SHARDSECURE

SHARDSECURE INSIGHTS: KEEP YOUR ORGANIZATION SAFE ONLINE

October is Cybersecurity Awareness month. This year, the focus is on individual data security practices with an important theme: “It's easy to stay safe online.” As a CISA Cybersecurity Awareness Month Partner, ShardSecure is offering our own variation with four steps every business should take to stay safe online.

1 Get state-of-the-art encryption tools

First, companies should secure sensitive data by implementing encryption technologies. File-level encryption is a common choice for separation of duties between data owners and infrastructure providers in order to protect against unauthorized access. However, traditional file-level encryption technologies often introduce complexity, impact performance, and lack resilience. The ShardSecure platform offers an innovative, agentless approach to file-level encryption that provides data security and resilience without adding complexity or slowing performance.

.

2 Increase organizational awareness

Over 3 billion phishing emails are sent every day, with attacks costing $2.7 billion in the US alone last year. But phishing attacks are just one of many cyberthreats that employees can fall prey to. Team members can put your organization at risk by accidentally disclosing sensitive data, downloading malware, choosing weak login credentials, and much more.

To combat these threats, robust security awareness training is necessary. Experts recommend incorporating strong password practices, cybersecurity exercises, and ongoing education into your company’s culture to minimize risk. Check out our other infographic, Data Security for Non-IT Staff, for more detailed suggestions

.

3 Keep data private

Part of keeping your organization safe online is keeping sensitive data private. The financial costs of a data breach include reputational damage, loss of customer trust, loss of IP, and significant legal and regulatory fines. To mitigate these costs, companies should establish strong access controls and data processing policies, and they may consider data anonymization methods.

As a 2023 Gartner® Cool Vendor in Privacy, ShardSecure offers features to help organizations safeguard their intellectual property, prevent unauthorized access, and gain assurance that their sensitive data is well protected

.

4 Invest in regular monitoring

Cyberthreats are a year-round concern, which makes strong cybersecurity an ongoing process. Organizations should continuously monitor their networks for unauthorized access, and they should consider using advanced AI monitoring tools and intrusion detection systems to do so. Businesses should also regularly update and patch software and devices — particularly in sectors like manufacturing and healthcare, which often rely on vulnerable legacy technologies.

The ShardSecure platform enhances data privacy, security, and resilience for organizations of all sizes, safeguarding sensitive data and mitigating top cyberthreats. To learn more, visit our resources page or book a demo today.

Gartner Disclaimer

GARTNER is a registered trademark and service mark of Gartner and Cool Vendors is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.