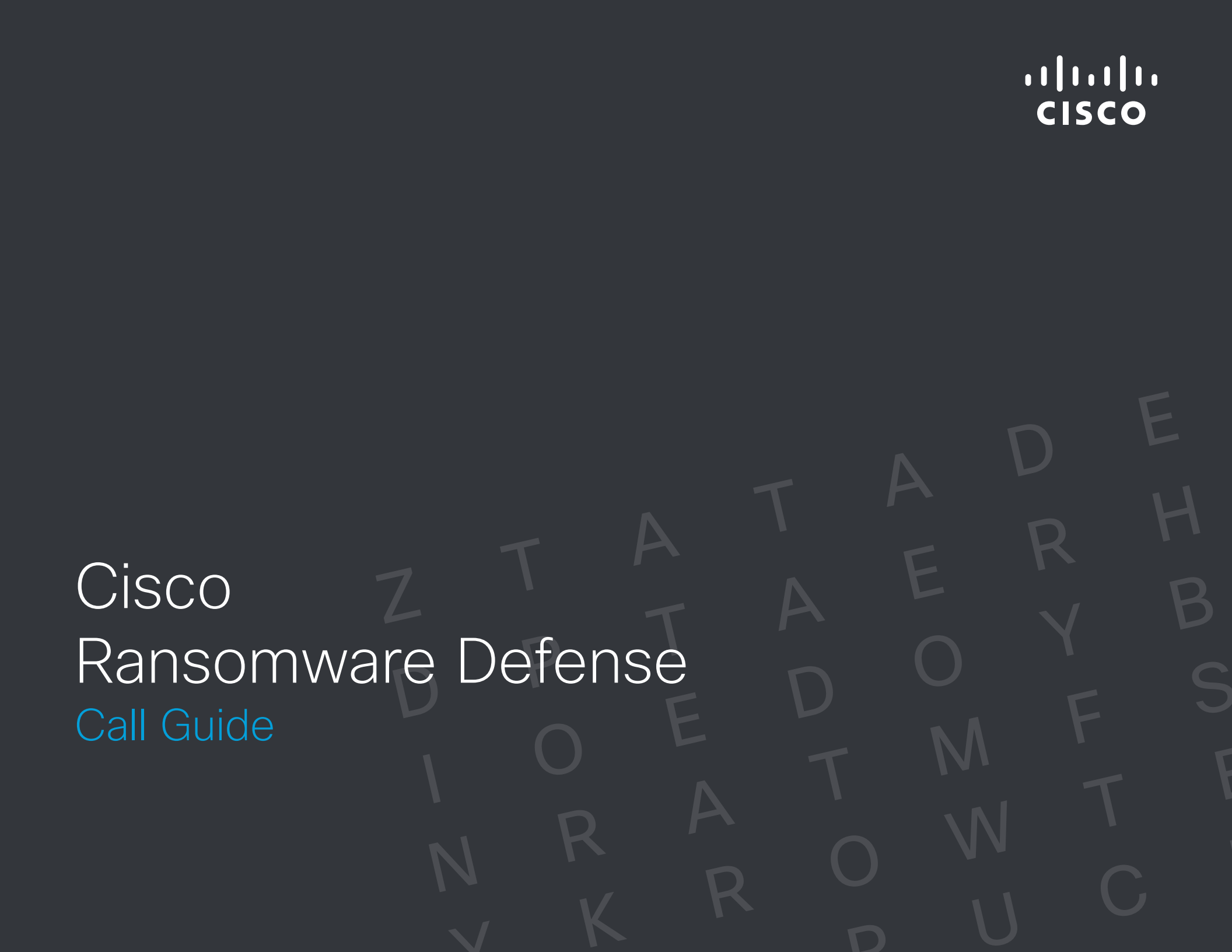
Cisco Ransomware Defense

Call Guide



Cisco Ransomware Defense

Purpose

This call guide is designed to provide a set of introductory questions to help you discover Cisco® Ransomware Defense opportunities. It can assist you in planning and executing an approach to prospects, engaging effectively on their terms, and transitioning into a sales pursuit when an opportunity appears qualified.

Your primary goal is to determine whether a customer warrants a conversation, either right now or in the future. If you perceive an immediate opportunity, your target outcome will be a meeting to understand the customer's challenges and opportunities.

Target Audience and Organizations

The Cisco Ransomware Defense solution targets enterprise, commercial, small and midsize businesses, and large public sector customers who need comprehensive security solutions to protect their organizations from threats. These days, every organization across every industry is a target for an attack.

The buying centers for security are also diverse. The primary audience for Cisco Ransomware Defense is IT security managers, chief information security officers, incident responders, and the overall security team at an organization. However, with security now a boardroom discussion, and security being implemented from the endpoint to the network, you will need to engage other teams beyond just security. Other buying centers include the desktop and endpoint team, networking team, CIO, COO, and even the CEO.

Why Engage?

Acquire New Customers

- Every organization needs security. Engage new opportunities by sharing the Cisco Ransomware Defense value proposition: Cisco Ransomware Defense reduces the risk of ransomware infections with a layered approach, from the DNS layer to the endpoint to the network, email, and the web. Cisco delivers integrated defenses with an architectural approach that combines ultimate visibility with ultimate responsiveness against ransomware.

Migrate Customers

- Migrate customers who are currently using antivirus, firewalls, intrusion prevention systems (IPS), and web and email security appliances from competitors such as FireEye, Palo Alto Networks, Lastline, Trend Micro, Symantec, McAfee, CheckPoint, Fortinet, and more.
- Migrate customers who use competitive products and who either are dissatisfied with their current vendor, have a subscription that is coming up for renewal, or have a product that is nearing end of life.
- Migrate customers who use a competitor's security products and yet still experienced a breach.

Up-Sell Existing Cisco Customers

- Up-sell Cisco Ransomware Defense to customers that have any level of Cisco products in their network architecture, even outside of security. Cisco builds security tools that communicate with each other and with other Cisco technology, to provide security everywhere across multiple attack vectors (endpoint, network, mobile, web, email, and cloud). Deploying fragmented offerings across multiple vendors can lead to less communication between point products, a lag in time to detection, and a higher total cost to build, manage, and troubleshoot.
- Sell the value of the Cisco streamlined solutions approach. Our tools are integrated, communicate and share information, provide faster time to detection, can lower OpEx, and are easier to manage through one trusted vendor. For more information on Cisco's Security Everywhere approach, review these materials: Cisco Executive Perspectives on Security and the Security Everywhere white paper.

Talking Points

The solution compromises the following core components:

- *Cisco Umbrella* protects devices on and off the corporate network. It blocks DNS requests before a device can even connect to malicious sites hosting ransomware.
- *Cisco Advanced Malware Protection (AMP) for Endpoints* blocks ransomware files from opening on endpoints.
- *Cisco Email Security with Advanced Malware Protection (AMP)* blocks spam and phishing emails and malicious email attachments and URLs. The technology is the same as that applied on the endpoint, but it's deployed at the email gateway.
- *Cisco Firepower Next-Generation Firewall (NGFW) with Advanced Malware Protection (AMP) and Cisco Threat Grid* sandboxing technology stops threats by containing known and unknown malware and blocking command-and-control callbacks to ransomware hosts.
- *Cisco security services* provide immediate triage in the case of an incident. They also streamline deployments of AMP, NGFW, and other solution products.

Competitive Positioning

- The security market overall is fragmented, with many point-product vendors whose standalone products focus on only one part of the network, causing disparate security.
- Only Cisco brings a security architecture to bear in confronting the ransomware challenge. Point products alone will not suffice. Our solution is backed by our industry-leading Talos Research Group, which has carried out extensive threat research on ransomware, powering our effective layered protection model.

Introduction

Hello, [Contact Name]. This is [Your Name] calling on behalf of Cisco and [Partner Name]. Do you have a few minutes to talk?

I'm sure you have seen stories in the media about the rapid increase in ransomware attacks. I just wanted to let you know about Cisco's full architecture solution, Ransomware Defense. Can I ask you [use Trigger Questions below]?

Our solution provides [use appropriate Cisco solution copy block below].

Trigger Questions

All questions are designed as an introduction to ransomware and the need for a layered security approach. Following the questions, you can dive into the components of the solution and how they will meet the customer's needs.

Trigger Question	Cisco Solution – With Cisco You Can
Do you believe your current IT security is protecting you from ransomware?	Cisco believes that in order to reduce the risk of ransomware infections, your security measures require a portfolio-based approach, rather than a single product. Ransomware must be prevented where possible, detected if it gains access to systems, and contained to limit damage. Cisco Ransomware Defense uses the Cisco security architecture to protect businesses, with defenses that span from networks to the DNS layer to email to the endpoint. It is backed by industry-leading Talos threat research for the ultimate responsiveness against ransomware.
Do you know that most ransomware attacks use DNS to gain access to your network?	Cisco Umbrella solutions will block the ransomware threats at the DNS layer, and prevent the attack from gaining access to your network, systems, and critical files. Cisco Umbrella is quick to install and provides protection against the majority of known ransomware attacks.
If compromised, are you confident in your time to detection and remediation?	Ransomware Defense consists of technologies that block threats, from the DNS layer to the network to the endpoint, with Cisco Umbrella, Cisco AMP for Endpoints, Cisco Email Security and Cisco Firepower NGFW. You can also segment your network with Cisco ISE pushing policies down to the network, and by using Cisco TrustSec® to contain the attack so ransomware cannot spread laterally. With Cisco AMP embedded everywhere – on the endpoint, in email security, and on the network with our NGFW –organizations can reduce their time to detection from days to minutes. With Ransomware Defense, organizations can use their network as an enforcer to contain the spread of ransomware. It will not be able to propagate as easily on the network in the worst-case scenario of an infection.

Objection Handling

Objection	How to Respond
I've never heard of Ransomware Defense. Is Cisco new to this business?	Cisco has been investing significantly in the improvements and posture of their security solutions. The Ransomware Defense solution is relatively new, yet the need for an integrated threat defense is not. The solution combines years of research and product advancements into one comprehensive solution that will protect you, from the network to the DNS layer to email to the endpoint. It is backed by industry-leading Talos threat research for the ultimate responsiveness against ransomware.
Is security a Cisco priority? I am only aware they sell routers, switches, etc.	
We have limited budget. I've looked at Cisco in the past, and your security products seem more expensive than other solutions.	Have you thought about financing through Cisco Capital®? Financing is very flexible. You can choose to defer payments to better reflect your return on investment and begin payments when the technology is up and running. Cisco Capital assists in moving forward your investment in technology to help your business and provides a finance solution that is tailored to meet your specific needs. Cisco Capital can finance the entire solution (hardware, software, services, and complementary third-party equipment). You can find out more about financing options at www.ciscocapital.com.
I already have a firewall and other great security products and services. What differentiates the Cisco solution from the products that protect me now?	Cisco believes that in order to reduce the risk of ransomware infections, your security measures require a portfolio-based approach, rather than a single product. If you already have a Cisco firewall or AMP, you can simply add the rest of the solution to your defenses. Cisco Ransomware Defense uses the Cisco security architecture to protect businesses, with defenses that span from the network to the DNS layer to email to the endpoint. It is backed by industry-leading Talos threat research for the ultimate responsiveness against ransomware. From here, you can go into the product talking points, listed under "Talking Points."
I currently have [xx] amount of Cisco security products already. Won't those protect me from ransomware?	Your existing security products will certainly help protect you. However, ransomware attacks are evolving at a quick pace. Their attack vectors alone are increasing as the malware becomes more sophisticated. Because of this, the Ransomware Defense solution encompasses multiple products that will give you protection at the DNS layer, network, email, web, and endpoints. Combined with our industry-leading Talos threat research, having the full solution deployed decreases your chances of an attack significantly. May I ask what products you already have deployed? (Compare and contrast with the solution product list under "Talking Points.")
With ransomware technology rapidly increasing, there is still a chance that I may be infected. What happens then?	In the worst-case scenario of an infection, dynamic segmentation with Cisco TrustSec (via Network as a Sensor and Network as an Enforcer) can block ransomware from moving broadly once it is inside the network. This is vital in helping ensure that it cannot run rampant in a network and affect a majority of systems. Cisco malware protection services (AMP plus Threat Grid) provide the ability to retrospectively remove the malware from endpoints where it has been seen. This means that in a worst-case scenario, one or two endpoints might be affected while the learning happens, and then the defense in-depth approach removes the malware from endpoints where it might sit dormant.
What about security for branch locations?	For branch locations that want direct Internet access but also protection against ransomware, Umbrella Branch on the Cisco Integrated Services Router (ISR) can be set up at branches for an initial layer of protection. Cisco Firepower Threat Defense for ISR, including AMP, can also be activated, increasing security for "HQ" level security at the branch. These both reduce WAN costs with no need to backhaul traffic.

Customer Interest Offers

Customer Buying Stage	Goals	Offer Call to Action
Awareness	Establish relationship and educate them about Cisco technology and solutions.	- Ransomware Defense At-a-Glance - Ransomware Infographic
Consideration and evaluation	Evaluate needs and demonstrate the value of Cisco technology, and help the customer understand how it compares to the competition.	- " Ransomware: Everything You Need to Know" White Paper - Ransomware Defense Solution Overview
Design	Provide design resources and help the customer better understand how to implement this solution.	- " Ransomware: A Layered Defense" White Paper - Recorded Demo and Webinar
Purchase	Close the sale. Customer is ready to purchase.	- Ransomware Defense Solution ID on Cisco Commerce Workspace (CCW)

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.**