

# Foundstone Data Protection Program

**Gain control over sensitive data, reduce the cost of data breaches, and achieve greater visibility into how data is used across your organization**

Some security experts say that there are only two types of companies: those that have been hacked and those that don't know they have been hacked. While it may be true that some of the largest security breaches involve very sophisticated criminals using advanced techniques, the painful reality is that data thieves only have to find one single exploitable opening.

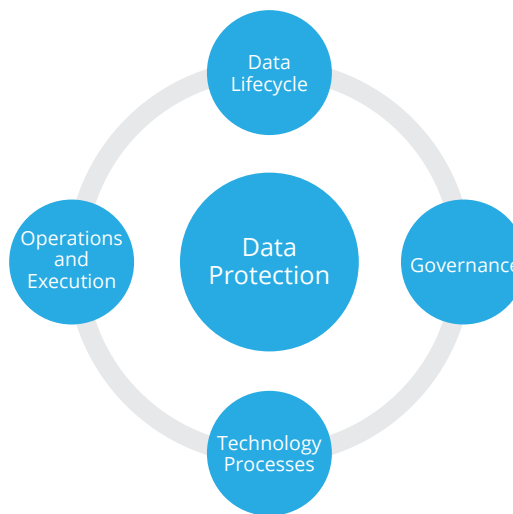
The cost of not deploying an effective data protection program can be catastrophic and lead to irreparable business reputation loss. Many breached organizations have learned this the hard way.

There is no better time than now to start a program to meet your data protection requirements in order to mitigate the risks associated with exposing customer data, losing intellectual property, or violating compliance obligations. Organizations are looking to data loss prevention (DLP) programs as part of a larger data protection strategy.

## Four Pillars of a Successful Program

The Foundstone® Data Protection Program is a comprehensive one, incorporating industry best practices and providing a standards-based holistic approach. It will enable your organization to successfully collaborate with internal and external teams, proactively

identify requirements and issues, set up processes for efficient operations, and transition to a mature and optimized state.



**Figure 1.** The four pillars of a holistic data protection program.

## Are you at risk?

The top common pitfalls for data protection:

- Lack of business involvement and leadership for data protection strategies
- Heavy reliance on technology to solve all data protection issues
- Lack of clarity on data protection priorities across the organization
- Not using a risk-based approach
- Absence of awareness and education programs
- Responsibilities and roles not defined and/or enforced
- False positives and unintended performance issues
- Misidentified or classified assets (lack of data ownership)
- A reactive approach to prior breaches
- Data boundaries extend to include partners and/or vendors

## DATA SHEET

### Data Lifecycle

Define data lifecycle elements that are critical to your organization. These can include:

- Business Units
- Business Systems and Applications
- Data Types
- Data Format and Structure
- Data Storage
- Data Flow
- Data Access
- Data Classification
- Data Retention
- Data Destruction

### Governance

Develop the governance framework for the program, which may include:

- Responsibility Assignment Matrix (RACI)
- Risk, Threat, Vulnerability, and Impact
- Data Protection Requirements
- Metrics and Reporting
- Enterprise Enablers

### Operations and Execution

Once a program is defined, it's important to focus on implementation phases and activities, including:

- Operations Model Alignment
- User Management
- Access Management
- Exception Management
- Support Strategy
- Monitoring
- Troubleshooting
- Incident Management
- End-User Communications
- Documentation Management
- Change, Configuration, and Release Management

### Technology Processes

Address key technology elements and processes, including:

- Evaluation Strategy
- Deployment Strategy
- Testing Methodology
- Performance Baseline Process
- Capacity Management
- Backup and Maintenance
- Disaster Recovery
- Business Continuity Planning

### The McAfee Difference

---

The McAfee® Professional Services team has a long history of working with clients across the globe, both as a technology partner to support our anti-malware, antispysware, and antivirus software solutions and also as a strategic advisor with product-agnostic, program-level engagements. Our teams of security experts assess network vulnerabilities, evaluate gaps in information security programs, offer strategies that meet compliance goals, and even help develop programs to prepare for security emergencies.

## DATA SHEET

### Scope

The scope of each engagement is custom fit to your organization's needs. A typical program includes one-on-one interviews with your key stakeholders, a thorough review of your current policies, directives, risk management program documentation, and information security governance materials.

All projects are managed using our proven Security Engagement Process (SEP) for PMI-based project management methodology. A pivotal aspect of this process is continual communication with your organization to ensure the success of our consulting engagements.

### Deliverables

The data loss prevention program report includes a detailed report and separate executive summary that includes the following areas:

- Strategic data protection roadmap customized to your organization
- Summary of prioritized findings and recommendations
- Trusted dedicated advisor during all phases to build or optimize the program

### Learn More

---

Fill the gaps in your information security program with trusted advice from the McAfee global professional services organization. We provide security consulting, customized product deployments, and training and advisory services. Our consultants can help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about integrating our services or visit [www.foundstone.com](http://www.foundstone.com) for more information.



2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo, and Foundstone are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 62314ds\_fs-dlp\_0516  
MAY 2016