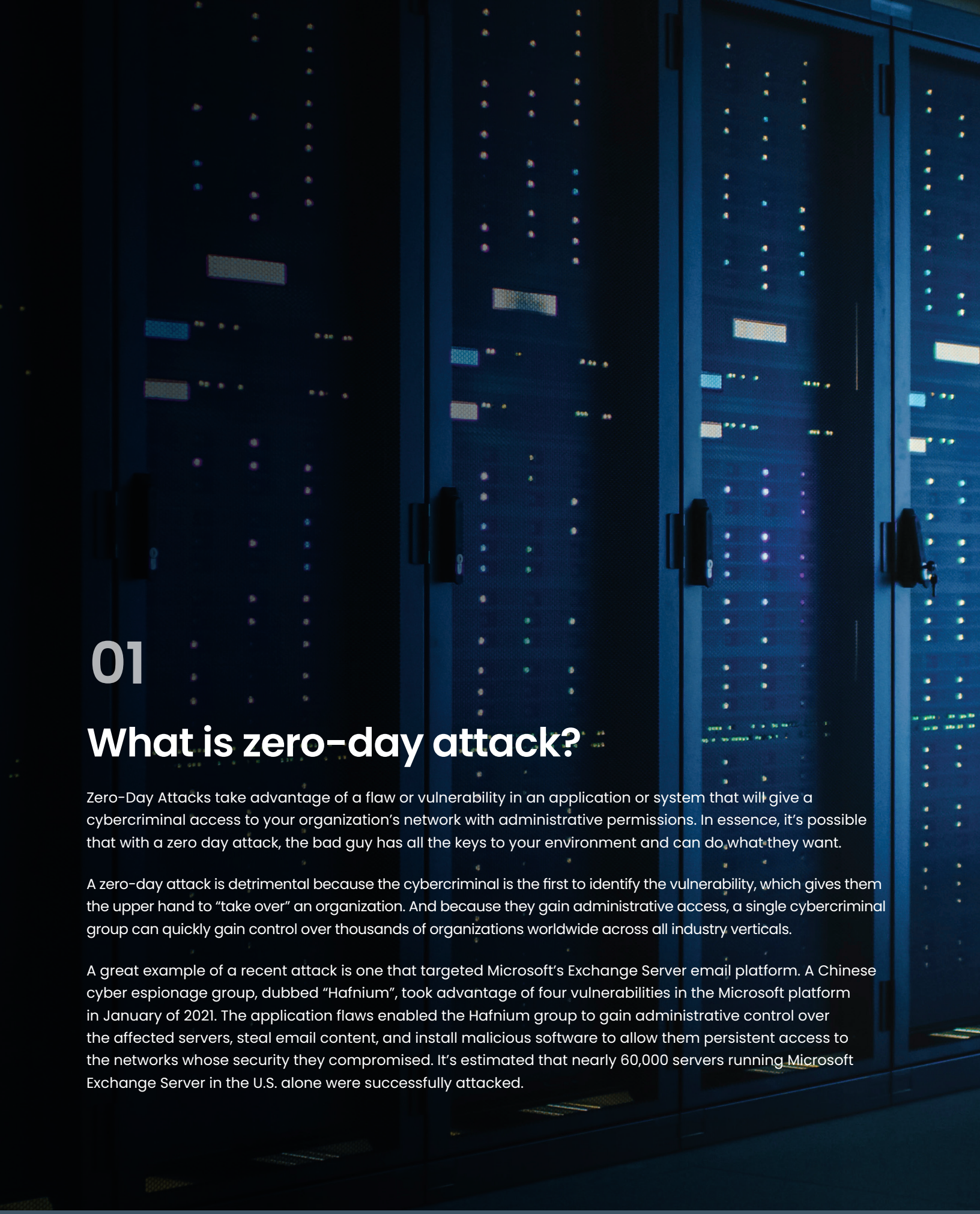
Logically™

CYBER FIRST. FUTURE READY.

Whitepaper

Protecting Against Zero-Day Attacks with Managed Security Solutions.

A Logically Whitepaper designed to help organizations understand the risk and impact of “zero-day” cyberattacks, and why they should consider outsourcing to a Managed Security Solution Provider (MSSP) to address their cybersecurity protection needs.



01

What is zero-day attack?

Zero-Day Attacks take advantage of a flaw or vulnerability in an application or system that will give a cybercriminal access to your organization's network with administrative permissions. In essence, it's possible that with a zero day attack, the bad guy has all the keys to your environment and can do what they want.

A zero-day attack is detrimental because the cybercriminal is the first to identify the vulnerability, which gives them the upper hand to "take over" an organization. And because they gain administrative access, a single cybercriminal group can quickly gain control over thousands of organizations worldwide across all industry verticals.

A great example of a recent attack is one that targeted Microsoft's Exchange Server email platform. A Chinese cyber espionage group, dubbed "Hafnium", took advantage of four vulnerabilities in the Microsoft platform in January of 2021. The application flaws enabled the Hafnium group to gain administrative control over the affected servers, steal email content, and install malicious software to allow them persistent access to the networks whose security they compromised. It's estimated that nearly 60,000 servers running Microsoft Exchange Server in the U.S. alone were successfully attacked.

So, what does this have to do with your organization? In a word, plenty.

In this paper, we'll take a look at zero-day attacks, who they affect, and what their impact is. We'll also offer some practical steps necessary to attempt to stop these attacks before they start, as well as remediate the situation should an attack be successful. We'll also spend some time focusing in on how outsourcing the work of securing your environment from zero-day Attacks may improve your organization's security stance while minimizing the expense of doing so.

The very concept may seem a little sensationalized and feel a bit like it's all fear, uncertainty, and doubt (better known as FUD). But the reality is zero day attacks represent one of the greatest threats to your business' very existence. There are a few reasons why every business needs to care about zero-day attacks:

They happen (more than you think)

At the time of writing this paper, there were more than 1,000 published zero day vulnerabilities documented in 2021. Some were found in products you know all too well - Windows, MacOS, Firefox, Chrome, and Internet Explorer - while others are in applications and services that only IT may be privy to. Each one of these represents a potential entry point for a cybercriminal to gain access to and control over some part of your organization's network.

It can (and will) happen to any organization

For some reason, there is still this lingering misconception that attacks only happen to large companies. But that simply isn't true. The cybercriminal world includes those who see a certain size organization, or industry vertical, untouched by the general cybercriminal masses. And so, they target those businesses. In other cases - like Hafnium - it's an opportunistic attack where the bad guys perform an automated scan of hundreds of thousands of IP addresses on the Internet. They look for those connected systems that respond in the desired way, indicating a potential victim organization. Hafnium doesn't care about the specifics of your company; if they are focused on enterprise healthcare organizations as their preferred target, they can easily sell the access they've achieved to another cybercriminal on the Dark Web.

They're dangerous

The Hafnium attack is the perfect example. Once attackers gained access to victim organizations, the security researchers that discovered the attack noted that they witnessed actions that included:

I. Creating of user accounts (so the bad guys can continue to access the victim environment even after their misuse of one account is discovered);

II. Dumping user accounts and passwords (that can be sold to those wanting to send out phishing attacks impersonating a legitimate user);

III. Stealing data that may include intellectual property, confidential information, personnel details, financial records; and moving within the network freely without detection.

They occur when you least expect it

Zero-day attacks can occur at any time, leaving organizations and their IT teams vulnerable. Unlike most other attack types, zero days aren't easily predicted or expected. Attackers are aware of this, which is why they'll often strike after hours when your security team isn't around to monitor for suspicious activities.

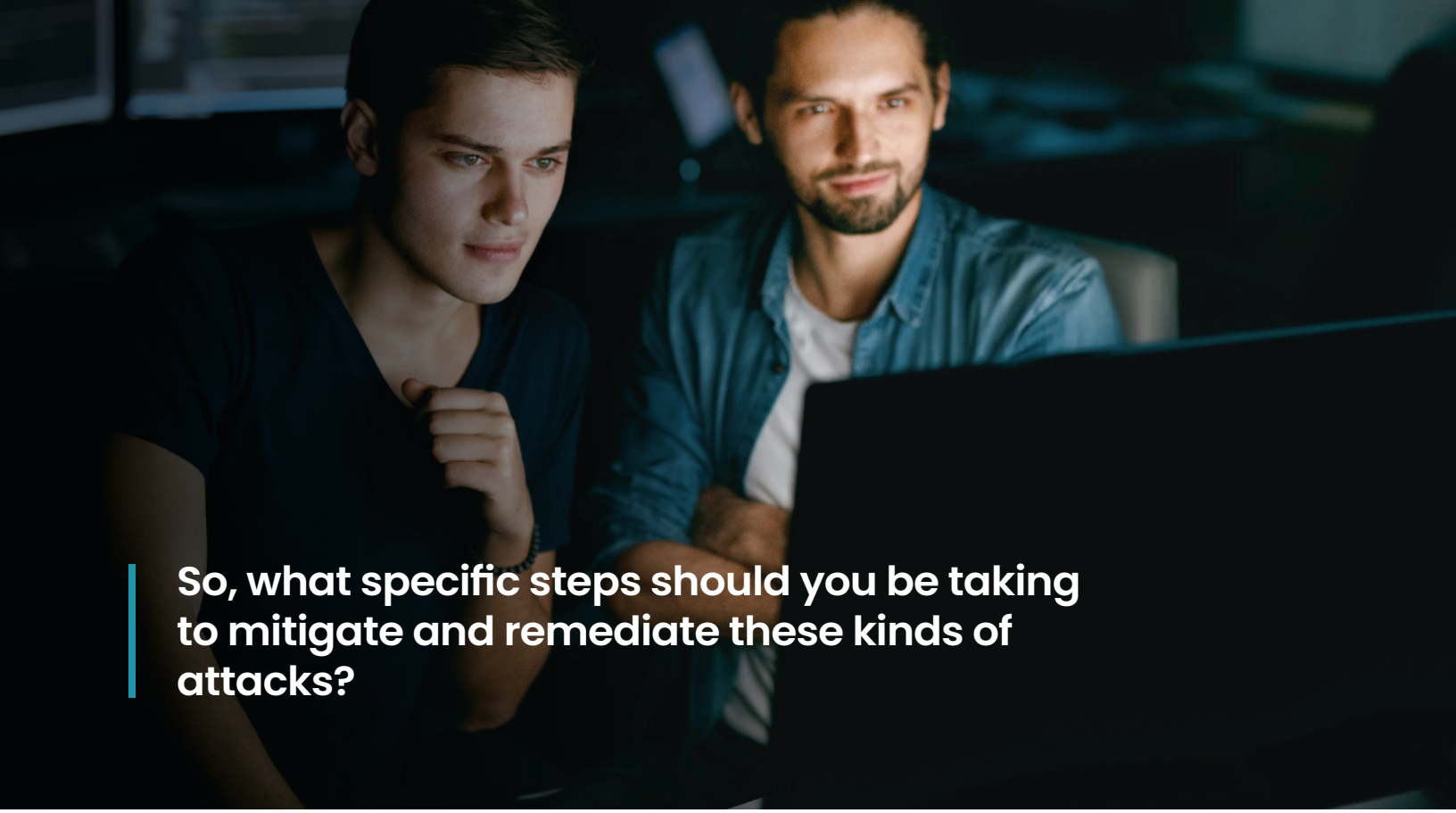
A security update may not be available for months

You're probably familiar with operating system and application updates that are regularly pushed out by software vendors. So it may seem reasonable to expect that, should a zero-day attack occur, an update will be out shortly. But that's simply not the case. With attacks like the previously mentioned Hafnium attack, it takes time to determine exactly what actions were taken, what flaws exist within the affected software vendor's code, how they can be fixed, and properly test to see if the fixes may negatively impact any other part of the product requiring an update.

In the case of Hafnium, the initial detection was in January of 2021 and Microsoft was not able to release updates and mitigation steps for the security team to put in place until March. In essence, every organization vulnerable to the software flaw were sitting ducks for two months.

Responding quickly to these kinds of attacks is critical

It may seem like your hands are tied when struck by a zero-day attack - but that's not the case. One critical step that your cyber and/or IT team can take is to quickly learn any insights from the attack to understand the situation better so that proper steps can be taken. For instance, your team might want to release new updates or use compensating measures to increase the state security around the affected application (more on this later).



So, what specific steps should you be taking to mitigate and remediate these kinds of attacks?

02 Protecting Against and Responding to a Zero-Day Attack

There are steps every organization can take both before and after they experience a zero-day attack. First, begin with some high-level preventative measures you can take.

01. Keep Systems Updated

At a minimum, we're talking about performing updates on every device, system, service, and application on your network. But the best approach to protect against zero-day attacks is by assessing your environment for vulnerabilities which would allow your team to develop a remediation plan to increase monitoring of the identified system or application. This would considerably reduce your risk of being exploited.

02. Have a layered protective security strategy in place

There's no silver bullet when it comes to security posture. A proper "defense-in-depth" security strategy involves protecting a number of aspects of your environment, including your network's perimeter (where data, traffic, email, and communications go in and out of the environment), your endpoints (this includes laptops, desktops, tables, etc.), users (even users can be taught to practice better cyber hygiene), and account credentials (to ensure the user of a credential is actually its' owner). The next step, while proactive in nature, is more about attempting to detect an attack rather than prevent it from happening.

03. Monitor for threats

Attackers need to move within the victim's network and can't help but trigger indicators of compromise (such as logging on at 3 a.m. on a Saturday or copying massive amounts of data out of the network). Monitoring your network and the systems, services, and applications that run on it continually for abnormal behavior is one of the main ways you can identify any post-zero day attack activity on your network. Lastly, it's important to have a plan in place of how you will respond to an attack.

04. Identify the scope of an attack

Understanding which systems and applications have been impacted or compromised is key to a swift response. This can include your directory service, cloud-based and on-premises resources, user endpoints, security permissions assigned, and more.

05. See if any mitigation steps or updates are available

In some cases, while there may not be a security update, there may be manual steps available publicly that can be taken to remedy the vulnerability temporarily.

06. Identify and close the initial point of entry

Stopping the attacker from being able to enter your environment is the first step to getting back to an operational and known secure state.

07. Remediate any changes

If you've been made a victim, it's very likely the attacker has moved about your entire network, making changes to provide them with persistent access to get in, as well as elevated permissions to enable them access any of your applications and data they like. Recovering and/or rebuilding the environment back to a state prior to the attack will be your next step.

To accomplish all this, there are a number of requirements around hardware, software, staffing, expertise, and experience that may not be readily available to an organization. You may think you would be able to implement all the preventative measures, but when it comes to continuous monitoring and knowing how to respond to a wide range of possible attack scenarios, you're looking at something that closely resembles a Security Operations Center (SOC) with multiple security professionals.

This is where it makes sense to consider using a Managed Security Solution Provider partner to provide these services.

03 Outsourcing Cybersecurity to a Managed Security Solution Provider

Cybercriminals today are experts in their craft, working daily to improve the effectiveness of their attacks. So, it's important that your organization be able to maintain a strong defense and an even stronger response should an attack be successful. Outsourcing this aspect of operations to a Managed Security Solution Provider (MSSP) is a viable choice for a number of reasons:

Your Staff is Limited (in more ways than one)

Most IT organizations struggle with bandwidth and limited cybersecurity expertise. Because your internal team is already occupied with day-to-day tasks to keep the business operational, cybersecurity can be a mammoth task due to its complexity. Managed Security Solution Providers have dedicated staff with years of cybersecurity experience that can augment your internal team to provide as much or as little hands-on assistance as is needed.

Cybersecurity is Not Your Expertise

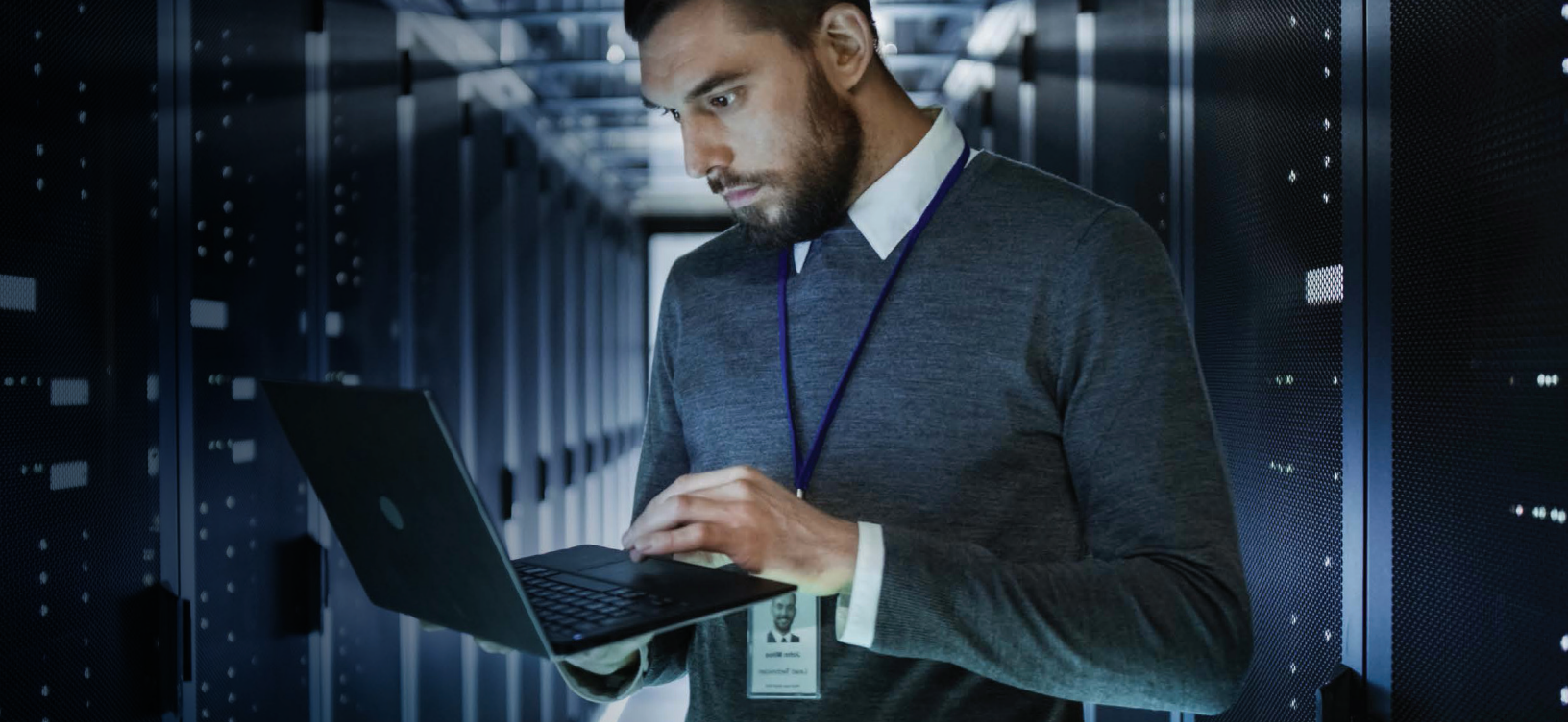
Cybersecurity is more than installing and configuring some security solutions in your environment. And responding to a cybersecurity incident is much more than just restoring affected systems. You need expertise that can help you establish an effective and dynamic defense based on current attack tactics, as well as already know what to do should you become the next victim of a cyberattack. Cybersecurity is everchanging and it's understandable if your internal team can't keep up with the latest cyberattacks especially when security isn't their forte. National Managed Security Solution Providers bring years of expertise securing customers of every size and industry, making the propping up of a solid cybersecurity stance much easier and effectual.

Your Budget is Limited

Even if you wanted to hire a Security team and start your own SOC, the investment required is significant. Rising salary costs paired with challenges in finding and retaining talent make it difficult to implement. Additionally, the required hardware and software just to have your SOC see the light of day means a heavy upfront capex investment. MSSPs offer a simple monthly opex cost that includes the experts, established process and the latest technology.

You Don't Have Time

Cyberattacks (including zero-day) occur daily. It would take literally months to setup a SOC. MSSPs can get your cybersecurity stance improved in a matter of weeks, helping better protect your organization now, not months from now.



04 What to look for in an MSSP?

Cybersecurity is no joke, so it's important that you be realistic about your internal capabilities and realize the value outsourcing to an MSSP can bring to the organization. If you are ready to make that leap, the last part of the process is to identify an MSSP that deliver on what they promise. Additionally, plenty of Managed Service Providers (MSPs) will tout that they provide cybersecurity service offerings adding to noise in the market.

The right cybersecurity offering (and, therefore, the right Solution Provider) should be comprehensive in nature; someone pitching "antivirus on your endpoints and patching" is only scratching the surface and won't be truly protecting your organization. When looking for an Solution Provider, their offering should include the following services to best prevent, detect, and respond to both zero-day and everyday cyberattacks:

Risk Assessments

While there are common best practices that can and should be implemented, your organization is unique. The right Solution Provider will perform a risk assessment of your business, looking at the security measures you have in place, both on-premises and in the cloud. It also includes a review of your supply chain for security weaknesses to provide a holistic picture of your security status and what can be improved.

Vulnerability Assessments

Proactive assessments of both your internal IT infrastructure and externally-facing parts of your network are important so that weaknesses can be found and addressed before attackers take advantage of them.

Layered Security Management

Many parts of your environment pose a risk, requiring a layered approach - these layers of protection range from DNS filtering against online threats to security awareness training. With the right security measures in place between the attacker and the vulnerable system or application makes it difficult for them to succeed. An experienced managed security solution provider can offer comprehensive security packages enabling small and midsize organizations to access best-in-class security solutions cost-effectively.

SIEM-SOC Monitoring

To be sure of any cyberattack having even the slightest measure of success within your organization, it is necessary to have a team of dedicated security analysts monitoring your network 24/7. Should something suspicious occur, they'll be the first to know and investigate accordingly.

The Security Information and Event Management (SIEM) solution provides a proactive approach to event monitoring with real-time alerts, trend analysis, and threat intelligence. With a SIEM-SOC solution, organizations don't need to spend most of their time and resources monitoring and reviewing event logs to identify and respond to security incidents.

Whether we're talking about the presence of ransomware, malware that allows attackers remote access, or indicators of compromise such as lateral movement between systems or the creation of accounts, the earlier these can be detected, the less impact an attack will have on your business.

Incident Response

Should your organization experience an attack, ideally, you'd want someone experienced at the helm of the response efforts. Solution Providers offering cybersecurity services have detailed incident response plans that ensure mitigation and remediation are swift and effective, no matter the type of attack. And, should you experience a zero-day attack, they can put mitigation measures in place to minimize the impact - even if no security update is available.

Choosing to Outsource Cybersecurity

Offense is the best defense, and this applies to cybersecurity. Businesses must anticipate an attack because a wait-and-see approach will never work in this day and age when cyberattacks are on the rise.

But this only happens if you have a proper defense and a team continually monitoring for potential threats.

By outsourcing your cybersecurity efforts to an Managed Security Solution Provider, you'll gain access to a team of seasoned experts that know the ins and outs of all things cybersecurity, the latest technology to combat attacks, and cutting-edge layered security that comprehensively seeks to prevent attacks.

Leveraging the right Solution Provider will help to ensure your organization is as secure as possible, knowing you have a team of experts on standby should the worst happen. And all this is accomplished affordably, driving down the cost of preventing your organization from becoming the next victim of a cyberattack.

Looking for the right MSSP to fortify your organization's security network? Talk to our team of experts - they can help!

Solidify your business' network now! ›

Logically™

About Logically

Logically is a leading national managed security and IT solution provider that helps organizations secure and support their businesses today, solve for tomorrow, and strategize for the future with cyber-first solutions. Our team of experts, including cybersecurity, engineering, networking, and cloud specialists, collaborate with customers to implement solutions that protect their assets, reduce risk, and optimize performance, end to end. Since 1999, we have made long-term relationships, customer service excellence, and purposeful innovation guiding principles to ensure customers have a trusted advisor at their side, helping them focus on their business, not the technology behind it.

From strategic planning and design to implementation and ongoing management, Logically takes a cyber-first approach from end to edge to cloud:

- Cybersecurity
- Compliance
- Data Center
- Cloud
- Network
- Collaboration

Visit www. logically.com to learn more.