10 Critical Strategies For Data Breach Prevention

Breach protection and detection is an ever-evolving challenge for security experts. While there is no catch-all solution when it comes to protecting sensitive data, there are resources you can take advantage of to put your organization in a better position to prevent data breaches. Below are 10 things you can do to keep your organization protected.

1 Identify Crown Jewels

Classify data according to it's value and sensitivity to the organization. Employ security controls and protection measures.

2 Understand Your Data

Know where your data lives and how it is accessed. You can't protect your data if you don't know where it is stored.

3 Security Aware Culture

Security belongs to everyone, not just the IT team. Implement a security rewards program to encourage accountability organization-wide.

4 Ditch AV, Install EDR

Anti-virus is simplistic and limited in scope. EDR is more holistic. EDR not only includes antivirus, but also contains many other security tools like firewall.

5 Deception Technology

Provides a low-cost method of determining if an internal or external breach is in process.

6 Laws & Requirements

Provides guidelines and best practices based on organizations industry and type of data they maintain. Non-compliance can result in fines or a data breach.

7 Develop A Response Plan

A response plan avoids scrambling to understand and respond to a breach, which can lead to expensive mistakes.

8 24/7 Monitoring

Use employees and partners to employ 24/7 monitoring. This will improve your mean-time-to-respond.

9 Patch Management

Implement a systematic process for identifying vulnerabilities, testing and employing patches to defend IT assets.

10 Check Yourself

Protect your network by limiting admin privileges, update software, backup data frequently on the cloud, and use 2FA.

Free Threat Assessment!

Uncover security and data breach risks with a free threat assessment. Our team of highly skilled security experts leverage best-in-class technology conduct Threat Assessments that evaluate your organization's cybersecurity policies, vulnerabilities, and protective measures. We provide consultative analysis, including actionable remediation plans, to help you establish a secure infrastructure and appropriate defense systems.