NUCLEUS RESEARCH

PKWARE DELIVERS SECURE ENTERPRISE ENCRYPTION

ANALYST
Barbara Z. Peck, Trevor White

THE BOTTOM LINE

Traditional perimeter cybersecurity is obsolete and cannot protect sensitive enterprise data. The business value of persistent data security can be measured with increased efficiencies, reduction of errors from manual migration of data, and secure risk management. With the increased sophistication of cyber-attacks and growing user reliance on the internet, computers, wireless networks, data mobility, and smart devices, the risk for data breaches continues to grow. Nucleus found that cybersecurity is a primary business objective but less than 50 percent of the c-suite business leaders were confident that their company's data was truly secure.

•••

OVERVIEW

Old-style cybersecurity focused on building a "wall of protection" around a corporate network. Perimeter protection includes systems such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and virtual private networks (VPN) designed to protect a server, network, or host. Access to information is controlled with passwords or privileges to protect access to information from unauthorized parties. However, networks no longer have distinct borders and perimeter security has failed to keep pace with the advances in technology and has proved to be inadequate in preventing cyber intrusions. Data is no longer stagnant, crossing networks, applications, and smart appliances and persistent encryption, that remains with the data, whether at rest or in motion, makes stolen data unusable and is the most effective way to mitigate cybertheft,

PKWARE' s Smartcrypt platform is a persistent end-to-end encryption application that manages data at rest, as well as data in-motion. Smartcrypt data discovery and encryption can be incorporated into existing business processes, without the need for new infrastructure and without disrupting user workflows. It integrates intelligent data discovery with strong data-level encryption—and does it in the same workflow. PKWARE's Smartcrypt is the only data protection platform that keeps information secure across the entire organization. From mobile devices to mainframes, it protects sensitive data from internal and external threats.

PKWARE has announced a partnership with Boldon James, a leader in automated data classification, to integrate data discovery, automatic classification, and encryption key management. In conjunction with the Smartcrypt application, this partnership will add additional accuracy classifying data to reduce the risk of costly data breaches and increase corporate productivity. Using automatic classification to apply data protection processes and achieving data security is no longer an obstacle for an organization.

THE BENEFITS

The greatest threat to data security is the user – either through negligence or intent. Sensitive information protected at the data level with key encryption can prevent most data intrusions or threats, avoiding costs of repairing breaches and avoiding reputational risk from negative reporting. Smartcrypt can also reduce data bloat with PKWARE's compression technology that reduces data volume during the encryption process.

In speaking with end-users, Nucleus found that deployments of PKWARE are fast and require few internal resources. The initial setup tends to be both simple and relatively low-cost compared to traditional on-premise solutions for two reasons: PKWARE manages all the hardware and software, and users require minimal training. For cloud users, the platform provides similar benefits, without any hardware expenses. Persistent data level protection gives an organization control over its sensitive information from creation through deletion. The business value of key controlled persistent data encryption is demonstrated by increased productivity, reduction of data breaches, reduction of errors from manual migration of data, and secure risk management.

AUTOMATION

Automation is a key value driver for PKWare customers. Traditional style searching and categorizing could take a midsized business several months of labor hours. With PKWare however, an organization can run the solution overnight, and use the data

the next day. Nucleus calculated that a mid-sized business could cut its time down from over 200 labor hours to as few as 4 hours for review, a 5000 percent increase in productivity.

PKWare also allows customers to choose what they want to do when the data is discovered and classified. The end-user can choose whether they want the data to be automatically encrypted, moved to quarantine or whatever else the end-user chooses to script, such as data masking. This is particularly beneficial for mid-sized companies that do not have the technical infrastructure or staff to manage large data discovery, classification, and remediation. PKWare does not require any active involvement from the end-user, meaning that it can be run without the oversight of a security professional. This enables corporations to run the solution and focus on other tasks, a very "set-it-and-forget-it" system.

CONCLUSION

PKWARE's Smartcrypt delivers key encryption across an enterprise protecting sensitive information at the data level, wherever it is used, shared, or stored. The primary benefit of data encryption is that even if an organization is breached, the stolen data is unusable without the encryption key. Key management can be a challenge since the key must reside in a secure environment with strong management controls. Evolving regulations for sensitive data, such as personally identifiable information (PII), in union with the business's security guidelines can only be managed by persistent data level protection with key encryption. Perimeter protection cannot provide the level of security needed in today's regulatory and technology environment.