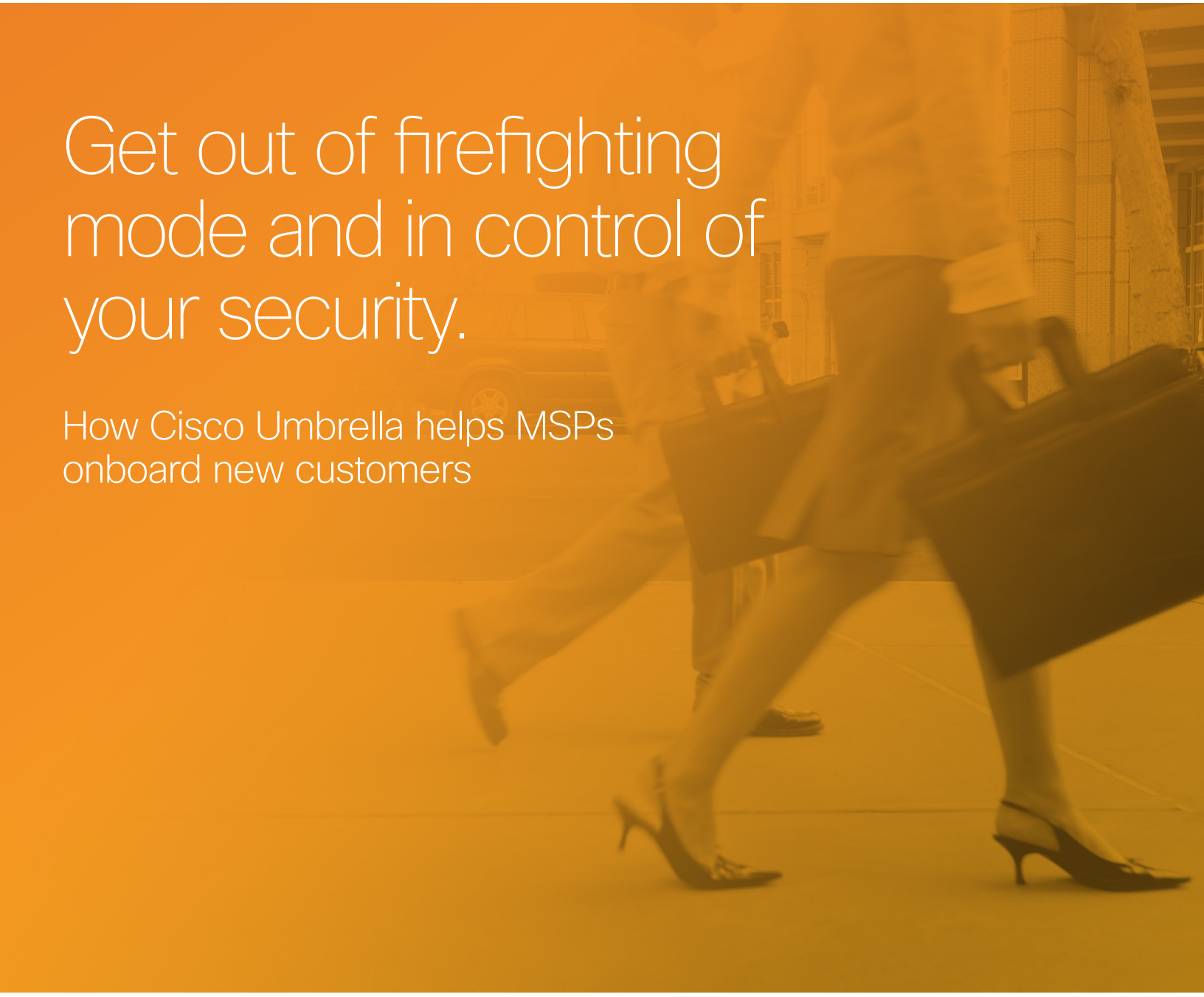
Cisco Umbrella

WHITE PAPER

Get out of firefighting mode and in control of your security.

How Cisco Umbrella helps MSPs onboard new customers



Introduction

As an MSP, you know the drill: You just signed a new customer and your team enthusiastically sets them up with your remote monitoring and management (RMM) software to move your customer from reactive responses to proactive control. The customer, on the other hand, just wants their current pain points to go away. They probably have been unhappy with their IT support. They are desperate for help. They count on you to put measures in place to ensure security issues do not arise again. And they want everything to be resolved from day one. That means you need to get up and running quickly.

But when you are under pressure, there is little time to audit a customer's existing setup, leading to a flood of new tickets for your team. It's a rough start because you are spending too much time reacting to problems instead of truly managing the network and infrastructure in a sustainable manner.

Fortunately, there is a better way to start quickly and build controls for the long term: Cisco Umbrella. Deploying Cisco Umbrella for MSPs takes minutes, giving you more time to do what you need. By cutting down the distraction from malware tickets, Umbrella for MSPs helps you onboard the customer from a calm, proactive stance.

It's time to get out of firefighting mode and get in control.

Moving from reactive to proactive security management

You are probably familiar with this scenario: You have just taken on a new customer for your "all you can eat" managed service. You have discussed a transition period to get the customer set up properly but they are pressing for immediate assistance. For most MSPs, the process of onboarding new customers can be intense. Though you may wait months for a prospective customer to sign, once they have awarded the contract, you have to move at warp speed.

You now have a huge spike in technical support requests. Your customer has a big backlog of both small and large IT issues that they have been waiting for their new MSP to resolve. Your customer expects you to make the previously unknown issues magically disappear. But this flood of tickets puts your engineers in firefighting mode, rapidly resolving small issues while leaving the larger causes unresolved. This is a common situation when misconfigurations, inadequate solutions, and lack of policy have created a perfect storm for a flood of infection tickets.

Often, you do not have time to fully audit their existing security solutions before taking responsibility for the infrastructure. Once you are busy responding to issues and closing tickets, it is hard to step back and make sure everything is properly set up.

You are in a bind: You do not want to dampen your customer's enthusiasm by delaying the onboarding process and postponing service delivery. And you certainly do not want to lose revenue. But you need to buy time to do things the right way with automation, alerts, and the appropriate setup.

"It's not uncommon for a customer to award a new contract on a Friday and expect service to begin on the following Monday."

The problems with firefighting

Competing priorities. You have to decide how to apply your time and resources to best serve your customers. Urgent issues with business-critical applications, network connectivity, and infections often create new fires and distract you from efficiently managing service delivery.

Exceptions per user leave you more vulnerable. Some applications require specific port or protocol access that can be impacted by security controls. To quickly set up these types of applications for "special" users, the previous IT provider may have created one-off exceptions to disable or modify security policies.

Shortcuts and rework are expensive. When you are in firefighting mode, you do whatever it takes to get the job done. Example: A customer calls dispatch with a network or phone system outage that the engineers are eager to address. To end the outage, they shut off everything that could be between the user and the network, including security controls. After the outage, these same engineers may put off reverting the changes.

Disabling security controls for troubleshooting. Sometimes security controls and other services like backup are shut off to facilitate troubleshooting. Frequently, the settings are not changed back, which results in holes in your security policy that could lead to future damage or infections and could increase your ticket count. Short-term fixes contradict long-term customer success.

Key questions to ask

- [ ] Do your engineers have expertise with the customer's existing firewall's security settings?
- [ ] What options cause a UTM/firewall to slow down or disrupt connectivity?
- [ ] Is antivirus deployed on all endpoints?
- [ ] Are customer computers able to run antivirus in full protection mode or are they too slow?
- [ ] Are there any devices or users that are made into exceptions?
- [ ] Is it possible to get a baseline of how many infections the customer had with the existing infrastructure?
- [ ] Are employees trained to not click potentially malicious links?
- [ ] What applications clash or crash with existing security and settings?
- [ ] Can an engineer tell which firewall ports are blocked?

Key question: How do you keep critical applications and infrastructure running while moving them to standards?

One of the biggest challenges to taking on a new customer is understanding and working with their existing setup. You need to balance maintaining current operations with progress towards a sustainable, automated, and proactive state. Security is a big part of that and infections can get in the way of achieving the long-term goal. Customers may already have unified threat management (UTM) or firewall and antivirus installed by the time they call you for help, so it is up to you to decide whether you can move them to your own stack, work with what they have, or suggest other elements that they may need.

In many cases, by the time your customer hires your MSP, they have already purchased expensive hardware and are not ready to part with it. You may have to support software or hardware in which you do not have expertise, making it difficult for you to discover underlying security issues.

"How can your Support team provide protection to a new customers IT infrastructure without resorting to a "rip and replace" mentality which is likely to be undesirable to the new customer?"

Discovery

It is up to you to discover what is going on in your customer's environment. An audit is the most effective way to get an understanding of a customer's environment and determine the best approach towards standardization.

Some mature MSPs go through an extensive audit process before onboarding a customer. They often charge the customer for the time spent transitioning to the MSP's standards and build in reactive hours as part of the transition. This is a good way of equalizing the upfront costs of discovery, but it can be a sales challenge.

Even with a thorough audit, however, MSPs may still encounter surprises. For example, a customer may have purchased your standardized firewalls, but someone annoyed with the limitations of the firewall and with keys to the closet (perhaps the CEO or another executive) has unplugged the appliance.

Standardization

Standardization is a cornerstone to the MSP business model – an essential way for you to provide sustainable and scalable, high quality customer support. The complexity of unfamiliar hardware and software across your customer's IT infrastructure can result in a spike in resources allocated to onboarding and to providing customer services.

You can approach standardization a few different ways. The "rip and replace" method of standardization is drastic but effective for long-term stability. In this situation, the MSP aims to replace the customer's unfamiliar or undesirable equipment with equipment endorsed by the MSP, to bring equipment up to the MSP's mandated security standards. The benefit is that the MSP can much more easily manage their customers' systems. But many customers are not up for the time and cost associated with rip and replace projects.

An alternative is "piecemeal" standardization in which the customer's equipment (hardware/software) is gradually replaced by the MSP. In this situation, the MSP reduces the setup cost burden and the time to provide service. This decreases the financial burden on your customer because it means there are less upfront hardware costs, but it increases the burden on your MSP because it requires you to work with hardware, software, and network configurations that might be unfamiliar. As the customers' virtual CIO, you can schedule refreshes, but this process extends the time to profitability.

Which of these costly onboarding nightmares have you experienced?

You provide both malware protection and remediation for a flat fee. But how well do you understand the associated costs? How might you simplify your process? You should understand some common problems that increase the cost of service delivery. When you are firefighting, these are often overlooked and can increase the time you spend managing your customers, remediating issues, and cleaning infected devices.

- **The firewall or network equipment is incorrectly configured.** We assume that if we have firewalls or network equipment in play, then they are plugged in and properly set up. Unfortunately that is not always the case, and it often takes a while to recognize. Frequently, MSPs will discover firewalls have been unplugged or disabled during past troubleshooting efforts.
- **Computers do not have antivirus or standard security protection installed.** It takes time to bring all endpoints into compliance. MSPs commonly discover that their customers have old computers that lack adequate antivirus protection. This may happen because antivirus causes a performance impact that makes older machines unusable, and other times because of a simple oversight. This can have a big impact on your MSP because you have to remediate more infections when you rapidly onboard a customer that does not have security protection on endpoints.
- **Special users with security exceptions.** These are VIPs or just random people whose security settings circumvent existing security policies. Most often, this is done as a quick and dirty workaround to bypass filtering or to make applications work. Unfortunately, it is difficult to identify these special users without a full audit. In the meantime, they might be exposed to more risk than other users.

Checklist for supporting unfamiliar equipment

- [ ] You have identified a firewall or UTM connected to the customers broadband internet, but it is an unfamiliar make/model. Can you support this unit effectively? Will the manufacturer offer you support? Is it even plugged in?
- [ ] You identify a recognizable antivirus solution on a customer's workstation, but is that software up to date and is that same software actually present across all workstations?
- [ ] Do you have a clear understanding of the applications in use and their various impacts on the network and the security stack?

The solution: Platform agnostic network security control

Hardware agnostic solution

Here's what you can do to offer immediate security company-wide and to minimize long-term rework: Build a layer of hardware platform agnostic network security controls that you can deploy easily and quickly to offer security intelligence and enforcement. This resolves the urgent need to prevent malware infections and block botnet callbacks, reducing your ticket count instantly. It also offers you the ability to cut reactive hours so that you can spend more time on the audit and discovery, building a better long-term IT strategy for your new customer. Applying a vendor agnostic network security layer helps you standardize and maintain a lower overall ticket count, making your new customer a more profitable one.

"How can an MSP reduce the typical spike in support requests that is generated by a newly onboarded customer?"

Cisco Umbrella for MSPs

Cisco Umbrella for MSPs works the way the internet works, offering a consistent layer of security through recursive DNS. It can be set up in minutes, no matter what hardware or software you run. You can secure corporate networks, as well as company-owned laptops, which may contain private company data, that leave the office.

You can deploy Umbrella for MSPs regardless of your customers' setups. By deploying Umbrella for MSPs, you give your team breathing room – they do not need to respond to so many infections because Umbrella provides automated protection. You just configure it and let it run.

First line of defense against threats. Umbrella is built into the foundation of the internet and blocks requests to malicious and unwanted destinations before a connection is even established – without adding any latency.

Visibility and protection everywhere. Umbrella provides the visibility needed to protect internet access across all devices on your customer's network, all office locations, and roaming users.

Customer-wide deployment in minutes. Umbrella is easy to deploy, enabling you to provide fast security for your customers, across all their locations and users.

Standardized settings. Manage all your customers' policies from one place. You can modify security controls by customer and have the granularity of control to manage access by user.

Centralized settings. The centralized settings feature in Umbrella provides a simple and powerful way for MSPs to create and manage settings that are shared among multiple customers and can be automatically applied from day one.

By automatically provisioning customers with your custom defined and tuned settings, they start with your defined security policies without touching a button, so you can be comfortable knowing that your new customers are protected from the start. Then once you have time or need, you can customize the customer's policy, with either reusable or completely new settings. The choice is yours!

It's easy to make changes later because centralized settings are truly linked between multiple customers. You can change the settings for all customers at once or by creating new vertical or use case specific policies specific for smaller groups.

Benefits

- Streamline your process
- It's easy to use without any need for specialized training
- Save time with standardization and automation
- Manage your customers with complete control and flexibility
- Over 2800 MSPs have deployed Cisco Umbrella for MSPs