Acronis Security Services

DEFEND AGAINST MODERN CYBERTHREATS

Data is now the world's most valuable resource. It empowers organizations to achieve their goals and, due to how vital it is for those organizations, it is targeted by cyberattacks that are growing in complexity and volume.

In response, organizations are utilizing more and more security solutions. However, today antiviruses miss 57% of attacks. Technology is no longer enough to stop cyberattacks. A broader approach to security is needed. In fact, every change to your IT infrastructure, such as the deployment of new business applications or BYOD devices or the utilization of cloud services, requires a security program review, as it might introduce new attack vectors.

The growing number of regulations that organizations face requires companies to establish privacy-centric processes or make mandatory security assessments. However, instilling keys skills and habits in all employees remains a priority: 47% of breaches are accounted to human error according to C-suites.

Cyberattacks are growing in sophistication and previously unseen malware strains are created and used every day. It's impossible to prevent every single attack, but organizations can detect it in time, limit the damage and potential losses, and take action to ensure the same exploit won't occur in the future.

ACRONIS SECURITY SERVICES

Acronis has been providing best-in-class cyber protection technologies for years. With the introduction of Acronis Security Services, Acronis provides a broader approach to cybersecurity. Our single-point-of-security offering now encompasses technology, people, and processes to solve today's safety, accessibility, privacy, authenticity, and security challenges within organizations of all sizes.

ACRONIS SECURITY SERVICES' BENEFITS

Security Assessment

- Improve organizational security posture
- Minimize remediation costs
- Meet industry regulatory requirements
- Align cybersecurity strategy and roadmap with business goals
- Gain clarity for IT investment decisions
- Get a remediation plan to mitigate risks

Security Awareness

- Increase personnel's readiness to meet cyberattacks
- Reduce the risk of human error
- Ensure compliance with regulations and established processes
- Reduce the number of security-related support calls

Incident response

- Ensure business continuity
- Limit the damage of security breaches
- Mitigate financial and reputational risks from cyberattacks
- Minimize system downtime

ACRONIS SECURITY ASSESSMENT SERVICE

Keep up with the growing regulatory compliance and rising digital threats. Review your security program, IT infrastructure, and prevention and detection controls to identify security gaps and vulnerabilities. Get recommendations by our cybersecurity experts to eliminate every attack vector to your data.

What you will get:

- Risk assessment – Evaluate your current security posture based on industry standards (e.g. NIST, ISO/IEC 27001). Assess your cybersecurity maturity and risk associated with third parties. Highlight security gaps that can lead to vulnerabilities.
- Vulnerability scanning – Proactively identify known weaknesses in networks, applications, and endpoints to limit the attack surface of your IT environment and ensure a secure software development lifecycle.
- Penetration testing – To identify network, mobile, web, and app attack vectors our cybersecurity professionals demonstrate how attacks are carried out and try to leverage exploits and bypass security controls to gain access to sensitive data.
- Social engineering – Evaluate employees' readiness to overcome cyberattacks from techniques like phishing that leverage human manipulation through email, phone calls, media drops, or physical access.
- Remediation – Get an executive summary along with detailed reports, including compliance, and a remediation plan for issue closure and risk mitigation based on the assessment techniques.

ACRONIS SECURITY AWARENESS TRAINING

Optimize your staff's effectiveness, mitigate various threats, including social engineering break-ins, and reduce any "read the book" delays through a security awareness training delivered by top cybersecurity professionals and tailored to your business needs.

What you will get:

- Role-based training – From basic to expert-level trainings for general employees, IT personnel, developers, and executives, including compliance training and modules designed to help prepare them for certifications such as CISSP, CEH, CCSK, etc.
- Versatile delivery options – Leverage more than 700 online modules or onsite training sessions tailored to the needs of your business and users.

ACRONIS INCIDENT RESPONSE SERVICES

Acronis' cybersecurity analysts and breach investigators deliver an instant reaction in the event of a security incident. You gain in-depth analysis via a comprehensive, holistic assessment of the environment and root-cause of the breach. A detailed remediation plan is provided, ensuring the proper actions are taken to recover and help your company manage regulatory requirements and any reputational damage.

What you will get:

- Identify damaged assets – Pinpoint damaged resources and uncover and analyze potentially damaged systems to understand the full scope of the breach.
- Business continuity – Isolate the threat to prevent it from spreading.
- Forensics – Analyze the root-cause and collect and preserve evidence such as use of HDD images, network traces, and memory dumps for follow-up investigations and court presence.
- Remediation report – Get a detailed report on the attack, including origin, hosts, application, malware analysis, and risk profile. A detailed roadmap will be planned and executed by our experts to ensure the incident is fully remediated. Recommended steps to prevent similar, future attacks are also provided as part of the report.
- Cost-efficiency – Convert unused Incident Response hours to other services on a yearly basis.

Acronis

Learn more at
www.acronis.com