Acronis

How to meet the challenge of zero-day threats

Zero day. Words that strike fear into the heart of any security practitioner.

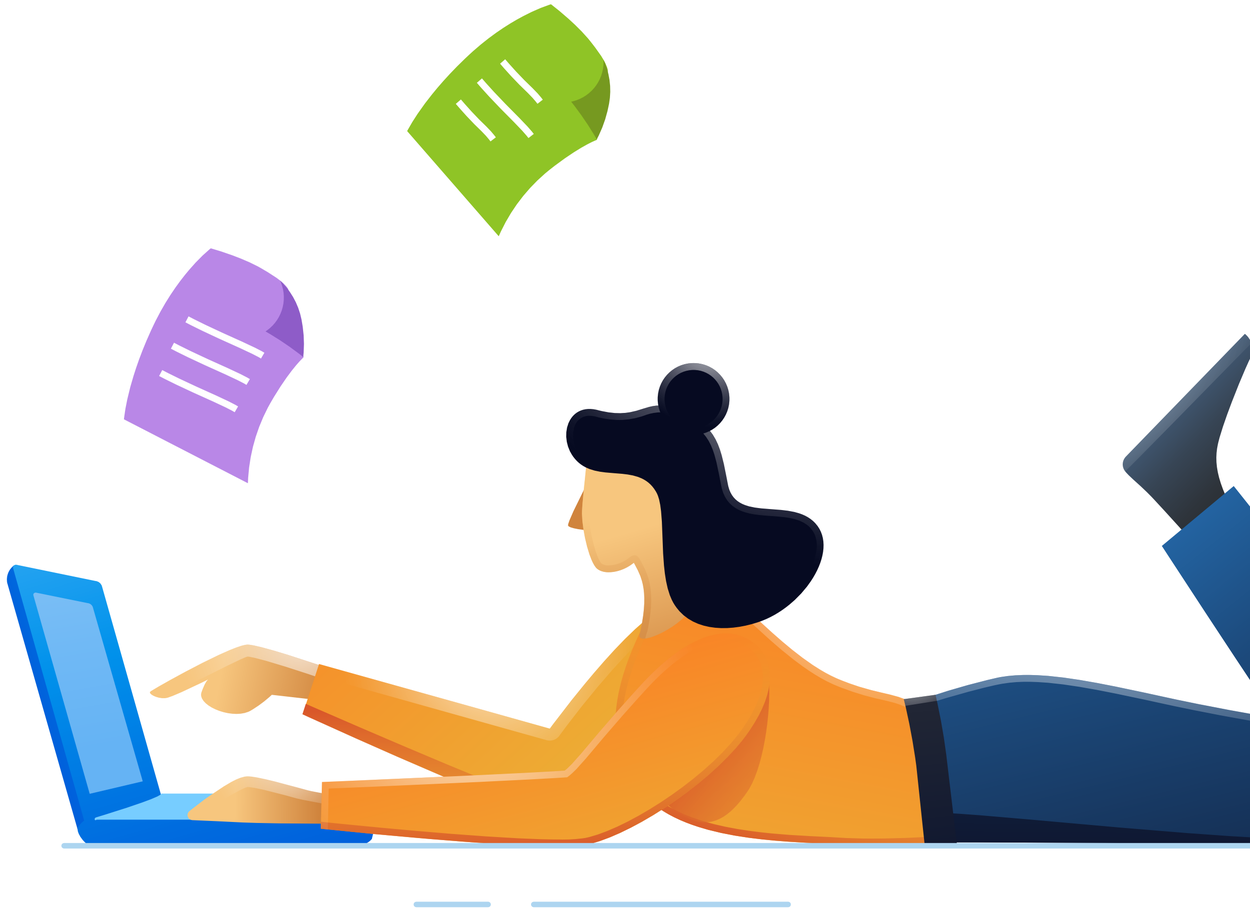
Just as it sounds, zero-day vulnerabilities give the vendor zero days to react: Once these vulnerabilities are discovered, an attacker can exploit them before the vendor has a chance to remediate. Within this window, attackers can exploit the newly-discovered vulnerability, either before vendors are able to create a patch or after a patch is released, but before IT teams can roll it out.

What this means for you as a managed service provider is clear: Unless you can stay ahead of attackers, you and your clients are at risk.

The massive growth of the MSP industry in the last five years (and especially the last two years, as organizations have scrambled to outsource their IT in the wake of COVID-19) has painted a target on your back. High-profile attacks such as Kaseya, SolarWinds, and Operation Cloud Hopper make it clear that cybercriminals and larger threat actors, such as advanced persistent threat groups (APTs), are out there looking for you.

Today, attackers are savvier than ever, and the number of zero-day exploits is accelerating. If you're prepared, you'll be better able to minimize the risk of a zero-day attack and boost your organization's resilience against possible attacks. As an MSP in a very competitive market, the best way to hold on to your clients is to offer them comprehensive cybersecurity options around zero-day vulnerabilities.

This white paper will look at why zero-day vulnerabilities present such a challenge to all organizations, but to MSPs in particular. It will also review some of the ways you can better protect your clients — and your reputation.



Why you need a new approach

In a zero-day attack, attackers generally choose one of two strike approaches:

- Broadly and quickly (very, very quickly), hoping to have a major impact before vendors can react.
- Quietly, stealthily, and closely targeted — thus increasing the chance that the vulnerability won't be readily discovered.

In the first category are the "smash and grab" type threats: Attackers prey on the most ubiquitous hardware and software combinations because they're easy to find and exploit. They may target ubiquitous attack vectors, including browsers and email, across popular OSs and apps.

Attacks in the second category aren't always so obvious, and can be far more difficult to detect. This second-strike approach is commonly seen with APTs, which typically rely on long dwell times, making use of lateral movement once inside the victim's network.

To better understand how to respond to zero-day vulnerabilities, it can help to understand what they are, how attackers think and operate, and the ways the landscape has changed over the last couple of years.

The changing zero-day landscape

While zero-day attacks are not a new phenomenon, things have changed over the last few years.

First, the frequency of zero-day attacks is increasing. According to a Ponemon report, 80% of successful breaches are caused by new or unknown zero-day attacks, with that number expected to keep on growing over the coming years.

However, identifying a vulnerability is not the same as remediating it. In fact, today's zero-day vulnerabilities present an even greater challenge to cybersecurity teams because of another phenomenon: the collapsing vendor response timeline.

The minute an exploit for a vulnerability is publicized, the clock starts ticking. Every system that has that vulnerability is potentially open to attack, sending vendors scrambling to release a patch. While vendors are serious about taking responsibility and providing updates as needed, the truth is that many zero-day exploits today become public before the CVE is published, and before a patch is available. In fact, with today's tightening timelines, a zero-day exploit often occurs even before the CVE is assigned, while the CVE is often published very close to the release of a patch. This leaves a significant gap during which your systems may be vulnerable.

In the face of this vulnerability onslaught, while vendors are generally responsible and release patches quite quickly, in practice, the actual time it takes to implement the patch on user endpoints can vary widely.

This is due to the complexity involved: Most IT teams don't know what software versions they have installed where, or that there is a new version available. And if they are aware of the new version, they may not be aware of which systems it applies to. Many organizations simply lack a comprehensive way to track this information and keep up with the deluge of patches.

Once an exploit is disclosed and the clock starts ticking, every single system with that vulnerability is in the crosshairs. And the complexity of patch rollouts — especially unscheduled patches — helps explain why 42% of exploiting actually takes place after the vendor has released a patch. The solution is out there, but implementing it nimbly is beyond these IT teams' capabilities.

The main reason attackers can keep on exploiting vulnerabilities months or even years after patches are released is because time needed for remediation is still too long.

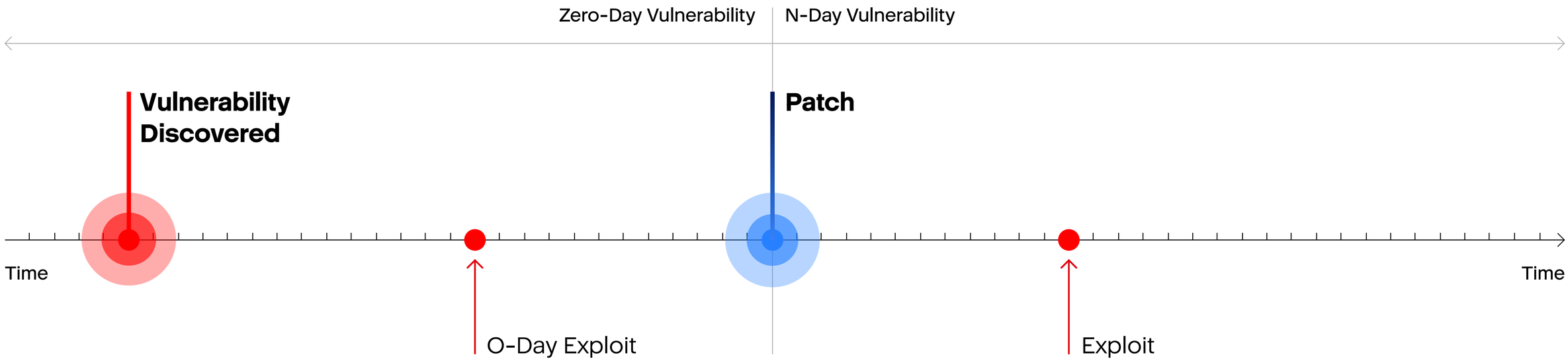


Figure 1: Zero-day timeline showing the gap between vulnerability discovery and patch release.

Why MSPs must prioritize zero-day vulnerabilities

Increasingly, MSPs are considered low-hanging fruit for cybercriminals. MSPs offer large, homogeneous attack surfaces, making them easy to reach and exploit. For example, all machines belonging to a single client, or even multiple clients, are managed centrally and may reflect the same OS version, patch level, etc.

This is what happened in December 2021's ManageEngine Desktop remote code execution attack, just the latest in a series of exploits of vulnerabilities in the ManageEngine suite. While an update was made available almost immediately, exploits were still being tracked in the wild — including by advanced persistent threat groups (APTs) weeks later.

The ManageEngine attack is unfortunately not unique; 2021 has been a year of ramped-up attacks on MSPs, such as July 2021's REvil attack on Kaseya's IT management platform, which led to business disruption for 1,500 companies and which combined an MSP-focused attack with a supply chain attack.

Attacks targeting MSPs are nothing new — back in 2019, ConnectWise, a Florida-based vendor of IT management software for MSPs, announced that several of its partners had been targeted through its remote-management systems. Clients of one MSP using ConnectWise included 22 towns and cities in Texas that were locked out of their own systems for $2.5M in ransom. But as companies shift core IT functions to MSPs, it seems clear that going forward, these attacks are going to increase significantly.

This means it's more important than ever for you, as an MSP, to use trusted tools to protect your clients and their end users.

To be a part of the solution for your clients, you need to start rolling out patches the minute the patches are released.

To increase clients' baseline protection, you must provide constant vulnerability scanning and keep clients up to date with the latest patches. But since there isn't always a patch available, you need to integrate patching with a variety of other solutions to provide more comprehensive coverage against zero-day attacks.

Zero-day protection: An MSP overview

While no single technology is going to offer enough protection against the kind of threats discussed here so far, MSPs can provide a greater degree of security using a combination of cyber protection services specifically focused on avoiding or mitigating the effects of zero-day attacks.

Firewall and URL filtering

The basic functions of a firewall are well established:

- Filter and verify network traffic, and monitor for suspicious behavior
- Close vulnerable ports and block unauthorized traffic

Modern networks should also implement web application firewalls (WAF), which offer protection against top web application security risks as identified by the Open Web Application Security Project (OWASP) — such as SQL injection, cross-site scripting, unauthorized resource access, and remote file inclusion. WAF analyzes the communication content to and from a web service, monitoring for vulnerabilities.

Extending the traditional firewall model are newer models like intrusion detection systems (IDS), which monitor and flag suspicious packets based on their contents, as well as intrusion prevention systems (IPS), which operate similarly but also block these packets. IPS monitors the network for suspicious activity, usually based on known signatures. Generally, these functions complement each other to provide tighter security.

Firewalls provide a vital defense system, particularly with the addition of layers such as URL filtering, which blocks access to known malicious sites, stopping malware in its tracks.

Effect against zero-day attacks

Although the popular perception is that they are not ideal to anticipate and defend against zero-day (or unknown) attacks, in fact they're a vital part of an organization's overall security preparedness. For instance, by blocking unnecessary ports and traffic, as well as through other features such as URL filtering, WAF, and IPS, firewalls can be a crucial first line of defense.

Zero trust with multifactor authentication

The zero trust network architecture model is a security framework built on the guiding principle that even if attackers are able to access your network, lateral movement and data loss should be limited.

According to Forrester analysts, zero trust is built around three core principles:

- All networks are untrusted
- Least privileged access must be enforced
- Assume breach; inspect and monitor everything

By segmenting off mission-critical information within your environment, the "blast zone" is limited in the event of an attack. With zero trust, a user or process with authorization to access one type of information is not necessarily given access to other types of information. Instead, all access is granted with an eye to the minimum privilege level needed to perform essential business functions.

Zero trust also relies heavily on multifactor authentication, which provides tighter security than just a single password.

Effect against zero-day attacks

While, as Forrester points out in their report, zero trust does not mean zero breaches, having this framework in place can work effectively to keep the impact of a breach to the barest possible minimum; for instance, by limiting lateral movement and restricting authorization to access data or run executables.

Secure development environment

Whether or not you're in the software business, software development has probably become a core part of your business. McKinsey estimates that more than half of the world's 20 million software engineers are working outside of technology industries in fields such as retail, financial services, manufacturing, and more.

This also increases risk because development teams working outside of the tech industry may not be familiar with industry best practices set by organizations like OWASP. Creating a secure development environment begins with ensuring that the entire development team is familiar with these best practices.

OWASP also provides guidance for developers to avoid the top ten most dangerous software weaknesses.

These best practices include:

- Adopt a security mentality across the entire software development life cycle (SDLC), from initial design and architecture all the way to production
- Encrypt sensitive data both in transit and at rest
- Verify compliance with explicitly defined security standards as part of routine QA
- Select data centers that meet high independent security standards, such as ISO/IEC27001, and are geographically and physically secure
- Segregate networks within data centers to limit exposure of service backends like database and storage
- Implement secure backup processes with routine verification and audits, including activity logs
- Ensure policies are in place for the secure destruction of sensitive data once it's no longer needed

Backup and disaster recovery

Having a system in place for backup and recovery provides essential protection against a wide range of catastrophes, both accidental (data deletion, hardware failure) and intentional, which includes data loss from a malware attack. A comprehensive backup strategy should include:

- Periodic backups, both full and incremental
- Multiple types of backup mediums (physical, cloud) as needed
- Regular testing to ensure the ability to fully recover as quickly as possible

In reality, backups are often performed at very long intervals even though best practices — along with a number of regulatory frameworks — may dictate a particular backup frequency. Many risk mitigation professionals suggest a restore drill and full testing of your disaster recovery environment on a semi-annual or quarterly basis.

Finally, even the best backup program is useless if you can't recover data quickly — particularly when you're working under less than optimal circumstances. Yet recovery steps are too often not tested, or it's difficult (or impossible) to recover to other hardware environments.

Effect against zero-day attacks

Securing data with a comprehensive backup strategy is a basic step that is surprisingly often neglected. With an effective backup program in place that takes a standard 3-2-1 approach (3 copies of data on 2 different media including 1 copy in a different physical location), client organizations have peace of mind knowing that their vital business data is secure — and avoid steep ransom payments to recover data that's been hijacked, corrupted, or encrypted in an attack.

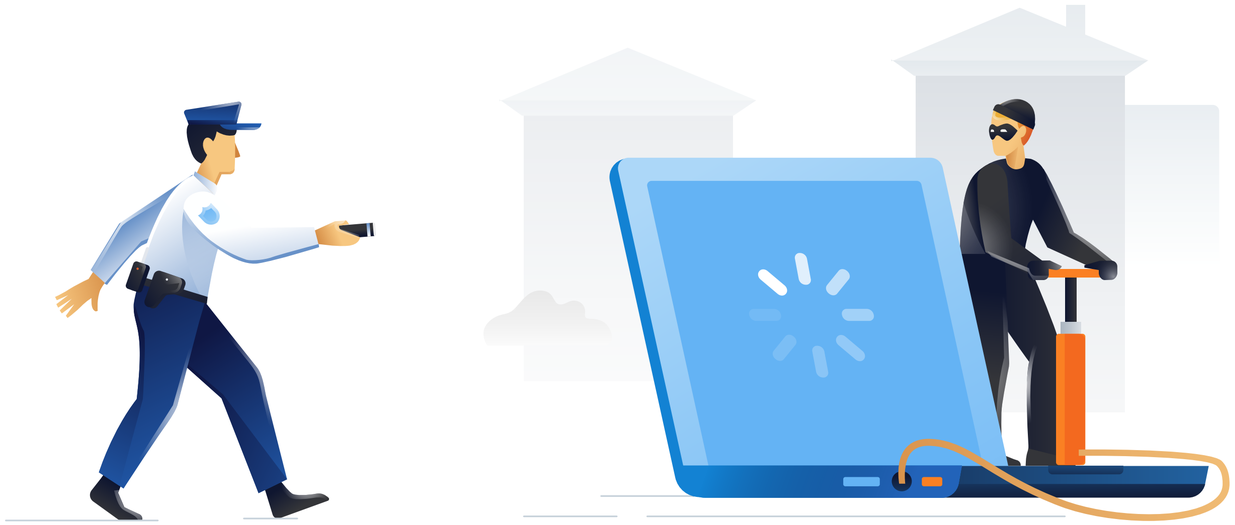
Other safety measures

Beyond the standard cyber protection services mentioned previously, MSPs are also starting to offer their clients more advanced offerings, including:

- **Exploit prevention:** Microsoft and other vendors may provide their own solutions aimed at mitigating the effects of vulnerability exploitation and stopping the spread of malware. Implementing these solutions will vary from vendor to vendor.
- **Behavior-based detection:** These solutions integrate machine learning (ML) to analyze complex heuristics and flag events based on statistics; while they may take some effort to configure and train, they can expand security capabilities considerably.
- **Endpoint detection and response (EDR):** Many of these tools are agent-based, but can be a useful complement for responding to advanced attacks and remediating breaches.
- **Next-generation dynamic scanning:** By identifying deviations from normal program execution flow at runtime, these solutions go beyond either signatures or heuristics to defend against malware threats commonly seen in malicious emails (such as phishing attacks, one of the most common attack vectors), as well as focused, large-scale attacks by APTs and nation-state actors.

Effect against zero-day attacks

Although these measures cannot anticipate a zero-day attack, they can work together to monitor, detect, and flag risks as they emerge. With these tools in place, your clients will receive meaningful, actionable alerts at the earliest possible opportunity.



Vulnerability scanning

Today's vulnerability scanning platforms generally take one of two approaches:

- Relying on databases of known vulnerabilities; this means they cannot detect unknown vulnerabilities
- Dynamic vulnerability scanners, often centered on heuristics of common exploit types, attempting to detect even unknown vulnerabilities

In either situation, finding vulnerabilities is not the same as remediating them. And neither of these approaches can provide truly comprehensive help when it comes to zero-day attacks.

That's why it's important to use integrated tools with simple dashboards that give you greater visibility when it comes to prioritizing vulnerabilities. That lets you manage all the tasks in your vulnerability assessment and patch management process. In fact, ideally, all of the components examined here should be able to work hand in hand, boosting security while minimizing administrative overhead.

Effect against zero-day attacks

Vulnerability scanners may not be able to detect zero-day attacks, since by definition, their signatures are unknown. However, with the rise in multiphased attacks, it is very likely that some component of a zero-day attack will take advantage of a known vulnerability. Therefore, you need to be able to provide optimal coverage to clients to ensure that they have insight into their entire environment.

Patching solutions

Patching solutions are a central part of any cyber protection strategy. These will work differently depending on the vendor; however, most fulfill three very critical core functions:

- Maintain an up-to-date inventory of all software assets in your network, including version numbers
- Compare current version numbers with an up-to-date patch database to determine if a patch is available
- Guide the IT team in deploying applicable patches to systems requiring them

Some patching solutions notify you of vendor patches as soon as they are available, while others allow you to schedule and orchestrate patching throughout the organization. However, as anyone who has ever been responsible for patching will know, having a solution available is not the same as rolling it out.

Therefore, wherever possible, patching solutions should incorporate automation to take as many manual steps as possible out of the hands of IT teams.

Most organizations have a number of mission-critical systems — particularly servers, that cannot simply be taken offline and upgraded. Therefore, updates are usually done on a set schedule, except for certain high-priority vulnerabilities.

For instance, most solutions will not actually perform the update for you. So, whether for routine patching or “out of band” emergency patch rollouts, patching can be a costly program in terms of manual effort to deploy, test, and roll back as needed.

Plus, keeping track of end-of-life products and keeping them safe can become very complicated. Many cloud-native patching solutions do not offer support for legacy, on-premises equipment.

Effect against zero-day attacks

As mentioned above, vulnerability scanners and patching tools cannot necessarily provide protection against zero-day attacks. However, when combined with vulnerability scanning, prioritization, remediation and patching, along with integrated dashboards and reporting, they offer not only resilience against attacks leveraging known vulnerabilities, they put infrastructure in place to protect yourself as soon as a vendor releases a patch for an emerging zero-day threat.

The heart of your vulnerability defense

So far, this white paper has explored a number of best practices and defense strategies that — when combined (since none is completely effective on its own) — can help keep your clients secure against zero-day attacks.

Due to the rise in threats and the speed at which zero-day vulnerabilities emerge and are exploited, it's more important than ever for MSPs to choose vulnerability scanners and patch management tools that they trust — and that they can use easily — to cut risk and mitigate problems quickly.

Acronis provides a complete cyber protection services delivery platform for MSPs with the broadest, most comprehensive coverage against all of today's threats, including zero-day attacks.

Acronis' platform includes:

Single-platform integration: A unified console view for data protection and cybersecurity across all your devices and environments: on-premises, mobile, and cloud

Broad coverage: Integrated patch management that covers over two different software applications

Custom coverage: Vulnerability assessment lets you choose your most critical machines and software, letting you take control of risk

Fail-safe patching: Unique to Acronis, this feature ensures that if a patch fails, the machine automatically restores the most recent image from before the patch from backup storage

Exploit prevention: With prioritization of the most vulnerable applications, such as collaboration applications

Flexibility and power: Apply one or more protection plans to the same device, giving your clients a one-stop shop for backup, vulnerability assessment, and more

Email protection against zero and n days

Acronis

To stand out in today's crowded MSP landscape, you need to be ready to defend against evolving threats. Partnering with Acronis lets you give your clients — and your own team — peace of mind by staying ahead of today's savvy attackers.

Acronis' Cyber Protect Cloud for service providers

will enable you to modernize your clients' security and backup with integrated cyber protection.

Try it here today

We're also featuring a limited-time promotional rebate for MSPs when you switch to Acronis Cyber Protect Cloud.