STASH®

Not Better Data Protection. Bona fide Data Protection

ACCOUNTANTS AND CONSULTANTS

Accounting and consulting firms are facing increasing external cyber attack as well as insider threats. They are seen as treasure troves by criminals, nation state actors, and even interested commercial parties who are attracted to the crown-jewel data with which firms are often entrusted. And often professional service firms are more lax on security than the corporations they represent. As the Panama Papers shows, even sophisticated firms can be hacked with devastating impacts on their reputations as trusted advisors to large companies or high net worth individuals with closely held secrets. The consequences of breach can be firm-destroying with massive financial and even political consequences for clients. The risk is as real for smaller firms as the largest.

"Rule 301 of the AICPA's Code of Professional Conduct requires that CPAs "shall not disclose any confidential client information without the specific consent of the client." Disclosure includes the loss of information to unauthorized individuals by malware, inadvertent disclosure, or other means. All CPA practice areas, including tax, audit, advisory, and other services, are affected by this ethics requirement, as well as by state and federal legal confidentiality requirements, because of practical considerations that entail the collection of massive amounts of confidential or private data."
– Cybersecurity Risks to CPA Firms, The CPA Journal

"It's not hard to see why accountants are vulnerable. First, they possess a trove of sensitive information about their clients—including Social Security numbers, birth dates, addresses and the names of family members. A hacker can easily use this information (and reconstruct passwords and answers to security questions) to gain access into the financial lives of individuals and inflict harm… As accountants increasingly expand beyond tax preparation into wealth management, the problem becomes even more pervasive."
– Accounting Today

"Similar to the old practice of keeping paper files under lock and key, partitioning of especially sensitive data should be practiced. Firms should have a data storage policy that only keeps documents on their main systems if necessary, then transferred to a more secure storage vehicle."
–Brandon Perry, Kennyhertz Perry quoted in Law Practice Today, American Bar Association

Whether you want to keep things to yourself or share with others, STASH delivers DSECaaS™ (data-security-as-a-service) to meet your needs. In a world of Open Networks and Bring Your Own Device, we focus on the crown jewels. On the data. On what really matters to your business.

STASH Data Protection for everyday valuable data and STASH HIBERNATE® for very long term data protection with data integrity for decades are the most impactful encryption and privacy Solutions ever developed to protect the actual data bytes themselves. STASH doesn't analyze, predict, try to defend, or react to data compromise after the fact like 99.99% of all other security options. When data is protected with STASH, it has a statistical probability of nil to breach, manipulation, loss, harm, or ransomware.

Data, network, and infrastructure agnostic, STASH is completely automated and simple to deploy, without changing anything about how you do business. Activated via SAAS, Secure Backup, & API.

AICPA | NIST | SOC 1 | SOC 2 | SOC 3 | ISO 27001 | Privacy Shield (Safe Harbor) | PCI- DSS | HIPAA

Digital Confetti® • Keys-on-the-Fly® • Data Integrity & Resilience for Decades • Cost Effective

+1 (844) 833-7373 Stash America LLC contact@stash.global