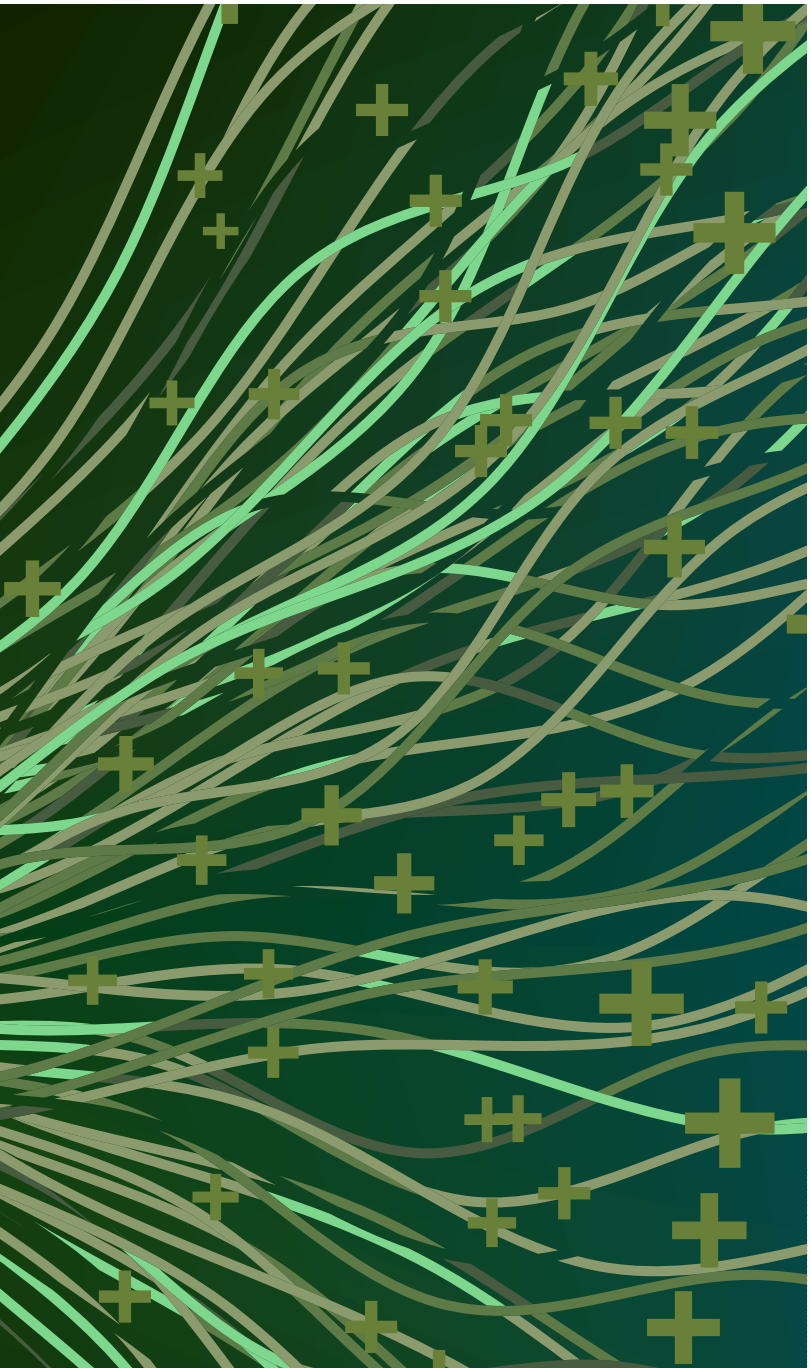
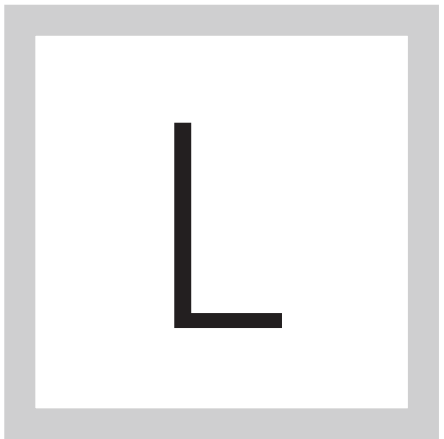


E-Guide

MANAGING ENDPOINTS WITH DEFENSE-IN-DEPTH

TechTarget | SearchSecurity



EARN HOW TO implement appropriate security controls for endpoint management.

MANAGING ENDPOINTS WITH DEFENSE-IN-DEPTH

Mike Rothman

Every day it seems you read about this zero-day attack, that botnet rising from the dead or another new, innovative attack targeting enterprise endpoints. Or all of the above. It makes even the most hardened security professional want to curl up into a fetal position and cry for his mommy. But sticking your head in the sand doesn't solve the problem, nor does it help us achieve our charter of protecting corporate information assets. I've had a number of conversations lately that ultimately ended with the realization that the organization can no longer trust its endpoints. This requires thinking about security in a fundamentally different manner.

I know the idea of giving up on securing the endpoint blows up how we've been taught to do things for years. What about the defense-in-depth security model? What about a layered security architecture? If you take a key layer out of the mix, where does that leave you? Actually, let me ask the question from different perspective: How are your current endpoint protections working for you? Yeah, I thought so. I also get that some of you don't have the option of giving

Home

Managing endpoints with defense-in-depth

up endpoint protections because auditors still require you to do the checklist fandango and make sure the AV box remains checked. So let me clarify: You probably still have to "protect" your endpoints, but you aren't expecting those controls to actually prevent an infection.

To be clear, a layered security architecture is still a good idea. If you are going to have a breach, at least make the attackers work for it. The point is to implement your layered security within the infrastructure you control, because you increasingly don't control the endpoints -- especially in today's world of bring your own device, or BYOD. Maybe it's a personally owned laptop belonging to a contractor brought in to rescue an off-the-rails development project. Maybe it's a business partner with access to your systems. Maybe it's your board members using their shiny new iPads to access corporate email. Regardless, you don't control those devices, and it's probably not worth the effort to mandate a certain type of device and then implement appropriate security controls.

It's easier to assume the endpoint is compromised, since if it isn't right now, it will be owned soon enough. Those pesky users keep clicking on stuff, and we all know how that ends. So, what to do? First, let's deal with the endpoint. I recommend you deem it a lost cause and reimage it. Today's malware doesn't

Home

Managing endpoints with defense-in-depth

really lend itself to being cleaned; don't even try. Start with a fresh operating system install and move on. Hopefully if good backup processes are in place, an affected user won't lose too much data.

Since we're assuming we can't trust endpoints, we need to protect things at the network layer, and that means network segmentation. A lot of network segmentation. You want your really sensitive information behind a "high wall," where anyone (or anything) accessing that data is strongly authenticated, and all transactions on the sensitive networks get monitored and applicable traffic captured. Again, these controls are not panaceas, but you want to make it hard to access your important stuff and even harder to exfiltrate it.

For the stuff that isn't that important, you can implement a less stringent set of controls. Maybe just making sure the devices connecting to your network are not steaming cesspools of malware upon connection. And you can look at what network connections devices make (by looking at applicable network flows) to ensure they aren't trying anything silly, like reconnaissance that could indicate an active attacker trying to do bad things.

It's interesting, but for all the people who shoveled dirt on the network access control (NAC) companies a few years ago, it turns out that technology is pretty applicable to deal with this concept of untrusted endpoints. You evaluate

Home

Managing endpoints with defense-in-depth

each endpoint upon connection and then, based on device type, security posture, authentication method and a variety of other policy triggers, decide what networks they can connect to.

Can a savvy attacker defeat segmentation and the way NAC appliances assign devices to specific network segments? Of course -- which is why it's important to also monitor your sensitive networks. Yes, that involves using a security information and event management, or SIEM, system that not only monitors and analyzes the events and configurations of the devices controlling your important data, but also likely does some full packet capture on the very sensitive segments. Why? Because you want to make sure you have sufficient data for a proper forensic investigation when you have an incident.

Remember, you can't entirely eliminate the risk of a breach. But you can make it harder on the attackers, and part of that may be treating your endpoints as the hostile devices they often turn out to be.

Mike Rothman is president and principal analyst of Security Incite, an industry analyst firm in Atlanta, and the author of The Pragmatic CSO: 12 Steps to Being a Security Master.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.