

Detect and defend against the latest cyberthreats

From Schaffhausen, Switzerland, Acronis leads the world in cyber protection, solving safety, accessibility, privacy, authenticity, and security (SAPAS) challenges with innovative backup, security, disaster recovery, and enterprise file sync and share solutions that run in hybrid cloud environments: on-premises, in the cloud, or at the edge. In August 2021, the company released the Acronis Cyberthreats Report Mid-year 2021 update, an in-depth review of the cyberthreat trends the company's experts are tracking. "While the increase in attacks affects organizations of all sizes, something that's under-reported in the coverage of current cyberthreat trends is the impact on the small business community," explained Candid Wüest, Acronis VP of Cyber Protection Research in a press statement.

Data Points from the Acronis Cyberthreats Report Mid-year 2021:

- The average cost of a data breach was around \$3.56 million. The average ransomware payment rose 33% to more than \$100,000.
- 4 out of 5 organizations experienced a cybersecurity breach originating from a vulnerability in their third-party vendor ecosystem
- The most attacked countries in Q2 2021 were the U.S., Germany, and the U.K.
- 94% of malware is delivered by email
- Phishing emails increased by 62% from Q1 to Q2

Since its founding in 2003, Acronis has been a recognized leader in data protection. In response to the rise of cyberthreats targeting backup files, agents and software, the company introduced its innovative Acronis Active Protection anti-ransomware technology in 2016, making it the first data protection vendor to integrate a

native anti-ransomware defense in its backup solutions. That machine-intelligence- and behaviour-based detection technology has since been expanded to address all forms of malware and other potential cyberthreats.

Today, Acronis has more than 1,600 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams.

The company's flagship product, Acronis Cyber Protect Cloud, empowers service providers with integrated backup, disaster recovery, antivirus, anti-malware, email security, URL filtering services, and endpoint protection management capabilities – enabling them to deliver comprehensive cyber protection services to their clients.

The Acronis Cyberthreats Report Mid-year 2021 is based on examining attack and threat data collected by the company's global network of Acronis CPOCs, which monitor and research cyberthreats 24/7. Malware data was collected by more than 250,000 unique endpoints around the world running Acronis Cyber Protect (either as a client of an MSP using Acronis Cyber Protect Cloud or a business running Acronis Cyber Protect 15).

The full report provides in-depth insights into the top security/threat trends the CPOCs observed during the first half of 2021, a review of malware families and related statistics, a deep dive into ransomware's most dangerous groups, the vulnerabilities that contribute to successful attacks, and Acronis' security recommendations for the remainder of 2021 and beyond.

A copy of the full Acronis Cyberthreats Report Mid-year 2021 can be downloaded from the Acronis website as well as the new Acronis Cyber Protection Week 2022 <https://tinyurl.com/ytat4xs3>

Acronis

Website: www.acronis.com

Acronis Cyberthreats Report: Mid-year 2021

Cybersecurity trends in the first half of 2021 — The assault on data continues

