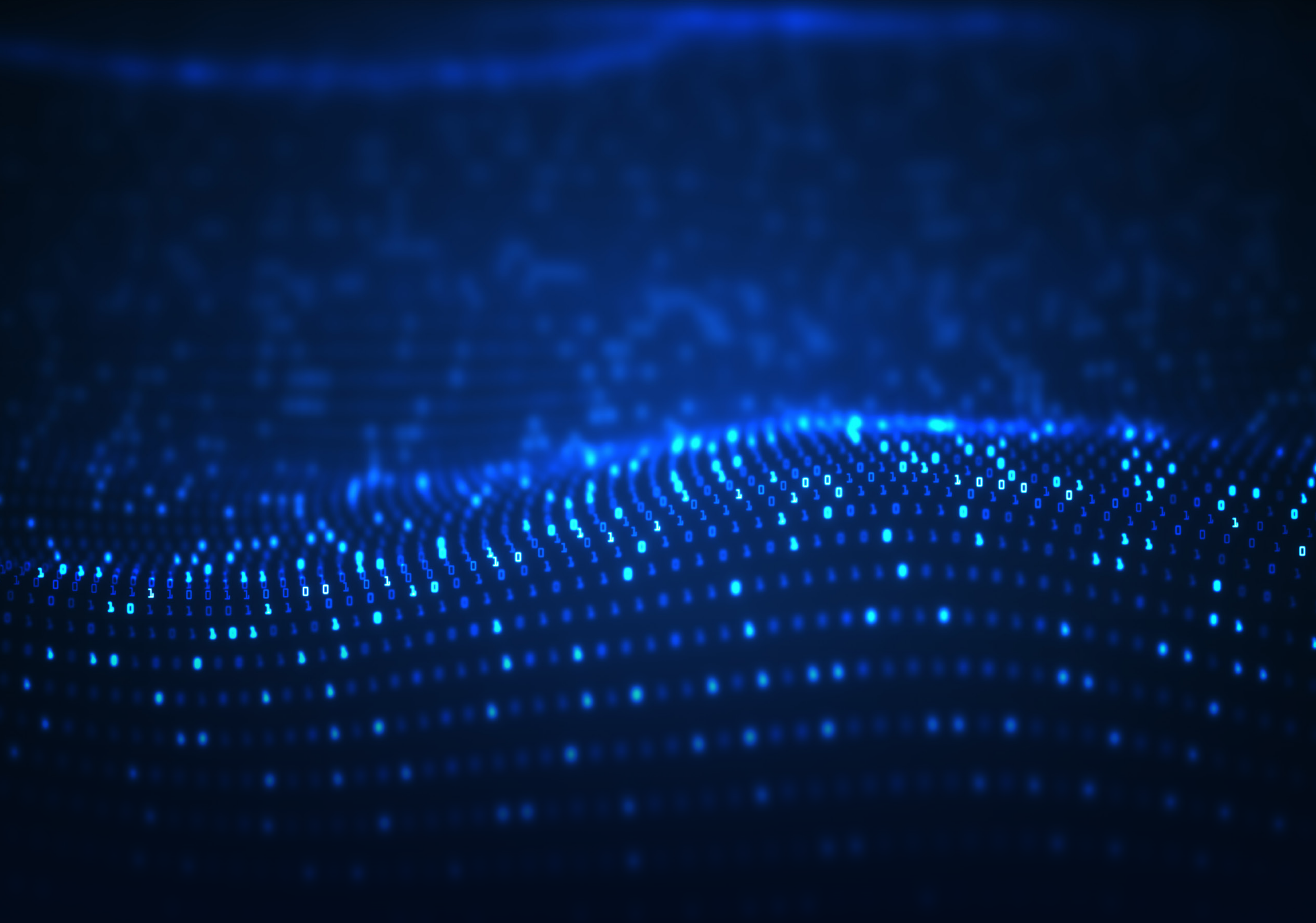
Red River

FOUR CRITICAL STEPS

TO ACHIEVING CLOUD SECURITY WITH MANAGED SERVICES



MSPs can help an organization achieve cloud security through strategic improvement. Moreover, they are an excellent business choice that enables companies to focus often-limited resources on what they do best. An MSP lets your business do your work while leaving cyber security to the experts.

When an organization doesn't have the resources — be it time, money or human resources — or the desire to make a change on their own, outside help is needed. MSPs have the technology and expertise needed to help an organization improve.

Red River recommends the following four steps for achieving cloud security with the help of an MSP partner.

STEP ONE: MANAGE ACCESS

The first step to securing an organization is to manage access. Potentially harmful access goes both ways; employees might accidentally visit malicious sites or download malicious software. Botnets could try to connect to the organization and initiate a DDoS attack.

Access can be controlled through:

- **Content filtering and Privileged Access Management.** Through the principle of Privileged Access Management (PAM), it's best if employees only have access to the content that's necessary for them to complete their work. Today, ads are everywhere, and these ads can contain potentially malicious files. Employees may accidentally access inappropriate things through the work network, especially if they are working from home and the boundaries between work and life have been blurred. To prevent employees from doing things like playing games on their accounts, content filtering and blocking is necessary.

- **Malware and phishing blocking.** Employees can accidentally download malware for numerous reasons. They may be trying to download faux software to complete a job, or they may have accidentally downloaded software that's similar to what they need. By blocking malicious programs automatically, employees can be protected. Likewise, employees can be notified of potential phishing attempts.

- **Protection against botnets.** Botnets are becoming a more serious problem now; even IoT devices like lightbulbs can be incorporated into a botnet. A botnet can severely slow down or damage a system or be turned against a system for a DDoS attack. Access needs to be controlled to protect against these types of systems.

- **URL typo correction.** Going to a different website (such as Goggle.com instead of Google.com) can be dangerous for an employee. Malicious attackers can camp "similar" domain names and try to get information from those who land there. URL typo correction can resolve this problem before it becomes a security risk.

Access control and management is a very important step toward obtaining better cloud security. The more access is secured, the better. However, most networks can't completely control their access, because employees are human and human error is, to a point, inevitable. This is what makes it necessary to use antivirus solutions, firewalls and other similar products.

STEP TWO: ENDPOINT PROTECTION

The number of endpoints the average network is being forced to protect is growing by the day. Today, companies have all sorts of user devices connected to a network – laptops, tablets, mobile phones, smart watches, TVs and so on – also known as endpoints. With employees increasingly working remotely, these endpoints are growing nearly exponentially. Once data is on a device, it's very difficult to control, so as much data as possible should be stored in the cloud rather than on user devices. Proper endpoint protection has to be robust, scalable and easy-to-use.

Modern endpoint protection consists of services that live on employee devices, making sure that these devices remain authenticated, encrypted and protected. These services are able to identify when an endpoint has been compromised, when malicious software may be able to transfer from the endpoint to the network and whether data itself has been fully protected. By engaging in next-generation endpoint protection, organizations can protect their own networks from potential intrusion.

Features of next-generation endpoint protection include:

- **Isolation.** Applications are able to be sandboxed in virtual servers, to prevent them from potentially executing malicious code, and to identify potentially malicious behaviors. The more applications are separated, the less likely it is that they could have an adverse impact on others.

- **Whitelisting.** Whitelisting is safer than blacklisting. Blacklisting involves a list of banned connections and applications. Whitelisting involves a list of allowed connections and applications, excluding all else.

- **Enterprise detection and response.** Next-generation machine learning algorithms are able to swiftly detect and respond to potential threats, using pattern recognition and samples that are programmed in. Over time, they get smarter and more accurate.

- **Exploit prevention.** Zero-day exploits, in particular, are very dangerous and very common; the second a new exploit is discovered, malicious attackers will attempt to use the exploit against anyone vulnerable. Next-generation endpoint protection can identify whether endpoints have been updated and protected against exploits, even denying them access until they have been secured and patched.

- **Antivirus modules.** Today's antivirus no longer relies on signatures from known malicious programs. Instead, they can identify brand new programs simply by their behavior. This makes them far more effective, as new malicious programs are coming out constantly.

Without endpoint protection, an organization's network can be compromised when an employee loses their phone, or when an employee downloads a virus on their laptop. Since cloud solutions are incredibly open and accessible, they are more likely to be accessed from a multitude of environments and services. Endpoint protection is what ensures that employees are connecting from non-compromised devices and that the data is safe to be transmitted.

Perhaps most importantly, next-generation endpoint protection can detect threats without human intervention. By automating the process, the organization can scale without using a tremendous amount of human and technical resources. With isolation, whitelisting, enterprise detection and response, exploit prevention and antivirus modules all working together, the system can be protected against most threats without having to escalate the situation to IT personnel – all in an automated, transparent way.

STEP THREE: END-USER AWARENESS

For nearly every organization, today, human network behavior continues to put an organization at risk. End-users can take actions that are unpredictable and risky, and they may not realize that they're doing it. For the most part, employees just want to get their job done. If IT security inhibits getting their work done, many employees will simply override the security if they are able to. They will self-service their own IT, change permissions and install software, as long as it gets the job done. And if end-users don't understand the risks involved, they are even more likely to do this.

It may not even be obvious to the users that they are doing something they shouldn't do. Phishing attempts are a notable issue. Employees will often believe emails when they receive them and will respond with whatever information is requested. A fake email from their own MSP could lead to them turning over their credentials, even if they could intellectually reason that their MSP would never need said credentials. People are human and make mistakes.

Thus, end-user awareness is one of the most important components to cloud security. Cloud systems will be connected to by devices from practically anywhere, making the system more vulnerable. Employees may connect with multiple devices, may leave these devices unlocked or may have their devices otherwise compromised. And they may not realize that this has happened, ultimately leading to everything on their system (and potentially their network) being compromised.

Awareness training moves in stages:

- **Annual and as-needed user training.** Users need to know what they need to avoid and what they can potentially expect first. To an untrained user, a phishing attempt looks like any other email. Untrained users may not realize they shouldn't install new applications, or they may not understand why they aren't allowed to share login information. But training can't be done just a single time, either. While training should be done when users are onboarded, training should also be refreshed at intervals and should cover the newest threats.

- **Phishing (and other attack) simulations.** Simulated malware attacks and phishing attempts are some of the best, most effective ways to see what employees will actually do when they're confronted by security threats. Phishing simulations do two things. First, they give employees practice at identifying and responding to phishing attempts. This will empower employees to do the right thing when a real attempt occurs. Second, they help identify the employees who could be most vulnerable to a phishing attempt. No one should be excluded. Not only should employees be tested, but also supervisors, managers and the C-suite. Often, it can be the C-suite who is most vulnerable, because they may not have attended the same training.

- **User and Entity Behavior Analytics (UEBA).** It is important that these trainings be tied to a metric so that their effectiveness (or lack thereof) can be measured. Once the simulations have been run, a thorough analysis and report using UEBA, or User and Entity Behavior Analytics. This will enable you to measure effectiveness of training and identify persistent violators of best practices so that they can be trained again.

In many ways, end-user vulnerabilities are the hardest to defend against. This is because there's no way manage how end users act every time; people are going to make mistakes. To protect an organization against intrusion, the best thing to do is to train employees and lock down the system to reduce the chances that they can make mistakes altogether. While people can be a security issue, the issue itself has to be countered through tech.

STEP FOUR: ZERO TRUST ARCHITECTURE FOR COMPLETE PROTECTION

Networks are growing in complexity, and as they grow, so too changes the mindset of how to best defend them. Initial cybersecurity philosophies revolved around protecting the perimeter, but these older philosophies did little to defend against malicious actors that had already breached said perimeter. A "perimeter protection" mindset is like a moat around a castle: It may be effective at keeping bad actors out, but once someone has breached that sole line of protection, there's no internal protection, leaving them free to cause potentially criminal mischief.

One option to better protect your networks is to have multiple layers of protection – think of it as concentric castle moats and walls – but the most cutting-edge cybersecurity philosophy is that of Zero Trust Architecture, or ZTA.

In ZTA, every interaction must be verified in some way, no matter if it's outside the "castle walls" or within. A Zero Trust infrastructure requires verification for individual profiles, applications, workflows, and sessions – every single time. There's a "moat" around every single interaction on the network.

In a video call between two people, for instance, both accounts – and the identity of those logged into them – are verified. The machines they're logged into are verified. When the application starts up, it is verified on both ends. If any one of these six variables is not correctly verified, the conversation does not occur.

This may sound like unnecessary jumping through hoops or "speed bumps" in the road, but a true Zero Trust Architecture deployment will make all these verifications in the back end. Many, if not most organizations are already on their Zero Trust journey with the apps they use every day, and you might not know it. Zero Trust has become a natural part of business enterprise modernization programs.

Even with better end-user awareness, employees are always going to have some level of vulnerability. They may try to download software that isn't properly signed, or they may visit websites that are either harmful or inappropriate. Through Zero Trust Architecture, the organization is able to protect against malicious actors and ensure the network and employees are both as secure as possible.

Advanced, next-generation protection like Zero Trust Architecture doesn't have to deny all connectivity, because it is better able to determine whether an activity is malicious or not. With a next-generation firewall and machine-learning technology, the system will be able to better determine over time whether an interaction is unusual for the network and whether it must be blocked. These next-generation solutions are able to identify malicious programs and connections even if they have never been seen before.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.