WHITE PAPER

Cyber protection across the NIST Framework with Acronis for MSPs

Introduction

Endpoint detection and response (EDR) and extended detection and response (XDR) are essential solutions to gain full visibility into attack surfaces, combat advanced threats and ensure efficient protection. However, resource and skills constraints often make these tools better suited for large enterprises with robust budgets and high-capacity IT security teams.

With AI-based attack analysis and response, security services such as managed detection and response (MDR) and market consolidation trends have transformed EDR and XDR security. These advancements make cutting-edge detection and response technologies more accessible and affordable to resource-constrained IT teams and service providers.

While an MSP's delivery of efficient protection is critical, the ability to only stop threats isn't enough. Today's MSPs should not only address cyberattacks, but also ensure data protection and business continuity. The most comprehensive cyber protection strategies should include safeguarding the primary target of intrusions — clients' critical data. As a result, managed security services should adopt tools to achieve holistic cyber protection and proactively harden environments. Unfortunately, this often leads to increased complexity, point-solution sprawl, administration challenges and alert fatigue.

About Acronis and the NIST Cybersecurity Framework

This white paper explores how Acronis can enable you to deliver integrated and consolidated cyber protection, which unifies cybersecurity, data protection and IT management. Acronis simplifies protection to help MSPs improve service delivery and provide unmatched security, business continuity and resilience to clients. With our cyber protection platform, you can identify vulnerable assets, proactively protect them, detect and block common threats, enable response and remediation, and recover from advanced attacks in a single pane of glass.

This white paper also outlines the delivery of comprehensive cyber protection based on the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework. Whether your clients want to qualify for cyber insurance, reduce cyberattacks or improve their cybersecurity risk management, the NIST Framework defines core cybersecurity processes and procedures. Acronis' integrated cyber protection capabilities are purpose built in alignment with NIST to ensure your clients' security.

Core functions of the NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework

The NIST Framework enables organizations — regardless of size, degree of risk or sophistication — to improve security and resilience by prescribing steps for detecting, managing and countering cybersecurity events. The Framework consists of six core functions that security programs should address to effectively mitigate security risks and deliver comprehensive protection and resilience. We will deep dive into each function in the latter portions of this white paper; but for now, let's briefly describe the six essential functions of the NIST Cybersecurity Framework:

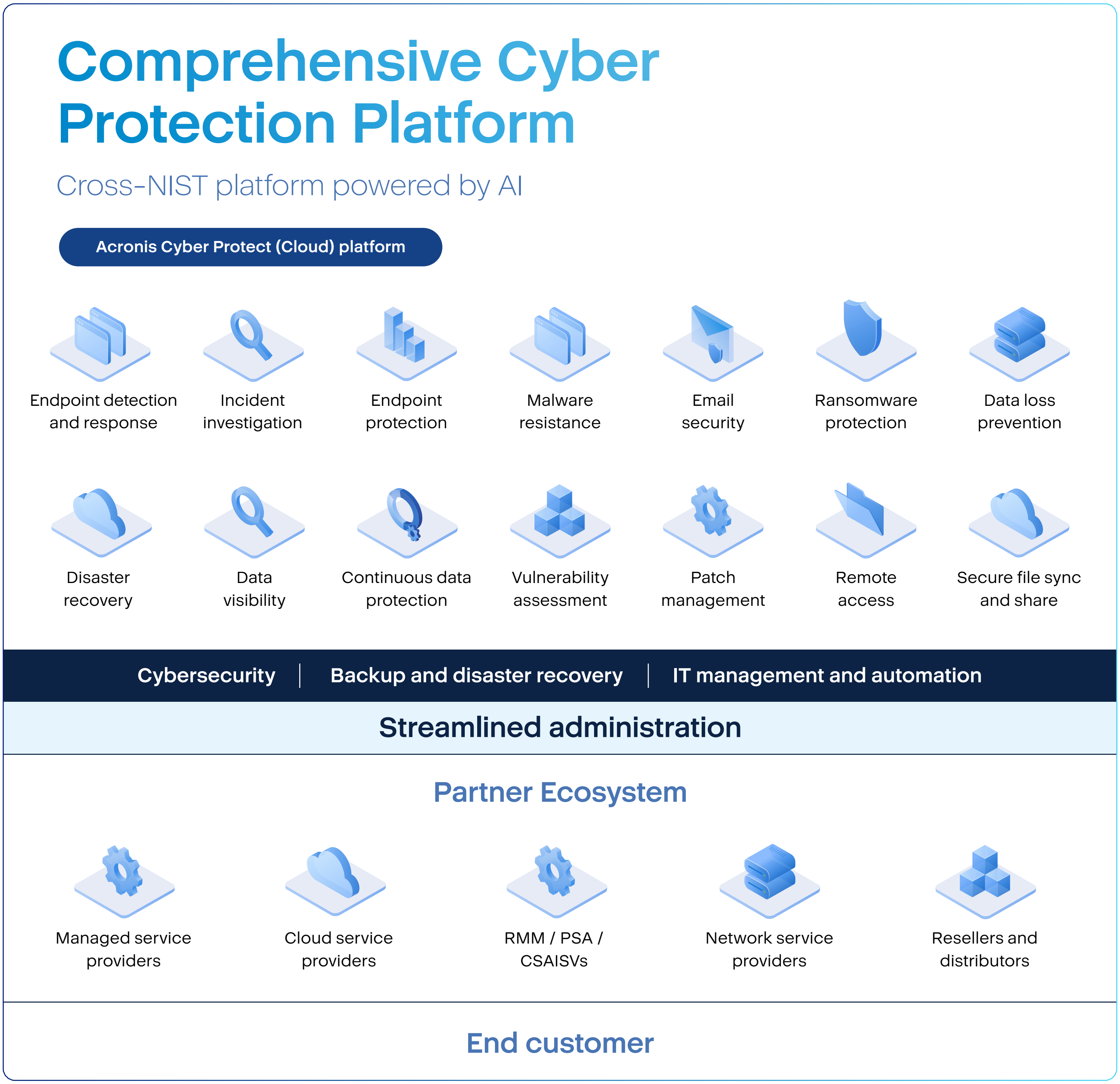
- **Govern.** Ensure that expectations, policies and cybersecurity risk management strategies are well communicated, implemented and monitored across your client's organization. Prioritize and reinforce the other five functions while factoring in the context of your client's business and their mission.
- **Identify**. Discover vulnerable assets you need to protect by establishing a baseline for what assets exist, what risks are associated with them and how these risks relate to your business goals.
- **Protect**. Proactively protect your environment to mitigate risks by developing and implementing appropriate safeguards to ensure data protection and services delivery. These can include access control and awareness and training.
- **Detect**. Effectively detect threats in a timely manner. Ensure you can identify anomalies and events with security controls and continuously monitor for security events.
- **Respond**. Respond to and remediate in-progress attacks and damage by containing threats, blocking malicious processes, preventing further spread and closing security gaps.
- **Recover**. Protect data and ensure business continuity with plans for data restoration in the event of a cybersecurity attack.

Function Unique Identifier	Function	Category Unique Identifier	Category
GV	Govern	GV.OC	Organizational Context
		GV.RM	Risk Management Strategy
		GV.RR	Roles, Responsibilities and Authorities
		GV.PO	Policy
		GV.OV	Oversight
		GV.SC	Cybersecurity Supply Chain Risk Management
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

* Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology (NIST)

Acronis Cyber Protect Cloud

The Acronis Cyber Protect Cloud platform is designed to provide consolidated cybersecurity, data protection and IT management in a single platform. This allows MSPs to rapidly launch and manage multiple services from this single platform, including anti-malware and anti-ransomware, endpoint detection and response and data protection. Acronis Cyber Protect Cloud right sizes to your in-house skills, budget and clients. Acronis Cyber Protect Cloud is easy to provision, manage and scale, and enables MSPs to rapidly deploy compelling solution offerings to clients, including vulnerability management, data protection, security, threat remediation and business continuity.



Comprehensive Cyber Protection Platform

Cross-NIST platform powered by AI

Acronis Cyber Protect (Cloud) platform

- Endpoint detection and response
- Incident investigation
- Endpoint protection
- Malware resistance
- Email security
- Ransomware protection
- Data loss prevention
- Disaster recovery
- Data visibility
- Continuous data protection
- Vulnerability assessment
- Patch management
- Remote access
- Secure file sync and share

Cybersecurity | Backup and disaster recovery | IT management and automation

Streamlined administration

Partner Ecosystem

- Managed service providers
- Cloud service providers
- RMM / PSA / CSAISVs
- Network service providers
- Resellers and distributors

End customer

Let's take a deeper look at how the six core functions of the NIST framework can be mapped across an organization using Acronis Cyber Protect Cloud

Acronis Cyber Protection NIST mapping

Cross-NIST Platform powered by AI

Govern

- Provisioning via a single agent and platform.
- Centralized policy management.
- Role-based management.
- Information-rich dashboard.
- Schedulable reporting.

Identify

- Software and hardware inventory.
- Unprotected endpoint discovery.
- Content discovery.
- Data classification.
- Vulnerability assessments.

Protect

- Security configuration management.
- Patch management.
- Device control.
- Data Loss Prevention.
- Security training.

Detect

- AI / ML-based behavioral detection
- Exploit prevention
- Anti-malware and anti-ransomware
- Email security.
- URL filtering.

Respond

- Rapid incident prioritization.
- Incident analysis.
- Workload remediation with isolation.
- Forensic backups.
- Remote access for investigation.

Recover

- Rapid rollback of attacks.
- One-click mass recovery.
- Self-recovery.
- Backup integration.
- Disaster recovery integration.

Govern

How Acronis supports the NIST function

With threats growing rapidly in sophistication, cybersecurity takes center stage with regard to managing organizational cyber risk. Your MSP business and clients need to ensure internal decisions are thoughtfully developed and executed to support a comprehensive cybersecurity strategy. Acronis Cyber Protect Cloud empowers MSPs to achieve desired outcomes across the other five functions, identify, protect, detect, respond and recover, while factoring in the expectations and considerations of senior leadership.

Cyber protection is not one size fits all. Not only should the necessary security measures be implemented, but also instituted within the context of the organization (your clients). This embodies developing a cybersecurity strategy, managing supply chain risks, roles, responsibilities and authorities, and overseeing the entirety of the security strategy. Acronis Cyber Protect Cloud enables IT teams and MSPs with a single platform designed for MSPs to deliver holistic cyber protection. Primarily, by centrally managing cyber protection on a single console with Acronis, you are better informed on how the other five functions are implemented — as well as how they are liaised with and monitored by stakeholders.

How Acronis helps

Provision via a single agent and platform

Acronis Cyber Protect Cloud offers a single platform that covers all the protection needs of service providers and their clients. The natively integrated solution unifies cybersecurity, backup, disaster recovery and endpoint management. Because we've consolidated multiple areas of protection on one robust platform, this significantly reduces point solution sprawl, mitigates human error and saves MSP budgets. Via a single agent, Acronis Cyber Protect Cloud makes it easy to add protection features and capabilities without requiring additional installation, cost or IT expertise. Additionally, with a single agent honing all protection services, the solution is light on resource consumption.

The goal is to ensure your services fortify cyber resilience to clients with an integrated solution ecosystem. By effectively reducing your clients' cyber risk and reinforcing their security posture, Acronis' single platform helps you readily evaluate existing protection measures and security vulnerabilities across your clients' IT environments to make informed decisions and pivot security strategies in the right direction.

Centralize policy management

From the same console, you can manage protection policy configuration with low management effort. For MSPs, ease of use is a primary concern. All too often, IT professionals are spread thin and juggling multiple siloed tools is inefficient. Acronis' single console helps you manage protection policies in one place — within a single dashboard. Your MSP business can review, update and enforce policies with ease as you and your clients' requirements continuously change. Whether the IT environment becomes more diverse, compliance regulations become more stringent, or the number of endpoints expand, you can easily adjust protection on the centralized console. You can create protection plans customized to the needs of your MSP business and clients.

Prevent unauthorized users with role-based management

Acronis Cyber Protect Cloud leverages strict role-based access control (RBAC) to safeguard your clients' IT environments. This feature enables you to define who is granted access to specific environments, from virtual machines and Azure instances in the cloud to hosts, clusters and groups of on-premises virtual machines. Your MSP business can permit access with high granularity by designating role-based access to any resource. RBAC helps to reinforce who is responsible and accountable for certain aspects of cybersecurity risk. It also helps to delegate the roles and responsibilities of cyber protection across your clients' organization.

Stay well informed with an information-rich dashboard

With Acronis, the comprehensive dashboard is equipped with customizable widgets that enable you to swiftly identify problems and shift priorities in the right direction. With Advanced Security + EDR, you can even view detection tactics and analyze a monthly and weekly comparison of detected adversarial activities. Equipped with this information, you are empowered to analyze, enhance and pivot the security strategy to better protect your clients against such tactics and reduce cybersecurity gaps organization wide.

Streamline and tailor reporting

Acronis' flexible reporting provides powerful insights to help you quickly pull client executive report summaries and communicate your MSP business's value to your client base. You can inform internal and external stakeholders on the performance of the current security measures you have in place to mitigate cyber risks. Thereafter, you can evaluate and improve your security strategy.

With a data-driven approach, these insightful reports help demonstrate your MSP business's ongoing efforts to mitigate cyberattacks. Reports can be presented to cyber insurance underwriters and compliance officers, demonstrating your MSP business's continuous measures to reduce cybersecurity risks — while helping your clients qualify for cyber insurance policies and maintain regulatory compliance.

Identify

How Acronis supports the NIST function

Acronis Cyber Protect Cloud helps your MSP gain a deep understanding of your clients' cybersecurity risk and identify organizational assets, systems and users. This ensures your technicians know precisely what, where and who they need to protect as well as the potential risks. With automatic software and hardware inventory collection, network-based and active directory-based discovery, and data classification, your MSP can develop a complete understanding of your clients' network, infrastructure and data.

Aside from pinpointing vulnerable assets, Acronis can help you enhance security policies, processes and procedures in alignment with your clients' risk management strategy and business needs. The solution is purpose built to help your MSP save time, refocus high-priority objectives and improve the overall service experience for your clients.

How Acronis helps

Discover unprotected endpoints

Acronis Cyber Protect Cloud will discover unprotected endpoints and streamline the provisioning process by installing multiple agents at once — in cloud and on-premises environments. Once your technicians import lists of assets and computers from the file, they can perform manual, local network-based discovery or active directory-based discovery. Acronis empowers an MSP to remotely deploy agents on discovered assets and auto-apply protection plans across your clients' endpoints and vulnerable assets. By auto-applying protection, the platform enables your technicians to provision services and remotely identify, assess and secure endpoints to help keep your clients safe.

Automatically inventory software and hardware assets

With Acronis, your MSP can, with minimal effort, schedule regular, automatic scans to inventory software and hardware assets on all protected endpoints, keeping inventories up to date and helping to scale with your clients' business needs. This includes CPUs, GPUs, RAM and network adapters. Acronis software and hardware inventory collection enables your MSP to browse and search all your clients' assets as well as filter specific criteria, including processor model, cores, disk total size and memory capacity.

Leveraging improved visibility, your MSP can proactively monitor security gaps and mitigate cyber risks in clients' hardware and software environments. The automatic scans enable you to streamline day-to-day operations, including IT management, to deliver comprehensive protection. Generated inventory reports are available to share with technicians, stakeholders and clients when discussing security strategy.

Classify sensitive data

Acronis Cyber Protect Cloud automatically classifies your clients' sensitive data. Leveraging predefined classifiers for sensitive data based on common regulatory frameworks like GDPR, HIPAA and PCI-DSS, Acronis identifies, assesses and securely manages valuable data. Acronis data protection maps helps MSPs to track protection statuses of important files, alerting your IT team as to whether your clients' files are being securely backed up. Acronis also enhances your MSP's visibility of data-rich environments involved in security incidents to foster swift, efficient response.

Protect

How Acronis supports the NIST function

Acronis Cyber Protect Cloud proactively defends your clients' technology infrastructure to safeguard against, prevent and reduce cybersecurity risk while delivering security measures to address the "Protect" NIST function. These measures include vulnerability assessments, patch management, device control, endpoint security management configuration, data loss prevention (DLP) and backup.

How Acronis helps

Find open vulnerabilities and automatically patch them

Assess and securely manage cloud and on-premises applications with vulnerability assessments and patch management. Acronis vulnerability assessments discover open vulnerabilities and prioritizes them based on severity. Vulnerability assessment scans are continuous and leverage daily updates of the Acronis vulnerability and patch management database, so an MSP stays ahead of the latest common vulnerabilities and exposures (CVEs). Acronis patch management empowers MSPs to patch over 300 applications with automatic patching that can be deployed on a schedule.

Strengthen device control

Ensure your clients mitigate their risk of data leakage by restricting the devices that pose a danger to their IT environments and businesses. Acronis gives MSPs complete control to block, allow or "read-only" the client's network-connected local workloads, including endpoints, ports, peripheral and redirected devices, clipboards and virtualized sessions. An MSP can create allowlists based on device type, USB (even on a granular level, down to serial numbers) and clipboard operations. Real-time alerts can be customized based on device and port type, keeping your MSP up to date on your clients' connected workloads.

Centrally manage endpoint security configurations and harden endpoints

Acronis helps MSPs simplify and streamline endpoint security management, eliminating the need to hire additional cybersecurity talent. Acronis centrally manages endpoint security configurations, so your MSP can use the built-in Acronis #CyberFit score to assess your clients' endpoint security posture and provide them with actionable recommendations. Via a single console, admins can remotely adjust and apply policies to all endpoint protection plans. This enables MSP technicians to easily manage cyber protection across multiple clients, per client or per endpoint — fortifying protection to ensure each endpoint is safe.

Prevent data leakage with data loss prevention (DLP)

Acronis prevents sensitive data leakage by controlling data flows inside the organization, stopping valuable data from ending up in the hands of unauthorized individuals. With behavior-based endpoint DLP, Acronis Cyber Protect Cloud automatically creates and continuously maintains business-specific policies to protect sensitive data at scale.

Back up data to ensure no loss

Acronis integrated data protection ensures an MSP can deliver best-of-breed backup and recovery services. Our award-winning data protection lets MSP technicians choose between file-level backup and full-image backup options — saving time and significantly reducing client downtime. With Acronis, you can back up individual files or safeguard an entire business with just a few clicks. Acronis helps drive competitive advantage for MSPs with reliable, efficient and secure backup and recovery. Additionally, Acronis backups leverage self-protection using integrated anti-malware scans to prevent ransomware and other malware on your clients' backed-up data.

Detect

How Acronis supports the NIST function

Acronis Cyber Protect Cloud detects and analyzes suspicious activity, threat anomalies and cyberattacks, while enabling you to stay ahead of cybersecurity threats by discovering and analyzing indicators of compromise (IOCs) and patterns that deviate from the norm. By aggregating and correlating complex threat data from cyber events, Acronis Cyber Protect Cloud alerts you to security incidents and helps you expedite response activities.

How Acronis helps

Get actionable threat intelligence with Acronis Advanced Security + EDR

Acronis Advanced Security + EDR provides actionable threat intelligence focused on emerging threats delivered by Acronis Cyber Protection Operation Centers (CPOCs), and our internal Security Operations Center (SOC) monitors the threat landscape 24/7 and provides actionable alerts which can result in automatic enhancements of policies.

Enhance protection to cover more attack surfaces with Advanced Security + XDR

With Acronis Advanced Security + XDR, protection is expanded to cover more attack surfaces. The solution not only offers endpoint security, but also email, collaboration application and identity protection. Acronis enables MSPs to gain critical visibility and detect and protect a wider range of IT environments to enhance their clients' cybersecurity posture, reduce cyber risk and bolster resilience.

Improve cost efficiency while you bolster your security service with Acronis MDR

For MSPs facing an IT skills shortage and experiencing resource constraints, Acronis Managed Detection and Response (MDR) is a powerful endpoint security service designed for MSPs. It enables you to gain all the benefits of EDR and XDR without requiring additional IT talent and its associated costs. From outsourcing day-to-day operations to responding to advanced security events, the MDR team helps you optimize resource allocation by delivering 24/7/365 monitoring, rapid detection, investigation, response to, and remediation of threats and attacks, as well as support — so you don't have to. MDR offers expert support in handling EDR and XDR to ensure unmatched business resilience, fewer false positives and faster response times.

Detect and stop threats with AI- and ML-based behavioral detection

Acronis detects and stops threats like malware and ransomware with AI- and ML-based behavioral detections. It continuously monitors and correlates events on an endpoint level to monitor suspicious activity, identify threat anomalies and detect malicious event chains that would otherwise seem benign when viewed as siloed events. You can leverage AI-based prioritization of security incidents across multiple endpoints — rather than a flat list of all alerts or analysis of hundreds of logs. This correlation of data allows you to detect and analyze cyberthreats that point solutions and signature-based detection would otherwise miss. Acronis Advanced Security + EDR saves an MSP from performing resource-consuming tasks, such as threat hunting, so they can focus on delivering quality security services.

Prevent vulnerability exploitation

Acronis uses behavior-based detection heuristics to prevent fileless attacks and vulnerability exploitation. These vulnerabilities can include patch vulnerabilities that can lead to cyberattacks, including zero days. Additionally, Acronis provides efficient protection against ransomware, malware and other unknown threats. An MSP and its clients can enjoy peace of mind knowing Acronis uses real-time protection and detects malware with exploit prevention technology — leveraging integrated technology with Intel® Threat Detection Technology (TDT) for increased protection.

Search for indicators of compromise (IoCs)

Acronis Cyber Protect cloud automatically searches for indicators of compromise (IoCs) based on the Acronis threat intelligence feed. An MSP can use this intelligence to better understand cyber events, respond to specific

IoCs found on endpoints and improve response times or mean time to respond (MTTR) for their clients.

Leverage award-winning anti-ransomware with automatic rollback

Acronis protects backups and endpoints against ransomware with award-winning technology. Ransomware and cryptomining process detection defend your clients' workstations, network and backups, while entropy analysis detects advanced ransomware threats — helping you to quantify the randomness of data sets and gain insights into complex intrusions. Automatic recovery of affected data works within seconds to roll your clients back to a preransomware state, and to quickly return them to normal operations and eliminate downtime.

Stop web-based threats in their tracks

Acronis stops web-based threats with our proprietary engine enhanced with industry-leading, third-party threat intelligence. We help an MSP to deliver comprehensive security services to their clients and support their efforts toward satisfying regulatory compliance. Acronis URL filtering lets service provider technicians control website access by using HTTP and HTTPS interceptors, managing exceptions for URLs and performing payload analysis.

Block any type of email attack in seconds

Acronis lets you deliver enhanced email protection to clients, blocking any type of email attack within seconds. Acronis lets you provision your clients' email security in minutes with no configuration changes via the same platform. Leverage our incident response service at no cost and effectively protect your clients against spam, phishing, business email compromise (BEC), spoofing, account takeover attempts, zero days, evasion techniques and advanced persistent threats (APTs).

Respond

How Acronis supports the NIST function

Acronis Cyber Protect Cloud simplifies incident response activities to ensure improved mean-time-to-respond (MTTR) cybersecurity incidents. Acronis offers cutting-edge capabilities to enhance the incident response process for your MSP, including swift incident prioritization and analysis, workload remediation and isolation, secure forensic backups and investigation through remote connection.

How Acronis helps

Leverage AI to get prioritized view across incidents

Acronis leverages AI to automatically correlate events and detect and prioritize security incidents — enabling an MSP to deliver enhanced protection to clients.

Completely outsource response and recovery if your IT team is strapped

With Acronis MDR, you have the option of fully outsourcing response and recovery to free up your IT professionals and enable them to focus on high priority initiatives.

Streamline incident analysis with guided interpretations

With Acronis EDR, incident analysis is streamlined with guided interpretations to make it more scalable for smaller teams. We've cut incident analysis times to just minutes with Acronis' AI-based interpretations of the attack chain in an easy-to-understand language that you can share with your clients, along with service provider technicians and other relevant parties.

Remediate threats and isolate endpoints

From containing the threat to collecting evidence and recovering, Acronis makes it easy to isolate endpoints and affected workloads — preventing lateral movement and other adversarial techniques used in cyberattacks. Get peace of mind knowing the impact of attacks are minimized, and remediate cyber incidents by killing malware processes, quarantining threats and rolling back changes.

Rapidly perform incident response with a single click

Acronis Cyber Protect Cloud gives you the flexibility to select the actions you want to take and respond in one click to deliver rapid response to clients. With easy, swift self-recovery that requires minimal IT intervention, an MSP can efficiently offload recovery to end users. Users can execute easy-to-follow, automated actions to contain threats, collect evidence and recover entire workloads and systems on demand.

Collect forensic backups

It can be challenging to maintain compliance for your clients, and running internal investigations can be costly. For most businesses, preserving forensic data is imperative to satisfying regulatory compliance and data protection laws. Acronis forensic backups simplify future analysis by collecting digital evidence, such as memory dumps, and helps you process information from disk-level backups. Acronis keeps your clients' key evidence securely backed up, so an MSP is equipped for future investigations — alleviating efforts and reducing costs.

Quickly remediate and investigate incidents with remote connection

Acronis helps you further remediate and investigate cyber incidents via a secure remote connection. Your MSP can remotely view the user's screen, provide white-glove support and guide specific tasks to fix issues. As an extension of your clients' team, Acronis enables an MSP to resolve issues faster, carry out further investigation and ensure your clients' business continuity.

Flexible reporting and report scheduling

Acronis EDR provides powerful reporting and flexible report scheduling through a single pane of glass, including active alert control, missing alerts, customizable dashboard widgets and more. Demonstrate your MSP's value through achieving faster operations and ease of renewals for your clients. With Acronis, an MSP is equipped to identify problems quickly, gain rapid access to management actions and swiftly report cybersecurity findings — internally or with clients. Reports are generated in XLS, PDF or CSV file formats. Acronis offers customized client executive summaries to drive strategic conversations with your clients and showcase the key performance metrics of your services with automated reporting.

Recover

How Acronis supports the NIST function

Leverage the best-in-industry recovery time objectives (RTOs) with Acronis Instant Restore. Acronis ensures your MSP can easily and efficiently restore your clients' assets and return them to normal operations after a cyberattack. Acronis Cyber Protect Cloud powers your MSP's delivery of reliable, timely and secure recovery to clients. Acronis fosters fast and holistic recovery to reduce the impact of cyber incidents, safeguard against reinfection and bring full-fledged recovery services to your clients.

How Acronis helps

Enable end users to recover faster and return to productivity

Acronis one-click recovery works with any backup location supported by the product and includes facilitating recovery passwords for enhanced security. In a single click, Acronis One-Click Mass Recovery restores your clients' data from a chosen backup point. In the case of large-scale incidents, an MSP is equipped to recover your clients' systems quickly — reducing downtime and cost.

Unlike mainstream security vendor solutions, Acronis Advanced Security + EDR, Advanced Security + XDR, and Acronis MDR empower you to recover your clients from cyber incidents with comprehensive solutions that ensure business continuity.

Automatically roll back ransomware attacks

Automatically roll back your clients from ransomware attacks with no manual effort required. With Acronis, automatic rollback is rapid — significantly minimizing the impact and potential damage of a ransomware event. Unlike traditional rollbacks, Acronis doesn't depend on the vulnerable Microsoft Volume Shadow Copy Service (VSS) copies that most ransomware targets.

Prevent the recovery of infected files

Ensure only clean data is restored on your clients' systems and workstations. Acronis restores your clients to a malware-free point, and the powerful anti-malware scans in Acronis Cloud find potential vulnerabilities and malware infections on full-disk backups in centralized locations — eliminating the risk of infected files being restored.

Perform attack-specific rollbacks

Acronis delivers attack-specific rollbacks that are a part of one-click recovery, helping your clients return to productivity faster. Following a cyber incident, Cyber Protect Cloud helps you recover files, reimage entire machines or failover to the cloud and keep infected machines for investigation and further recovery. Attack-specific rollbacks give an MSP flexibility, increase the speed of recovery and reduce data loss.

Ensure secure file- and image-level recovery

Acronis' best-of-breed file- and image-level recovery fortifies your defenses against ransomware.

Safeguard business continuity with preintegrated disaster recovery

With preintegrated disaster recovery (DR), you can protect your clients' critical organizational assets against data loss for true business continuity. Acronis' preintegrated disaster recovery includes support for all major hypervisors and operating systems, support for multiple networks and VPN-less deployment. Discover hybrid disaster recovery that helps an MSP run failover not only to the Acronis Cloud, but also to the MSP-managed infrastructure, which can be hosted on MSP premises or even on client premises.

Simplify cross-NIST security with cyber protection

Acronis delivers integrated cyber protection built with an MSP-focused mindset beyond combatting advanced threats. Our Cyber Protect Cloud solution leverages industry-leading technology to ensure your services are equipped to solve today's cyber protection challenges in precise alignment with the NIST Cybersecurity Framework. By enhancing your MSP's delivery of efficient cybersecurity and data protection in one solution, your service brings unmatched business continuity to clients without the complexity of juggling multiple tools. The ease of use and flexible management of the Acronis Cyber Protect Cloud solution seamlessly integrates with your security stack — giving you powerful insights into your clients' environments to enhance cybersecurity risk management and bolster cyber resilience.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate, and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com.

Acronis Cyber Protect Cloud empowers you to provide holistic protection across NIST

TRY NOW

REQUEST DEMO

Acronis

Learn more at
www.acronis.com