Acquire new business by implementing CIS Controls with **Acronis** for MSPs

Recruit new customers and increase average contract value with compliance-discovery and Acronis-powered cyber protection

CIS Controls provide a universal, practical and internationally recognized framework for organizations to govern their cyber protection measures. For managed service providers (MSPs), CIS Controls are a useful tool to discover customer compliance needs and gaps, and propose what services customers require across a wide range of legislations and industries.

With Acronis Cyber Protect Cloud, MSPs can now address many more CIS Controls and Safeguards in one platform. Rather than implementing and operating over seven disparate products and services, Acronis' natively integrated cyber protection enables MSPs to onboard customers and provision services more quickly, while operating at higher efficiency and lower cost.

UNLOCK OPPORTUNITIES

Identify compliance gaps to solve with managed cyber protection services.

CREATE BUDGETS

Justify that clients allocate budgets to mitigate risk of compliance breaches.

PROPOSE SERVICES

Create proposals with Safeguard gap analysis and service mapping.

IMPACT 15 OUT OF 18 CIS CONTROLS

Fully or partially facilitate, enable or validate 46 Safeguards across 15 Controls in one platform.

MAP COMPLIANCE STANDARDS WITH EASE

Understand and satisfy customer needs per regulatory frameworks like PCI DSS, HIPAA and GDPR.

MONITOR AND REPORT COMPLIANCE POSTURE

Leverage Acronis alerting and reporting GUIs and APIs to track status and breaches.

RECRUIT CUSTOMERS WITH ASSESSMENTS

Use compliance posture assessments as a tool to forge new customer relationships.

UPSELL WITH WHITE-SPACE ANALYSIS

Guide periodic business reviews with CIS Controls to identify customer needs and service opportunities.

ACTIVATE 7-IN-1 CYBER PROTECTION

Deliver backup, management, XDR, email security, DLP and file sync and share from one console.

IDENTIFY NECESSARY SECURITY MEASURES WITH REGULATORY AND INDUSTRY FRAMEWORKS

There are 18 CIS Controls subdivided into 153 Safeguards, organized into three Implementation Groups that cover more or less rigid security best practices. CIS Controls and Safeguards are also mapped, referenced and benchmarked against a wide variety of compliance frameworks such as NIST and FISMA, ISO/IEC, PCI DSS, HIPAA, GDPR, CMMC, Essential Eight and many more government or industry regulations. In addition, CIS Controls are often used by cyber insurance companies to determine the policy of underwriting, and are commonly referenced by governance, risk and compliance (GRC) tools. With CIS Controls, MSPs can identify what Safeguards each customer requires and assess which Safeguards must be enabled to comply.

IMPACT 15 OUT OF 18 CIS CONTROLS WITH A SINGLE PLATFORM

CIS Controls specify cyber protection measures and not any products to facilitate, implement or validate such measures. It can take dozens of tools and automations to meet the Safeguards of each Implementation Group. To contain complexity and cost, MSPs can impact 15 out of 18 CIS Controls with Acronis Cyber Protect Cloud. Acronis takes the heavy lifting and cost out of compliance by fully or partially facilitating, enabling or validating 46 out of 153 Safeguards in a single cyber protection platform.

SERVICE	CIS CONTROLS AND SAFEGUARDS *
Acronis Cyber Protect — Core	**1.1** – Establish and maintain detailed enterprise asset inventory. **1.2** – Address unauthorized assets. **1.3** – Utilize an active discovery tool. **1.5** – Use a passive asset discovery tool. **3.11** – Encrypt sensitive data at rest. **3.14** – Log sensitive data access. **4.5** – Implement and manage a firewall on end-user devices. **8.2** – Collect audit logs. **8.5** – Collect detailed audit logs. **8.12** – Collect service provider logs. **10.1** – Deploy and maintain anti-malware software. **10.3** – Disable autorun and autoplay for removable media. **10.6** – Centrally manage anti-malware software. **10.7** – Use behavior-based anti-malware software. **11.1** – Establish and maintain a data recovery process. **11.2** – Perform automated backups. **11.3** – Protect recovery data. **11.4** – Establish and maintain an isolated instance of recovery data. **11.5** – Test data recovery. **13.1** – Centralize security event alerting. **15.1** – Establish and maintain an inventory of service providers.
Acronis Advanced Backup	**3.11** – Encrypt sensitive data at rest.
Acronis Disaster Recovery	**3.14** – Log sensitive data access.
Acronis Management	**2.2** – Ensure authorized software is currently supported. **2.3** – Address unauthorized software. **2.5** – Allowlist authorized software. **2.6** – Allowlist authorized libraries. **2.7** – Allowlist authorized scripts. **4.1** – Establish and maintain a secure configuration process. **7.3** – Perform automated operating system patch management. **7.4** – Perform automated application patch management.
Acronis XDR	**4.11** – Enforce remote wipe capability on portable end-user devices. **9.3** – Maintain and enforce network-based URL filters. **10.1** – Deploy and maintain anti-malware software. **10.2** – Configure automatic anti-malware signature updates. **10.4** – Configure automatic anti-malware scanning of removable media. **10.5** – Enable anti-exploitation features. **10.6** – Centrally manage anti-malware software. **10.7** – Use behavior-based anti-malware software. **17.9** – Establish and maintain security incident thresholds.

SERVICE	CIS CONTROLS AND SAFEGUARDS *
Acronis DLP	**3.1** – Establish and maintain a data management process. **3.3** – Configure data access control lists. **3.7** – Establish and maintain a data classification scheme. **3.13** – Deploy a data loss prevention solution. **3.14** – Log sensitive data access.
Acronis Email Security	**9.6** – Block unnecessary file types. **9.7** – Deploy and maintain email server anti-malware protections.
Acronis File Sync and Share	**3.4** – Enforce data retention. **3.11** – Encrypt sensitive data at rest.

* Fully or partially facilitated, enabled or validated by Acronis Cyber Protect Cloud.

Acronis

Learn more at
www.acronis.com