ACE DATA SECURITY WITH THESE 4 FUNDAMENTALS

WHAT IS DATA SECURITY?

Data security is an ongoing process that ensures your data is protected against cyber threats in all states—in use, at rest, and in motion. Get the basics of data security right, and reinforce your data security strategies to better protect your organization's data.

1 KNOW YOUR DATA

Getting to know your data is the first step in data security. Identify, locate, and classify data to focus your money and time on the most important files and folders.

TYPES OF DATA

BUSINESS-CRITICAL DATA:
If customer data like PII/ePHI, financial, or marketing information falls into wrong hands, it can destroy the business or its customers' privacy.

UNSTRUCTURED DATA:
Organizational files or folders that are unsystematically stored in random file systems—not classified according to security implications they might be subject to.

REDUNDANT, OBSOLETE OR TRIVIAL (ROT) DATA:
Duplicate files, outdated data, non-business files, and other junk data that takes up large amounts of disk space often adds to data storage costs.

Employ data discovery software to locate data in all these categories.

2 MANAGE YOUR DATA ENVIRONMENT

Are you keeping track of your data? Do you know which users have access to the data you hold? If you answered no, then it's time to change things up.

Track, control, and respond to unauthorized actions with your file system. Be on the constant lookout for suspicious file or user activities to spot potential threats promptly.

4.1 BILLION
Number of data records compromised in the first half of 2019 alone.

THE 3 PILLARS OF DATA MANAGEMENT

- Audit file systems
- Monitor user activity
- Track and control endpoints

3 SPOT HIDDEN FILE SECURITY RISKS

Discover and rectify permission hygiene issues, excessive privileges, and other vulnerabilities plaguing your sensitive data.

Provide appropriate protection to these sensitive files to prevent them being overexposed to malicious insiders or hackers. Use a data risk assessment tool to double check that your sensitive data is housed in a secure location.

$3.86 MILLION
Global average cost per data breach in 2020.

Companies that had open files with sensitive data in 2019.

4 PREPARE FOR CYBERSECURITY THREATS

Anticipate and plan for threats such as ransomware, phishing, and even insider attacks. A dependable data leak prevention tool can help safeguard your data from sudden attacks or breaches.

To safeguard organizational data, you need to block malicious activity at all fronts. Periodically review and refine your strategy, and strengthen your data security posture. Gauge and invest in the right tools to keep your data safe.

Healthcare organizations targeted by ransomware attacks in 2018.

HOW DATASECURITY PLUS CAN HELP SECURE YOUR DATA

DataSecurity Plus is a unified platform offering visibility and security into your data environment. Monitor and secure data and end-user activity to protect your files from malicious attacks.

- Make informed decisions on file security using file server auditing software.
- Identify files with security vulnerabilities by analyzing file permissions.
- Detect and quarantine potential ransomware attacks early on.
- Locate and classify sensitive data (PII/ePHI/PCI) to ensure data privacy of your clientele.
- Block unauthorized use of USB devices, and prevent data loss via peripheral ports.
- Ensure compliance to GDPR, HIPPA, SOX and other data privacy laws by verifying data classification requirements.

Explore the functions of DataSecurity Plus using a free, 30-day trial. Write to us at support@datasecurityplus.com.

Download it now

ManageEngine DataSecurity Plus

www.datasecurityplus.com