Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **July 2021**
Sponsored by **Acronis**

Evaluating Advanced Email Security: A Guide for MSPs

Executive Summary

Even a casual reading of the daily news is replete with stories of cyberattacks against organizations across healthcare, government, education, and critical infrastructure (e.g., Colonial Pipeline). Many of these attacks leverage email as the initial attack vector. Organizations are struggling with how to best protect themselves, and few have the internal IT security assets and cybersecurity talent to do it alone. In parallel, managed service providers (MSPs), security value-added resellers (VARs), and cloud distributors are looking for new value-added services from trusted partners to take to market. The juxtaposition highlights the opportunity for safeguarding email from current and evolving threats.

This white paper is written to help MSPs, security VARs, and cloud distributors (hereafter "MSPs" to refer to all three) understand the current cyberthreat landscape and the opportunity for advanced email security solutions that safeguard their customers while offering an additional stream of recurring revenue.

What is the opportunity for MSPs from advanced email security solutions that safeguard their customers while offering a new stream of recurring revenue?

KEY TAKEAWAYS

The key takeaways from this white paper are:

- **Email Security is a Unique Challenge**
  The weaponization of email by cybercriminals has given rise to multiple threats including phishing, business email compromise (BEC), malware, ransomware, and zero-day attacks. Security hinges on scanning 100% of traffic in real-time, with no email unassessed before delivery.
- **MSPs Can Improve Email Security for Customers**
  Every organization is facing the threat of phishing, business email compromise and spoofing, advanced persistent threats and zero-day attacks. MSPs can play a frontline role in defending a customer's email flow.
- **A Checklist for Advanced Email Security Solutions**
  MSPs evaluating advanced email security solutions should be on the lookout for key attributes and characteristics across 16 different areas. A checklist can assist you in the decision-making process.
- **Evaluate Solution Efficacy before Purchasing**
  Several approaches are available to MSPs for evaluating the efficacy of advanced email security solutions before purchase, including reviewing independent test lab results and putting a solution through a real-world test.
- **Evaluate the Strength of Prospective Vendors**
  Assess the market and business strength of prospective advanced email security vendors, making sure the prospective vendor will be around for the long term. Good signals include time in market, existing partnerships, global presence, and complementary growth opportunities.
- **Acronis Brings Much to the Table for MSPs**
  The new Advanced Email Security solution for Acronis Cyber Protect Cloud enables MSPs to protect their customers from email-based threats. The solution enables a set of complementary advanced email security features, adding an additional layer of protection.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Acronis. Information about Acronis is provided at the end of the paper.

What is Advanced Email Security?

Cybercriminals have weaponized email for the delivery of multiple types of cyberthreats. Basic email security techniques identify some of these threats, while advanced email security aims to put a stop to the remainder. The variation in attack types means advanced email security must focus on the many, not just a single attack vector. It's a design question of "and also." This section looks at what makes advanced email security different from basic email security.

PHISHING AND RANSOMWARE

Phishing and ransomware have become significant threats.[1] Cybercriminals unleash general-purpose and targeted phishing attacks to steal account credentials, access commercially sensitive and valuable data, and distribute malware. Ransomware attacks can cripple victims for days or weeks—or even put them out of business entirely—and always wreak havoc on an organization's customers (e.g., inability to access fuel supplies, health services, or attend classes). Email is commonly viewed as the dominant vector for initiating cyberthreats, and organizations need to strengthen protections against phishing, spear phishing, and whaling attacks, along with ransomware distribution.

APTS AND ZERO-DAY ATTACKS

Advanced persistent threats (APTs) and zero-day attacks are particularly pernicious cyberthreats. APTs hide in email messages or attachments as benign and non-malicious, and after sliding through undetected, sit and wait for a countdown to end or an execution signal to be given. Zero-days arrive as never-seen-before cyberattacks and are not detected by comparisons with known threat signatures. Cybercriminals can easily and quickly create zero-days by leveraging artificial intelligence (AI) and machine learning (ML) technologies to form ever-changing weapons of compromise. Detection of APTs and zero-day attacks necessitates going far beyond the capabilities included in basic email security tools. Advanced techniques are required that recursively unpack messages and attachments to identify hidden threats by comparing code behavior with normal operating parameters, and correlating a wider set of underlying access, network, and operating signals to identify new malicious threats.

Cybercriminals have weaponized email for the delivery of multiple types of cyberthreats.

MULTIPLE THREATS, MULTIPLE DEFENSES

The email channel is subject to multiple cyberthreats. Any solution that optimizes for a single threat offers false assurance by blinding defenders to the wider threat context. Advanced email security solutions cannot afford to be reliant on any single approach, layer, or method, but must instead leverage an ever-changing and continually improving set of coordinated defense layers that together provide overall coverage against known and new threat types. Cybercriminals are continually innovating and optimizing their attack campaigns—including designing methods to evade security detection methods—which means that solutions relying on past successes are likely to be quickly compromised.

SCANNING 100% OF TRAFFIC IN REAL-TIME

At least half of all email traffic is spam: unwanted commercial pitches that waste time, divert attention, and clog up user inboxes. Basic email security solutions are good—although not perfect—at identifying and blocking spam.

Of the non-spam email traffic, a small percentage is malicious, dangerous, and should never be delivered to user inboxes. Since it only takes a single email to start a phishing, ransomware, or business email compromise (BEC) attack, scanning less than 100% of traffic in real-time is a dangerous design principle.

No organization can afford to take a sampling approach to scanning both external and internal emails for email-borne cyberthreats. Internal emails can be even more dangerous than external ones, because a compromised account after a phishing attack can be used to spread malicious content internally by trading on the trust implied by requests coming from a colleague's email account.

RAPID DEPLOYMENT

We live and work in an era of speed with instantaneous global communications, rapid supply chain coordination, and digital–physical processes that often appear magical. In such a context, no MSP has the bandwidth or stamina to opt for a multi-year, multi-month, or even multi-week deployment of advanced email security. Speed is the name of the game. Solutions that offer rapid deployment and quick time to value enable MSPs to focus on the offer, not getting the deployment checklist perfect before being even able to start.

INCIDENT RESPONSE SERVICES

Every organization—MSPs included—is impacted by the global cybersecurity talent shortage.[2] Few can find enough well-trained experts to staff current security areas, let alone emerging ones. When partnering with a vendor for advanced email security services, the ability to access complementary skill sets for incident response makes for a streamlined adoption process, as well as enabling the ongoing operation and optimization of the solution, whether it is handling of reports from users or fine-tuning the system. The availability of timely, expert assistance from the vendor for issues, incidents, and any other technical enquiries decreases the cost and risk of aligning with a new offering, enabling current security staff to rest at ease knowing that the vendor's team serves as an extension of their Security Operations Center (SOC) team.

No organization can afford to take a sampling approach to scanning both external and internal emails for email-borne cyberthreats.

DETECTION SPEED

Email is not a real-time communication tool; that's the domain of collaboration apps like Microsoft Teams Chat, Slack, and instant messaging services. Still, there is a general expectation of quickness. People understand a delivery delay of 10-20 seconds, but if they are waiting a minute or more for an email that they know a colleague or customer has just sent, they start to think something is broken. Once several minutes have passed, they are likely to call the help desk to investigate.

To fit within the ecosystem of usage, advanced email security solutions must execute their assessment checks as fast as possible, without giving the appearance of hindering or slowing the flow of email communication. They must also not allow threats to pass through unchallenged. Some advanced email security offerings require 5-20 minutes to check an email message—this is unacceptable because it forces security professionals to choose between delaying all email traffic or scanning less than 100% and remediating threats after delivery.

Improving Email Security for Customers

MSPs can improve email security for customers by stopping four types of advanced email-borne cyberattacks that bypass traditional basic email security defenses. In this section, we briefly examine the four threats requiring advanced protections.

PHISHING ATTACKS

Phishing attacks seek out victims who will take an action that aligns with the interests of the cybercriminal but not their own. Cybercriminals send phishing lures to steal user account credentials, gain access to sensitive data, or install malware on the victim's device for an immediate or future attack. Lateral phishing (also known as internal phishing) leverages the initial foothold of a compromised account to compromise further internal accounts or launch phishing attacks against the organization's customers, partners, and prospects. Spam has frequently been used in recent years as a means of delivering phishing lures and other malicious payloads, such as ransomware. Stopping phishing attacks before they hit user inboxes shuts down a significant threat vector for organizations using email.

BEC ATTACKS AND SPOOFING ATTEMPTS

BEC attacks and spoofing attempts do not deliver malicious payloads, but instead slip malicious intent into seemingly normal business processes, such as changing a bank account number for upcoming payroll, diverting funds for a large vendor payment, or requesting an urgent wire transfer to secure a secretive business acquisition. The absence of a malicious payload makes such attacks impervious to traditional email security methods, which is why they've been successful in stealing tens of millions of dollars in some attacks, and over $1.8 billion in total during 2020.[3] Spoofing, such as lookalike domains or display name deception attacks, play on human fallibility in missing minor deviations in the spelling of email addresses and domain names, among other methods.

BEC attacks don't carry malicious payloads, making them impervious to traditional email security methods.

ADVANCED EVASION TECHNIQUES

Evasion techniques used in malicious email campaigns seek to hide the true intent of a payload from security processes, such as verification tests in virtual sandboxes, burying malicious content several layers inside files and URLs, and bait-and-switch attacks that only activate malicious links after security processing is complete and the marked-as-clean message has been delivered to a user's mailbox. Cybercriminals are aware of the increased defenses being installed to foil their attacks and are fighting back with new and novel techniques to slip through hardened defenses unnoticed. Detecting advanced evasion techniques requires continuous vigilance.

APTS AND ZERO-DAY EXPLOITS

APTs seek to gain a beachhead on endpoints from which to launch further attacks, and zero-day exploits attempt to use newness as a means of evading defenses built to protect against known exploits. Cybercriminals innovate to create next-generation exploit techniques, which by implication demands advanced email security protections capable of detecting unknown exploits.

Critical Capabilities: 16-Point Checklist

MSPs evaluating advanced email security solutions require a set of complementary capabilities across numerous feature areas. In this section, we present a checklist to aid evaluation activities. See Figure 1 for a summary.

Figure 1
Checklist for Advanced Email Security

Checklist Item	Characteristics to Avoid	Preferred Characteristics
Threat coverage	Single focus	Broad and deep
Level of analysis	Original packaging	Deep analysis of URLs and attachments
Multi-layered analysis	Monolithic	Multi-layered
Speed	Disrupts email flow	Seemingly invisible
Threat detection accuracy	High level of false positives	High threat detection accuracy in independent evaluations
File functionality post-scan	Neutered, broken, inoperable	Fully functional
URL scanning	Deny list only	Blocking known and unknown malicious URLs
Threat intelligence	Single source, unavailable	Multiple sources
Anti-BEC	Weak protection against content without a malicious payload	Implementing network-level checks such as domain spoofing, SPF, DKIM, and DMARC
ATP capabilities	Known threats only	Known and unknown threats
Zero-day detection	Analysis at the application/malware level	Analysis at the CPU/exploit level
Anti-evasion	Can't address evasion techniques	Designed to counteract advanced evasion attempts
Protection before the inbox	Detection mode, where emails are sometimes scanned after they reach the end user's inbox	Prevention mode, where emails and URLs are always scanned before delivery to the end user
100% dynamic scanning of content	Reliance on signatures without dynamic scanning	Full file/URL dynamic rendering for all content
Incident Response	Unavailable	Integrated in the solution at no additional cost
Reporting	None, irregular, basic	Regular, detailed

Source: Osterman Research (2021)

MSPs evaluating advanced email security solutions require a set of complementary capabilities across numerous feature areas.

CHECK 1: THREAT COVERAGE

Email is under attack from multiple threat types, including next-generation exploits and attacks. An advanced email security solution must take a broad and deep look at each message—along with any attachments and links—to investigate the possibility of cyberthreats combining several attack types. Optimizing for a given

threat type (like phishing) may be valuable for stopping those dangers, but will by design ignore wider risks.

CHECK 2: LEVEL OF ANALYSIS

Advanced email security solutions must ignore how an email and any attachments are initially packaged. Cybercriminals hide threats in seemingly benign packaging, such as a Word document or zipped file. Breaking apart the original packaging of each email and any attachments is the only way to identify malicious threats trading on surreptitious delivery. Each individual element should be checked for threats in deep analysis of several nesting levels.

CHECK 3: MULTI-LAYERED APPROACH

Multiple advanced security tools should work in combination to assess the basic elements of email messages and attachments for different types of cyberthreats. Developing an overall perspective based on a detailed analysis of each message and attachment element provides strong assurance either way that a message is benign or malicious. Multiple independent layers working in tandem provide room for identification of advanced new threats and attack patterns.

CHECK 4: SPEED

Advanced email security solutions need to pass the phone test. When a user is talking to a colleague or customer, the comment "I have just sent you an email" should be followed within several seconds by the email being delivered. If delivery feels slow and the user continually clicks the Send/Receive button, the natural flow of email has been disrupted. Users start thinking that something is broken when email messages are not delivered for several minutes or longer.

Advanced email security solutions must be both fast and accurate. One only is not good enough.

CHECK 5: THREAT DETECTION ACCURACY

Speed of operation is one side of the coin for advanced email security solutions, and accuracy of judgment is the other. Declaring threat-laden email messages and attachments as safe and delivering them to end users must be avoided. An advanced email security solution with high detection rates and low false positives is crucial for gaining users' trust.

CHECK 6: FILE FUNCTIONALITY POST-SCAN

Files must be checked recursively for embedded and hidden threats, otherwise the advanced email security solution isn't doing what it should. But once checked and marked as benign, the file delivered to the end user must be as fully functional as possible. It should not be neutered, broken, or inoperable. Users facing broken files will revert to unsanctioned tools that bypass security checks, opening the organization to more significant security threats.

CHECK 7: URL SCANNING

URLs included in email messages and attachments can lead to malicious sites that deliver malware, ransomware, APTs, and other threats. An advanced email security solution must check the URL against known malicious sites, visit the destination site and recursively scan for threats, evaluate domain registration recency and provenance, and check for lookalike and soundalike domain names that could indicate a spoofing attempt, among others.

CHECK 8: THREAT INTELLIGENCE

New cyberthreats emerge every day and businesses can't afford to remain unprotected. Threat intelligence services that seamlessly integrate with an advanced email security solution enable comprehensive protection against emerging email-borne dangers, quickly rendering new threat campaigns ineffective.

CHECK 9: ANTI-BEC

It is crucial for businesses to be able to detect emails that do not necessarily include malicious files/URLs but pose a threat due to impersonation. Many spoofing attempts can be identified by assessing the alignment between key email security declarations held in the customer's DNS record, such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting and Conformance), along with DNSSEC (Domain Name System Security Extensions). When combined with IP reputation checks, non-alignment between these elements can raise doubts as to the authenticity of a given message.

CHECK 10: ATP CAPABILITIES

Advanced threat protection (ATP) refers to a bundle of capabilities that go beyond scanning for known threats only. ATP includes protections against impersonations, zero-day attacks, weaponized links and attachments, and credential phishing campaigns that target sensitive data, among others. A strong list of ATP capabilities is a good sign that a given advanced email security solution is focused on dealing on more than just identifying known attacks with familiar signatures.

CHECK 11: ZERO-DAY DETECTION

A zero-day attack leverages a software vulnerability (also known as a "bug") that is either unknown or unaddressed by the software vendor. Advanced threat protection modules, such as sandboxes and content disarm and reconstruction (CDR), usually scan at the application level, relying on known data or behaviors. A zero-day attack starts at the CPU level with an attempt to execute malicious code. Hence, a more deterministic way to check for zero-days is to leverage CPU-level data to catch the attack at the exploit level.

CHECK 12: ANTI-EVASION

The inclusion of innovative evasion techniques used by cybercriminals needs to be accounted for in the design of advanced email security solutions; to act as though evasion techniques won't be used is shortsighted. For example, one common evasion technique is to check whether a document is being opened in a virtual sandbox, and if so, to not deploy the included malicious payload. Another technique is to check the details of the IP infrastructure requesting a URL link, and if it comes from an IP address space known to belong to a security service, to deliver a benign page rather than the malicious one. Advanced email security solutions require their own level of surreptitious evasion of evasion techniques to clear the veracity of each message, attachment, and link.

The inclusion of innovative evasion techniques used by cybercriminals needs to be accounted for in the design of advanced email security solutions.

CHECK 13: PROTECTION BEFORE THE INBOX

It is critical for organizations to deploy their advanced security solutions in a way that provides their users protection before the inbox, also referred to as "prevention mode". Prevention mode makes sure every email and URL is scanned before it is delivered to the end user. The alternative to this is operating the system in detection mode, which first delivers the email to the user, and then completes the scan in the background, pulling the email from the user's inbox in case it is found malicious, which exposes the organization to risk in case the user opened the email before the scan was completed.

CHECK 14: 100% DYNAMIC SCANNING OF CONTENT

Today's advanced security solutions cannot rely exclusively on the use of signature-based detection and other static checks. They need to actively scan the content, detonating a file or a URL on a virtual machine to check it in real-time. Additionally, a partial scan of the content, due to scale or performance considerations of the email security solution, will leave the organization subject to risk.

CHECK 15: INCIDENT RESPONSE

MSPs benefit from incident response services offered by solution vendors, enabling them to leverage the strength of partners rather than having to establish new skill sets internally. Incident response services should offer:

- Ongoing technical and product support.
- Escalation routes for difficult issues.
- Technical troubleshooting.
- Optimization of the system with rules and policy settings for the specific organization, as informed by newly encountered threats.

Incident response services should offer ongoing support, escalation pathways, and technical troubleshooting.

CHECK 16: REPORTING

Not allowing threats through to customers is an important outcome, but without any sense of the quantity and variation of blocked threats, customers are likely to become indifferent and apathetic towards the service. Reporting capabilities offer a regular stream of updates to customers, enabling them to understand the types of threats they are subject to (and protected from), which can aid in their own efforts to strengthen defenses such as adding a new security awareness training module or an additional level of advanced protection. Reporting also reinforces the need for and efficacy of current security capabilities, which aids with customer retention and safeguards your recurring revenue streams.

Evaluation Criteria and Best Practices

In this section, we outline evaluation criteria and best practices for MSPs when evaluating advanced email security solutions.

EVALUATING EFFICACY PRE-PURCHASE

Evaluating the efficacy of advanced email security solutions is a challenging, difficult, and nuanced task. There are no industry-accepted test suites to test against. Cybercriminals are continually innovating attack types and vectors, including leveraging current social and economic news to trick victims. Vendors of advanced email security solutions play a good marketing game of claiming to be "the best" at identification rates, speed of assessment, and overall efficacy, but do not disclose the full details of their protection arsenal so as not to tip off their adversaries and thus neuter their products. This combination of factors presents great challenges for customers hoping to assess advanced email security solutions prior to purchase and deployment.

There are three good approaches for MSPs when doing comparative analysis:

1. **Refer to Evaluations from Independent Testing Labs**
   No MSP wants to partner with an advanced email security vendor that can't deliver the goods. SE Labs, a private, independently owned and run testing company that assesses security products and services, carried out a detailed and nuanced test of eight competing email security solutions in early 2020 using live, targeted email threats. The report by SE Labs outlines its testing and rating methodology and is available for download and review.[4] Note that Acronis' Advanced Email Security solution for Acronis Cyber Protect Cloud is powered by Perception Point, whose detection rate has surpassed any other evaluated solution.
2. **Deploy for Supplementary Protection**
   MSPs can configure an additional advanced email security solution to receive all the marked-as-clean emails processed by its current email security stack. Emails marked clean are then evaluated by the supplementary solution for undetected threats. Reporting can be used to highlight how many additional threats were identified and captured. The underlying assumption of this approach is that if the supplementary solution captures additional undetected threats, then it should also capture any of the threats already detected by the current email security stack. This approach is a real-world, high-stakes test because it functions using the actual email traffic flows of an MSP.
3. **Deploy for Primary Protection in Assess-Only Mode**
   Vendors of advanced email security solutions may offer an assess-only mode of their technology to enable MSPs to gauge efficacy. In assess-only mode—also called monitoring or non-blocking mode—all emails are delivered to end users, but reports are kept of the count and types of messages that were identified as malicious. Email messages are not removed from the standard email flow for end users—therefore not impacting communications—while the security team is able to assess efficacy based on real-world email traffic flows.

Evaluating the efficacy of advanced email security solutions is a challenging, difficult, and nuanced task.

For the second and third approaches above, having as little to install as possible is best, and interfering with current email flows as little as possible is also preferred, e.g., not having to change MX records. A zero-install, zero-impact approach provides MSPs with the assurance that current email traffic flows are not compromised during testing, and that once testing is complete, the exit pathway is just as simple.

ASSESS VENDOR STRENGTH

Assess the market and business strength of prospective advanced email security vendors. Important factors in assessing the strength and long-term viability of a vendor include:

- **Time in Market**
  For how many years has the prospective vendor been in business? Vendors with more than a couple of years—or even a decade—under their belt have a proven track record of delivering value, weathering disparate economic cycles, and adapting to the changing dynamics of the advanced email security market.
- **Spread of Current Partnerships**
  What is the extent and breadth of current partnerships between the prospective vendor and other MSPs in your market and beyond? Prospective vendors with strength in this area are more likely to already have a strong partnership program, including onboarding support and ready-to-use marketing resources. Being their first partner carries risk.
- **Global Presence**
  It's an easy but ultimately empty promise for a prospective vendor to claim "global presence" based on a single office location and a single rack in a data center somewhere. It is much more difficult and costly for a vendor to open offices in multiple locations around the world, secure a physical presence in data centers in multiple geographies, and develop the capabilities to store and secure data locally to meet the patchwork of data sovereignty laws around the globe. These difficult and costly moves provide a good indication of strength to potential customers.

Assess the market and business strength of prospective advanced email security vendors, along with complementary growth opportunities.

ASSESS COMPLEMENTARY GROWTH OPPORTUNITIES

Establishing fewer but stronger partnerships enables MSPs to reduce complexity, simplify operations, and streamline go-to-market strategies. What are the complementary opportunities to grow with a prospective vendor beyond just advanced email security? What other security, data protection, and general IT services are available that can be used by an MSP for cross-sell and upsell opportunities, thereby increasing monthly recurring revenue from customers who have experienced the value of the initial offering?

The Acronis View

Advanced Email Security for Acronis Cyber Protect Cloud, powered by Perception Point, focuses on enabling MSPs to protect their customers from email-borne threats running rampant across the world. The Advanced Email Security offering includes a set of complementary features to elevate email protections:

- **Anti-Spam**
  Anti-spam filters and IP reputation checks root out spam and stop it from clogging user inboxes. Communication graphs are automatically created to identify established patterns of communication by email and deviations with malicious consequences.
- **Anti-Evasion**
  Embedded files and URLs in email messages and attachments are recursively unpacked to seek out evasive techniques included by cybercriminals. Each unpacked element is separately analyzed by the Advanced Email Security protection layers, and files and URLs are dynamically scanned using multiple application versions and launch patterns to root out new evasion techniques.
- **Threat Intelligence**
  Several separate threat intelligence services are used by Advanced Email Security to bring the latest insights on new and emerging threat vectors into service. The solution draws on Perception Point's own threat intelligence service, based on threats encountered by the entire customer base, as well as additional threat intelligence services from external security vendors and the cybersecurity community.
- **Anti-Phishing**
  Multiple phishing filters are used to identify and stop phishing attacks, including a proprietary image recognition engine that checks for inappropriate and malicious usage of the top 1000 brand images at destination URLs. The Advanced Email Security offering also leverages anti-phishing defenses from several other security vendors to strengthen URL reputation checks.
- **Anti-BEC**
  Machine learning algorithms protect against spoofing attacks by evaluating alignment between SPF, DKIM, and DMARC records, along with wider IP reputation analysis. Deviations from standard operations raise warning flags that are used to prevent suspicious content from reaching end users, such as BEC attacks using lookalike domain names and display name deception tricks. Anti-BEC also includes usage of VIP lists to detect impersonation of display names, usage of similar brand names with minor changes, impersonation of known brands, text and language analysis, and other methods.
- **Static Signature-Based Analysis**
  Detection of known threats using multiple signature-based anti-virus engines in combination with a unique detection engine for identifying the more complicated variety of signatures. Signature based detection is applied to emails and files to root out malicious, suspicious, and dangerous attacks.

The Advanced Email Security offering focuses on enabling MSPs to protect their customers from the plethora of email-borne threats running rampant across the world.

- **Next-Generation Dynamic Detection**
  Prevent APTs and zero-days through unique, CPU-level protection technology that focuses on deviations from standard flows in the assembly code. By analyzing the runtime execution flow of applications, new attacks can be blocked at the exploit stage before malware has even been released. Unlike CDR solutions, content functionality is not compromised.

Summary and Next Steps

Organizations face significant ongoing threats through email messages, attachments, and embedded links. Advanced email security solutions are available to safeguard the email channel with next-generation protections. MSPs have an opportunity to significantly elevate their email security services and earn recurring revenue by offering services built on top of the Acronis Advanced Email Security solution for the Acronis Cyber Protect Cloud platform.

Sponsored by Acronis

At Acronis, we believe the data, applications, systems, and productivity of every organization should be protected against loss, theft, and downtime—whether it's caused by cyberattacks, hardware failure, natural disaster, or human error. From MSPs supporting clients to enterprises serving global users to organizations handling sensitive data, we lower risks, improve productivity, and ensure your organization is #CyberFit.

Driven by our passion to protect every workload, we've created the only all-in-one cyber protection solution for environments of any size—and solved the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern world.

Our unique combination of automation and integration enables all the prevention, detection, response, recovery, and forensics capabilities needed to safeguard your data and digital infrastructure while streamlining protection efforts.

Acronis is an established partner to MSPs in the cybersecurity and data protection industry for more than 18 years. In fact, our flagship product—Acronis Cyber Protect Cloud, integrating data backup and disaster recovery, next-generation anti-malware, and endpoint protection management, is specifically designed for service providers. The solution supports rich integrations with RMM and PSA tools, hosting control panels, billing systems, and marketplace providers and provides an API for any custom integrations. It also provides service providers with a multi-tenant portal, pay-as-you-go pricing, white-labeling capabilities, and reseller management.

Acronis Cyber Protect Cloud has five advanced add-on packages that allow MSPs to enhance their cyber protection services with advanced security, backup, management, disaster recovery, or email security capabilities. This enables service providers to deliver superior protection to customers while controlling their total cost of ownership.

Learn how Acronis lets you deliver cyber protection easily, efficiently, and securely:

- Contact Acronis Sales for a live product demo tuned to your use-case
- Start your complimentary 30-day free trial
- Visit our Resource Center for white papers, case studies, ebooks and more
- Check out the Acronis blog

Acronis

www.acronis.com

@Acronis

+1 781 791 4486

Elevate email protection for your clients and earn additional recurring revenue by offering services built on Acronis Advanced Email Security.

[1] Osterman Research, *How to Reduce the Risk of Phishing and Ransomware*, March 2021, at https://ostermanresearch.com/2021/03/17/orwp_0336/

[2] Osterman Research, *How to Minimize the Impact of the Cybersecurity Skills Shortage*, October 2020, at https://ostermanresearch.com/2020/10/30/orwp_0334/

[3] FBI, *FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics*, March 2021, at https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

[4] SE Labs, *Email Security Services Protection (2020 Q1)*, March 2020, at https://selabs.uk/reports/email-security-services-protection/