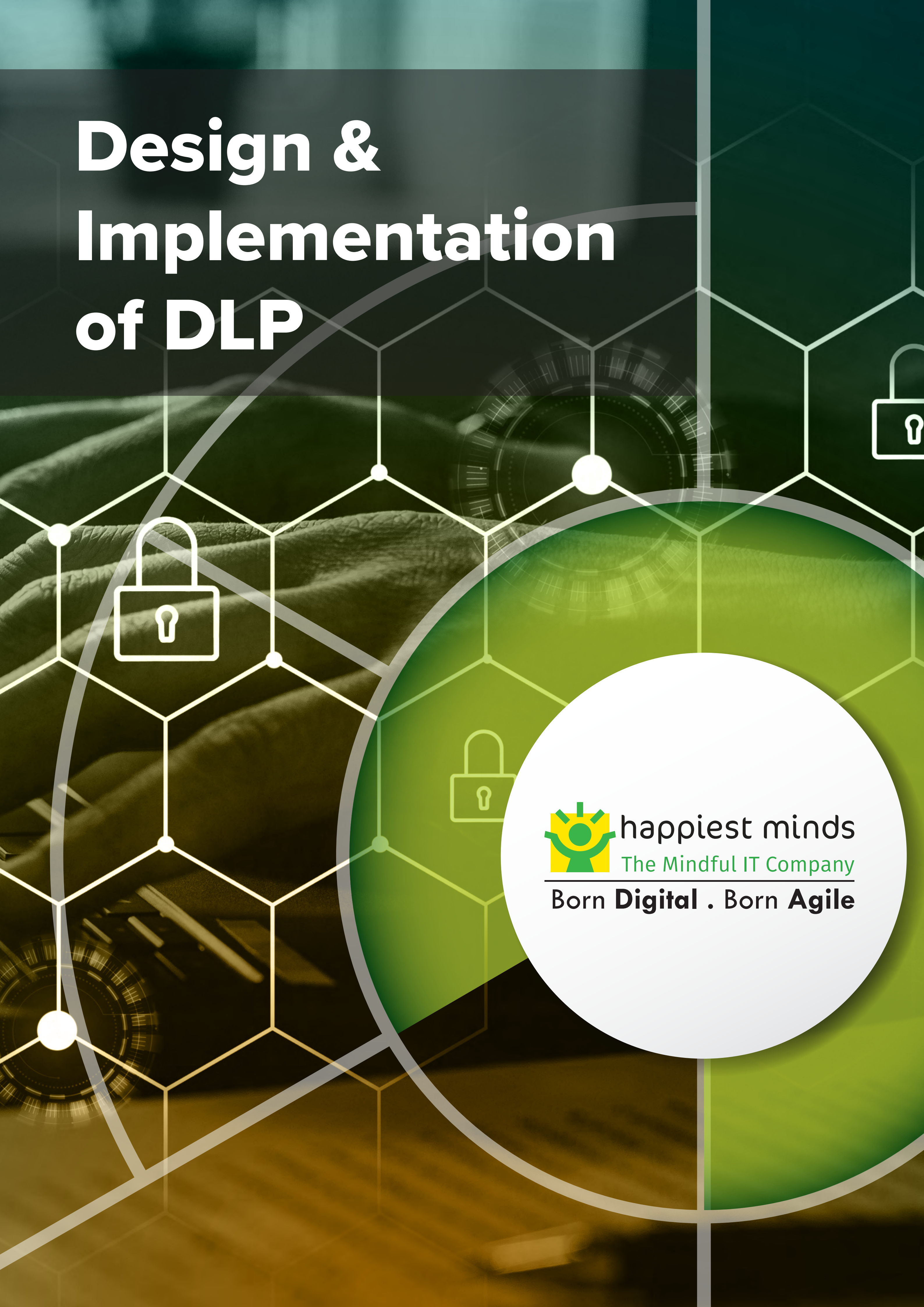
Design & Implementation of DLP



happiest minds

The Mindful IT Company

Born **Digital** . Born **Agile**

Introduction

Data is often stored, used, and exchanged inappropriately. It is exchanged inside and outside the organization with vendors, partners, end-users, consumers, etc. Data is stored in, and accessed from, databases, document repositories, file shares, end-user file systems, and portable storage. Therefore, data is vulnerable to leaks from various sources: it can leak over email, be posted to a website, be printed, or be stored inappropriately. Failure to implement controls to protect against accidental data loss and targeted attacks aimed at stealing sensitive may result in risks of non-compliance, fines, lawsuits, loss of competitive advantage, or damage to the brand and reputation. Customers thus need solutions that will protect their sensitive information.

The problem of Data or information leak is pertinent. 80-90% of all leaks are unintentional, requiring security protocols to be in place so that all functions and processes operate smoothly. The reasons for data leaks can be attributed to the following:

1. **Availability of data**
2. **Growing number of constituents**
3. **Protecting everyone's interests is complex**

This whitepaper provides you detailed information on how you can implement the right data protection to secure your sensitive data through DLP technology.

Before diving into the DLP technology, let us first understand the importance of data security and what are its key requirements.

Importance of Securing Data

Securing and protecting sensitive data is crucial to organizational success. Information leakage is becoming an absolute priority to customers for several reasons. What's important to understand is that data leakage is a business problem, not just an IT problem. And, to ensure business continuity, a foolproof data security plan is critical.

The key is to implement a technology solution that enables business processes (low negative impact) with a bifurcated strategy:

- Identify and fix broken business processes to stop the unintentional leaks – that's 80-90% of the problem solved
- Focus on the high-risk areas of the enterprise
- Outsource partnerships – account for 30% of all leaks

- High-value data
- Develop security and policy practices to secure your data
- Ensure controls map to both users, data, and vector
- Implement a means of mitigating that risk, including enforcement of both data and user policies that map to business processes
- Make the digital barrier high enough that you can deter and/or identify the intentional leaks by identifying the broken processes. You automatically reduce the risk of intentional leaks, employ a solution that helps you enforce and refine written policies, and empower the business units to become content-aware

What are the key Data Security requirements?

Accuracy

- Multiple Detection Techniques, Incl. Fingerprinting
- Natural Language Processing
- Detection Validation

Coverage

- Broad Array of Communication Channels
- Network and Endpoint
- Structured and Unstructured Data

Policy Framework

- Across Network and Endpoint
- Content, Context, and Destination Awareness
- Selective Enforcement

Management & Reporting

- Centralized Management and Reporting
- Built-in Policy Templates
- Automated Incident Remediation and Reporting

What is DLP?

Data Loss Prevention (DLP) is a computer security term referring to systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage). Through content inspection, contextual analysis of transactions (attributes of the originator, data object, medium, timing, recipient/destination, etc.), and a centralized management framework, DLP systems are designed to detect and prevent unauthorized use and transmission of confidential information.

Why do organizations require DLP?

Organizations process information that can often be classified as sensitive, either from a business or legal point of view. In addition to the risk of intrusion and gaining access to sensitive information by unauthorized persons, there is also the risk of intentional or unintentional transmission of intellectual property or other valuable information outside the organization. Many large companies now oversee government and commercial regulations that mandate controls over information, including HIPAA in health and benefits, GDPR, GLBA and Basel II in finance, and Payment Card Industry DSS standards. Some of these regulations stipulate regular information technology audits, where organizations can fail if they lack suitable IT security controls and due-processes standards. In addition to protecting data on remote cloud systems, DLP can help achieve data visibility in larger enterprises and enforce security in remote or Bring Your Own Device (BYOD) work environments.

DLP strategy for effective Data Protection

DLP solutions are an effective way to implement an organization's data protection strategy

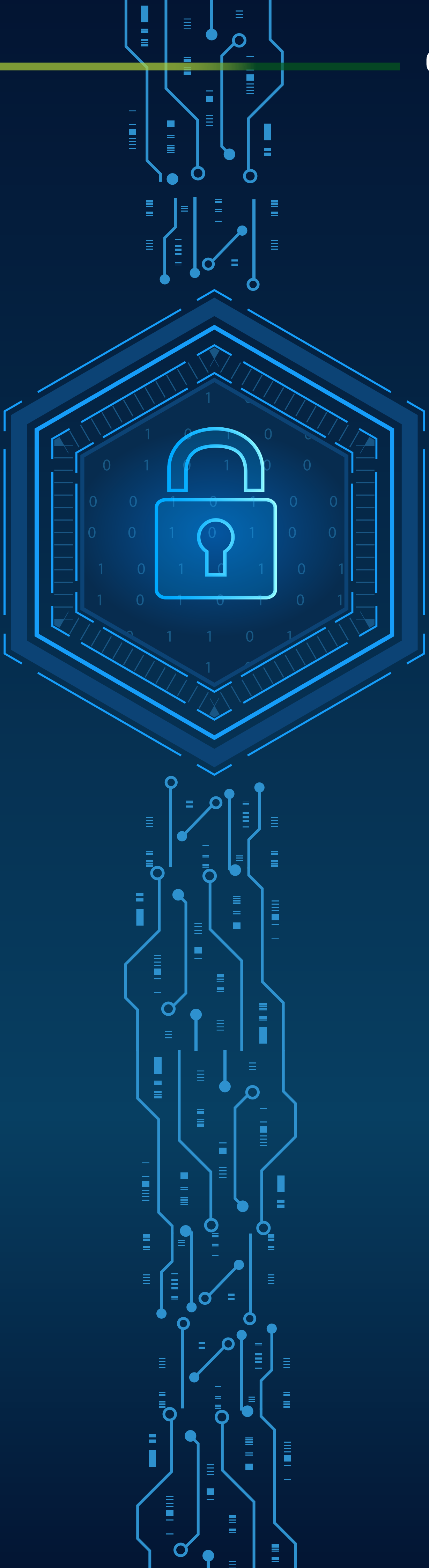
- Includes capabilities to discover, monitor, and protect information
- Includes data at rest, in use, and in motion
- For all types of data, even proprietary
- Content aware, user aware, regulation aware
- Policy controls and analysis and reporting

DLP Models

We need models to define/scope what a DLP system should perform, and a model is used to describe the technology in precise terms.

Three States of Data

- Data in Use (endpoints)
- Data in Motion (network)
- Data at Rest (storage)



DLP for Data in Use:

Emails, USB devices and endpoint channels (IM, FTP, HTTP/HTTPS & webmail) may lead to data leaks at endpoints.

DLP technology provides a secured channel by limiting user access to sensitive data that is actively being processed by an application or endpoint.

DLP for Data in Motion:

The data in motion may be compromised using these channels SMTP, FTP, HTTP, or HTTPS. DLP technologies are required when confidential data travels across a network to ensure that it is not sent outside the company or to unsecured storage locations. This step involves a lot of encryptions. Since so much business communication occurs over email, email security is particularly crucial.

DLP for Data at Rest:

Securing data is necessary even when it is not in use or motion. Data stored in various storage mediums, including the cloud, is protected by DLP systems. DLP can include controls to guarantee that only authorized people have access to the data and to track their access if it is stolen or leaked.

The primary DLP implementation architectures are Discovery, Network DLP, Endpoint DLP, and Cloud DLP. DLP is not solely a security-related choice.

DLP system & architecture

1. Discovery:

Discovery detects all the sensitive data connected to the organization.

- Scans all the devices and network that has stored confidential documents
- Logs what is discovered and sends a notification. It finds data at rest in the network.

It can scan data on file servers, databases, and content collaboration applications like Microsoft SharePoint.

2. Network DLP:

Network DLP is a technology for securing an organization's network, which includes Email, Web Applications, HTTP, HTTPS, FTP, SFTP, etc.

Email: All corporate emails will be using the On-premises Exchange Server or Cloud O365 to deliver the emails. We can prevent a data breach in the SMTP channel by integrating DLP Email gateways in the network.

WEB: Similarly, we can integrate the existing On-premises proxies/gateways into the DLP. The proxies analyze the data loss in web channels like HTTP, HTTPS, and FTP.

3. Endpoint DLP:

The Endpoint package/agents will be installed in the end-user device. The agent which is running on the end-user device contains policy information and will be monitoring for any sensitive data breach via Endpoint channels like Endpoint HTTP, Endpoint HTTPS, Cut, Copy, Paste, Endpoint Printing, Endpoint Applications, etc.

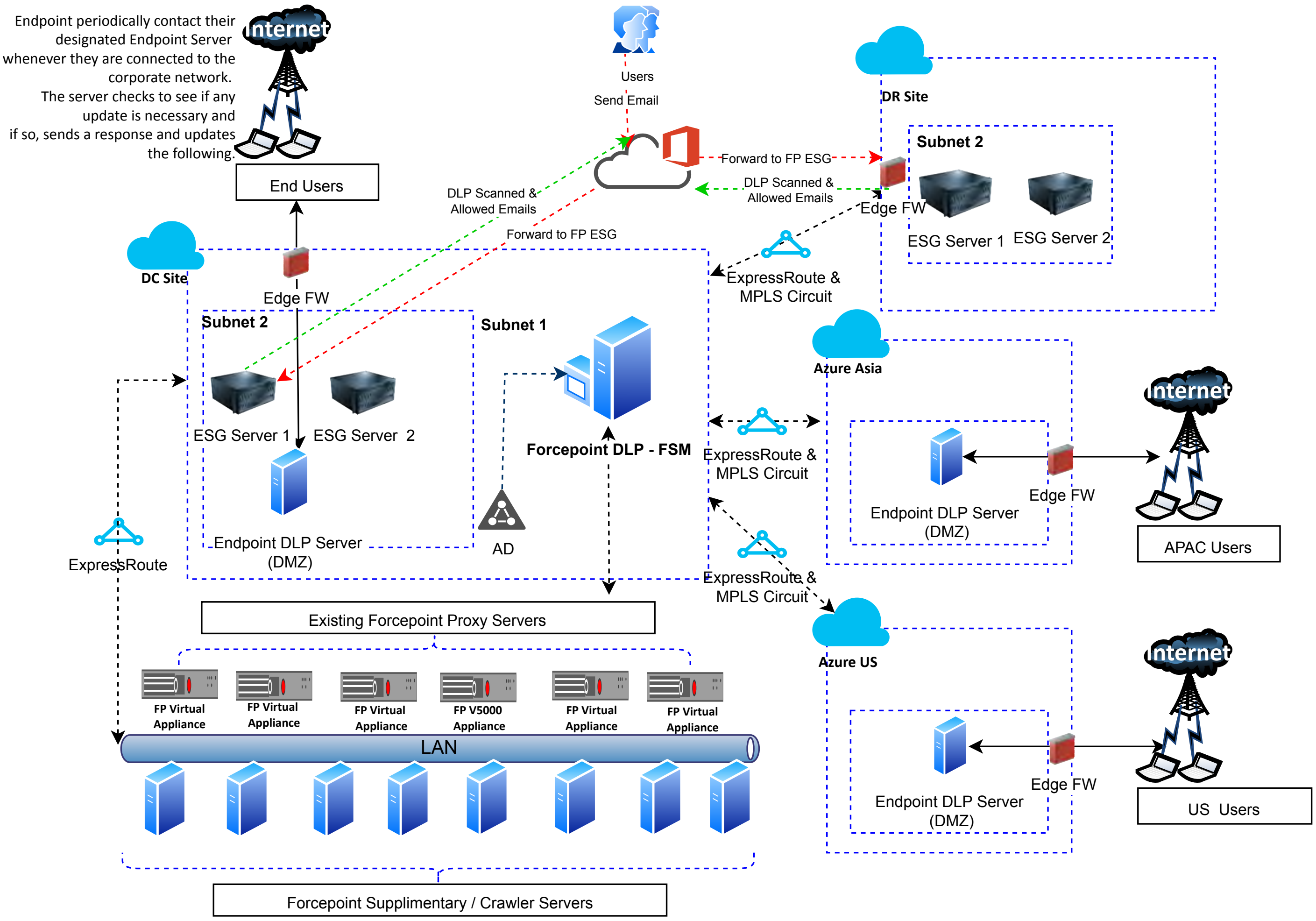
4. Cloud DLP:

Cloud data loss prevention (DLP) helps keep an organization's sensitive or critical information safe from insider threats and accidental exposure. Cloud DLP solutions provide visibility and protection for sen sitive data in SaaS and IaaS applications. Cloud DLP is a primary capability of a Cloud Access Security Broker (CASB). It's advanced analytics on cloud applications, offering protection against data threats such as

- Data movement across unmanaged Shadow
- IT Data stored in the public cloud
- Data movements across different cloud applications

Happiest Minds Play in Implementing Forcepoint DLP to a Critical Administrative Services and Information Management Company

FORCEPOINT ENDPOINT & EMAIL DLP ARCHITECTURE


Endpoint periodically contact their designated Endpoint Server whenever they are connected to the corporate network. The server checks to see if any update is necessary and if so, sends a response and updates the following.
Internet
End Users
Users
Send Email
DLP Scanned & Allowed Emails
Forward to FP ESG
Forward to FP ESG
DLP Scanned & Allowed Emails
DR Site
Subnet 2
Edge FW
ESG Server 1
ESG Server 2
ExpressRoute & MPLS Circuit
DC Site
Edge FW
Subnet 2
Subnet 1
ESG Server 1
ESG Server 2
Forcepoint DLP - FSM
Endpoint DLP Server (DMZ)
AD
ExpressRoute
ExpressRoute & MPLS Circuit
ExpressRoute & MPLS Circuit
Azure Asia
Endpoint DLP Server (DMZ)
Edge FW
Internet
APAC Users
Azure US
Endpoint DLP Server (DMZ)
Edge FW
Internet
US Users
Existing Forcepoint Proxy Servers
FP Virtual Appliance
FP Virtual Appliance
FP Virtual Appliance
FP V5000 Appliance
FP Virtual Appliance
FP Virtual Appliance
LAN
Forcepoint Supplimentary / Crawler Servers

Strategy & Objectives

- Prevent Data Loss from multiple channels (HTTP/HTTPS, Email, Endpoint HTTP/HTTPS, Removable media, and Printing)
- Integration of existing Proxies with DLP to analyze the data loss in HTTP and HTTPS channels
- Implementation of Azure Forcepoint ESG in HA mode to monitor the outbound emails
- Preventing sensitive data from being shared with unauthorized third parties

Solution

- Assessment of client network architecture & derived an architecture for Forcepoint DLP
- We have deployed Endpoint DLP and Network DLP in a very compact environment
- DLP deployment includes DSS sever, Endpoint servers, ESG, OCR, and Crawler server
- DLP setup, documentation & User acceptance of functional and operational tests
- Roll out of Forcepoint DLP agents to end-users and Email roll out to ESG
- Data-at-Rest enablement for file servers & databases

Key Enablers

- Enabled predefined policies for quick assessment & benefit realization
- Showcased discovery policies to enable scanning of sensitive data in the client network
- In-depth understanding of various tools, their applicability & quick rollouts
- A comprehensive, detailed & defined methodology
- Provided KT includes how to protect sensitive data at the element level with masking and encryption strategies

Value Delivered

- Enforced consistent DLP policies across all channels (Network, Endpoint, and Discovery)
- KT has been given to Incident Response Team to address High Priority incidents to deal with Breaches immediately. Also, how to differentiate between TP and FP incidents
- Helped the customer understand what types of sensitive data are being shared across all channels. KT has given on how to mitigate in later phases
- Helped the client to fix the latest log4j and XML attacks by upgrading the entire DLP setup from 8.8 to 8.9.1 post-implementation

Conclusion:

The DLP framework is compatible with all business types: Financial, Health care, Transport, Education, and other sectors. Enabling a proper policy framework is highly recommended. Apply the risk formula for data loss. Once your security team understands and applies the risk formula for data loss, it can collaborate with data owners to identify and prioritize data assets. In addition, every risk-mitigation activity should be designed to lower the rate of occurrence (RO) of data loss. RO is the proper measurement for tracking risk reduction and showing the ROI for DLP controls.

Author Bio

Manu B K is a Senior Engineer, IMSS at Happiest Minds Technologies. He has 6+ years of experience in Data Security, Proxy, and Email Security. He has worked as a Data Security, Web Security, Email Security Implementor, Consultant, and Administrator and has successfully delivered multiple projects on DLP, Email Security, and Proxy. Manu graduated from VTU, Belgaum University, and is a Certified Implementor and Administrator in Forcepoint DLP, Web Security, and Email Security