Strengthen Open-source Security in Times of Crisis

Most of 2020 was a tough year on many fronts. The global pandemic forced organizations to re-evaluate business models and embrace digital transformation to address macroeconomic uncertainties. Working from home became the new normal for many industries, with employers and workers adjusting to new ways of working. Students moved to online classes at all levels of the education system.

Cybercriminals have used these shifts as an opportunity. They've effectively ramped up activity and retooled their approaches. Experts predict that global losses from business-related cybercrime would hit a record $1 trillion in 2020. And an INTERPOL assessment shows a significant target shift to major corporations, governments, and critical infrastructure.

Pandemic-related security incidents have included a wide range of attack vectors. Examples include:

- Ransomware
- Credential phishing
- Denial of service (DoS) attacks
- Malicious attachments and links
- Business email compromise scams
- Fake landing pages

- Malicious downloaders

Cybercriminals are targeting infrastructure that hosts different types of sensitive data such as employee personally identifiable information (PII), corporate data/intellectual property, and customer information. In response, businesses are rapidly assessing the security of their infrastructure to ensure that they have adequate security measures in place.

Open-source Security

Open-source software is very popular and should be a key part of your security assessment. In a Red Hat survey, 95% of enterprise leaders indicated that open-source is strategically important to their infrastructure software strategy. Many organizations use open-source databases (such as MySQL and PostgreSQL) and NoSQL databases (such as MongoDB, Cassandra, and others). In recent years, organizations have used these databases for mission-critical production environments. For example, software-as-a-service providers leverage the technology to stay on the cutting edge. More traditional enterprises in finance, healthcare, and education use it to support analytics.

However, a recent Codemotion report highlights common open-source security issues and the importance of a "secure by design" strategy. Best practices including securing passwords, designing with least privilege, sanitizing inputs, avoiding misconfiguration, and adopting version control can address common security issues.

Storage also plays a critical role in enhancing data security. Security should be always-on, invisible to the user, and without performance impact or required management. Purity data services continuously protect data at rest with encryption that's built-in, always-on, and always in-line. There's no impact on performance, no administrative overhead, and no key management. Pure accomplishes this while providing impact-free, AES-256 data-at-rest encryption.

The Pure FlashArray™ platform is:

- Federal Information Processing Standards (FIPS) 140-2 certified
- National Institute of Standards and Technology (NIST) compliant
- National Information Assurance Partnership (NIAP)/Common Criteria validated
- Payment Card Industry Data Security Standard (PCI-DSS) compliant

Pure also helps streamline GDPR compliance and offers (in partnership with Thales) full pathway encryption with data reduction.

Ransomware Protection for Open Source

Protecting data against a ransomware attack is one of the biggest concerns of CIOs and CISOs. Using the Pure Storage Ransomware Assessment tool, you can assess your organization's risk and be better prepared to safeguard your backups from attack.

If you find that your systems are at risk, Pure FlashBlade® with SafeMode™ snapshots can help protect your data. SafeMode snapshots create immutable, read-only snapshots of backup data and associated metadata catalogs after a full backup. SafeMode snapshots are policy-based, so no one—from ransomware attackers to rogue admins—can delete, modify, or encrypt them. These space-efficient snapshots offer scalability as well as quick database recovery, cloning, and FlashArray's six nines of proven availability.

For example, building a MongoDB replica set in Amazon Web Services (AWS) is easy. Lock the file system on the MongoDB node, copy the Pure Cloud Block Store™ volume, and connect the new volume to the replica set node. Then, simply start MongoDB and join the node to the replica set. Recovery from a failed node is just as simple: Lock the file system on one of the secondaries, copy the Pure Cloud Block Store volume, and connect it to the recovered node. Recovery is quick and easy, with no performance impact, no database stoppage, and no lengthy data copy over the network.

Modern Secure Storage for Open-source Databases

Cybercriminals are quick to identify opportunities. And the pandemic provided them. Open-source databases have gained wide adoption and become targets for these criminals. Pure Storage® agile data services can help by delivering a Modern Data Experience™ that complements open-source security, so you can spend less time managing storage during this challenging time.

Check out our webinar with industry experts from DBTA to find out more about modern storage needs.