GLOCO Enterprise Insider Threat Security Solution

PREPARED FOR

GLOCO MEDICAL DEVICES

PREPARED BY

Afraz Siddiqui | Brice Norton |

Sandra Dube | Matthew Cole | Paul Oehler

EXECUTIVE SUMMARY

GLOCO Medical is a growing medical device manufacturer based in Cambridge, Massachusetts. Although currently operating in the one campus location with 1500 employees. GLOCO's customers are primarily hospitals and insurance companies throughout the United States of America. GLOCO's enterprise system landscape is a combination of IT network and hardware platforms, several datastores, and enterprise ERP and CRM applications.

PROBLEM TO SOLVE: GLOCO's VP of Information Security was contacted by a well-respected white hat security researcher claiming that GLOCO's confidential company data was available on the dark web, a portion of the internet that requires specialized tools to access. According to the researcher, the exposed data comprised of GLOCO customer data and intellectual property data for GLOCO's medical device designs. This triggered an immediate investigation and audit of GLOCO enterprise applications and systems to verify the researcher's claims, determine if the breach or attack was still ongoing, and attempt to identify the external threat. The internal security team confirmed the data loss, however, their findings pointed to an insider threat having carried out the data exfiltration. Law enforcement was immediately called in to investigate. It was clear that GLOCO had a serious data loss problem.

GLOCO's VP of Information Security brought in an external team to improve the company's internal security posture. ProTech_t Security Consulting, a highly specialized security team was hired to provide a solution that will detect and prevent data loss incidents caused by internal threats. ProTech_t Security Consulting has been in business for over 10 years and specializes in insider threat security investigations and solutions. The overall goal of the project is improving GLOCO's internal data security posture. ProTech_t Security Consulting proposes a Data Loss Prevention solution and updating GLOCO's current security processes and policies to achieve operational efficiency.

PART 1: Business Requirements

1.1 BUSINESS OBJECTIVES

- Improve GLOCO's security posture against internal threats
- Improve internal security processes
- Minimize risk to the business and reduce operational costs

1.2 BUSINESS CONTEXT

GLOCO's recent security audit revealed that while they have sufficient capabilities in place to mitigate external threats, they are lacking the appropriate measures to prevent and react to a data loss event from an inside threat. Unfortunately, the security audit was unable to identify the exact source of the recent security incident, which reiterates the need for a Data Loss Prevention (DLP) solution. Employees are lacking in the awareness of how to identify and protect sensitive information. They also do not have the proper tools to work efficiently while maintaining the security of GLOCO's customer, partner and intellectual property data.

To prevent data loss in the future ProTech_t has the following recommendations for GLOCO:

1. Implementing DLP at the network layer. This is the most comprehensive and least intrusive measure to implement. This allows sensitive data to be monitored and reported as it travels through the network.
2. Deploying a DLP endpoint solution. This prevents employees from sending sensitive data from GLOCO devices to non-approved locations as well as restricts the ability to save data to non-company approved devices, such as thumb drives.
3. ProTech_t will propose the creation of an Incident Response Team, whose focus will be the monitoring and response to security events as they happen.

1.3 USER STORIES

The result of the DLP implementation will focus on three facets.

1. Network Control
2. Saving Permissions
3. Security Team Response

USER STORY 1: ***As an employee I should not be able to send any sensitive data outside of the company.***

Without any data loss prevention hardware or software environment, employees have complete freedom to misuse accessible company data. While good faith operating assumptions can be made for all levels of employees, a more aggressive approach is necessary to mitigate internally originating data loss and risk. Without a DLP solution, employees can easily send and receive all types of data – sensitive or not – out of GLOCO without warning or detection. Additionally, employees can currently utilize the GLOCO network to use protocols such as (S)FTP and HTTP(S) to directly upload files, folders, and archives to remote unsecured locations. To flag, mitigate, and prevent this type of activity – accidental or intentional – a network layer DLP appliance should be installed. This hardware appliance will sit at the outer edge of the corporate network and detect sensitive information leaving the company's network. Once the DLP appliance is in place, an employee attempting to send sensitive data will trigger a response from the security team. In addition to installing a DLP appliance, a DLP management console will also be installed. This management component will allow GLOCO's security team to actively update DLP protocols and models as needed, as well as track trends and see alarms raised by inappropriate data usage.

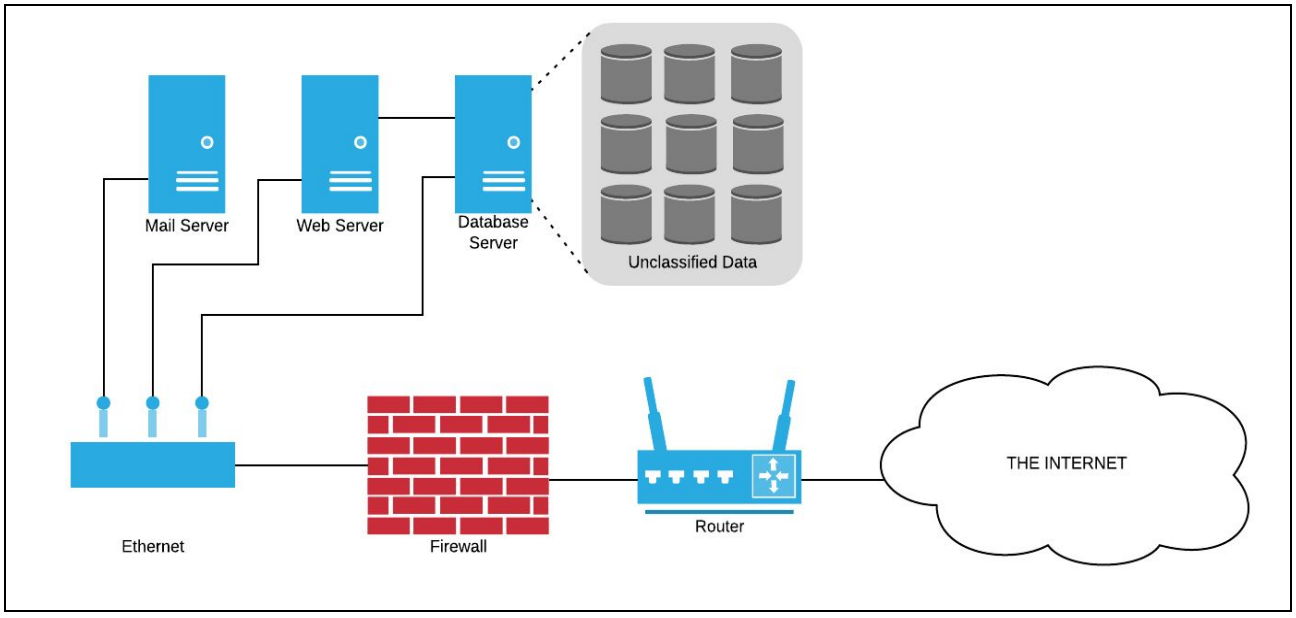

Figure 1. GLOCO Corporate Network (As-Is)

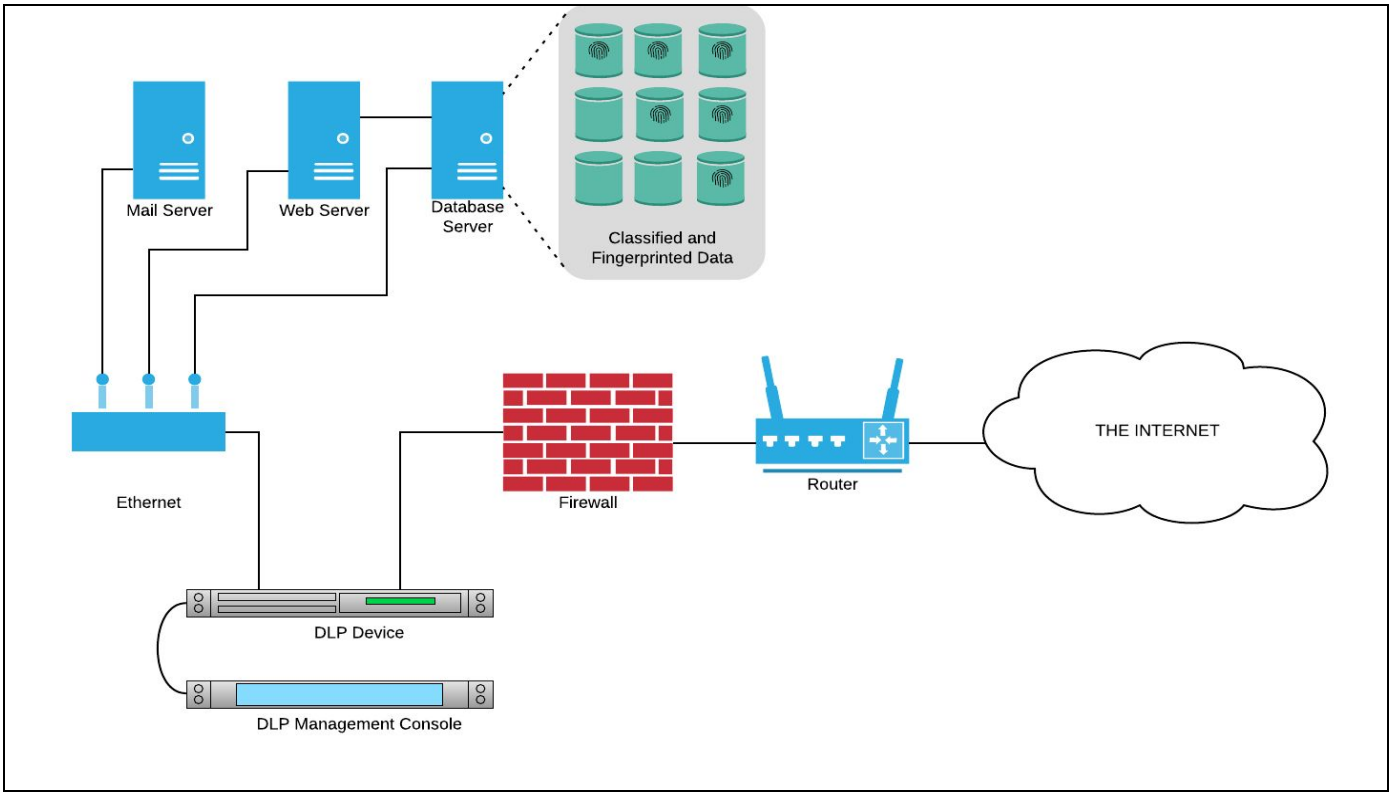

Figure 2. GLOCO Corporate Network (To-Be)

USER STORY 2: ***As an employee I should not be able to save any sensitive GLOCO data on non GLOCO approved equipment.***

Currently, employees can bring their own drives and hardware, saving sensitive data directly off the network and on to external drives. To ensure that data does not leak via hardware that comes in the front door of GLOCO facilities, it is imperative to employ endpoint DLP and issue corporate hardware. Endpoint DLP will serve the same purpose as the DLP appliance on the network, however, it will do so for files being written to the drive. Rather than warning and catching sensitive outbound data, as employed on the network, the endpoint DLP will enforce stricter file saving and copying procedures. All GLOCO issued desktops and laptops will have endpoint DLP installed on them. GLOCO issued external USB drives will be registered and encrypted to allow employees to copy data to them. This will ensure that data can't be copied from a GLOCO device onto a non-GLOCO device or USB drive. GLOCO will not be supporting a BYOD program at this time.

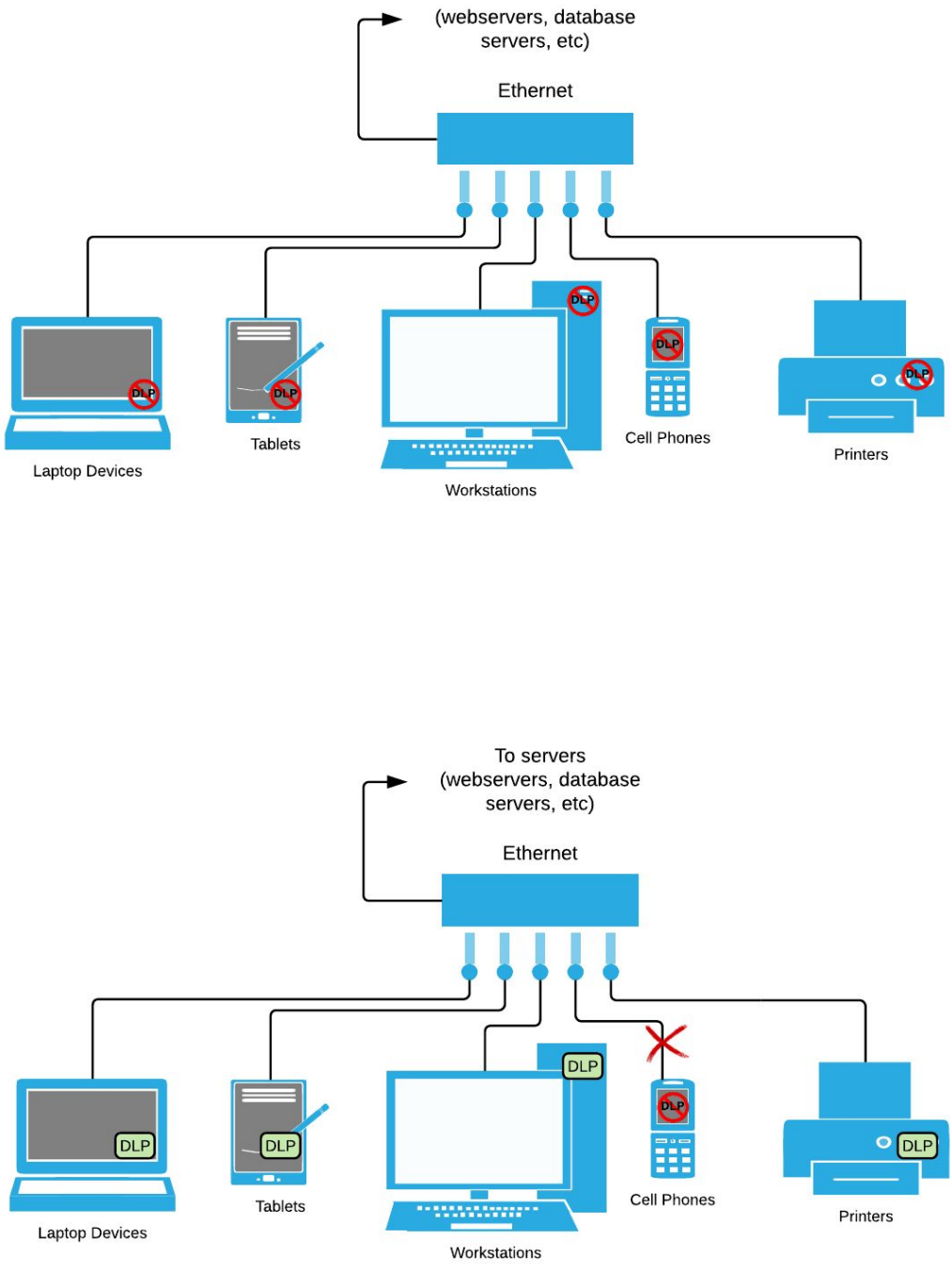

Figure 3. GLOCO Network Configuration (As-Is) and (To-Be)

USER STORY 3: ***As a member of the Security Incident Response Team I should be able to quickly anticipate, identify, and respond to internal application/system anomalies.***

Currently, GLOCO does not have a dedicated incident response team within the security team. Integrating DLP solutions and aggregating threats, trends, and anticipated warnings will help shift the security team's mindset from reactive to proactive. It is vital to setup a dedicated incident response team and deploy a security monitoring dashboard to quickly anticipate, identify, and respond to breaches and leaks. The dashboard will offer real time activity feeds of employee interaction with DLP equipped environments. All externally routed messages will be checked, flagged, and caught in a repository viewable in this dashboard. In addition, repeat violators, systematic trends, and DLP based issues – such as false positives – can and will be identified here. Lastly, the dashboard will fully integrate with the network based DLP Management appliance for streamlined changes and updates.

1.4 FUNCTIONAL REQUIREMENTS

Table 1.4 Functional Requirements

Epic	User Story		Acceptance Criteria
Insider Threat Assessment	U1.1	As an employee I should not be able to send any sensitive data outside of the company.	• Block data that has been classified as sensitive from leaving the network. • User should be notified that they cannot transmit data in this manner and that the security team has been notified.
	U1.2	As a security team member, I should be informed if an employee attempts to transmit sensitive data outside of the company network.	• Receive an alert from the DLP device if an employee attempts to transmit sensitive data outside of the network.
	U1.3	As a member of the security team, I should be able to see flagged sensitive data transmitted on the GLOCO network.	• All data in motion on the network should be inspected. • Sensitive data should be disallowed from leaving the network.
	U2.1	As an employee I should not be able to copy sensitive data to a non-approved external hard drive or USB thumb drive.	• Block data that has been classified as sensitive from being copied to non-GLOCO devices. • User should be notified that they cannot copy data in this manner and that the security team has been notified.
	U2.2	As a security team member, I should be informed if someone attempts to copy data to a non-approved device.	• Receive an alert from the DLP device if an employee attempts to copy data to a non-GLOCO device.
	U2.3	As a member of the security team, I should be able to apply	• Data at rest or in use should be encrypted.

		encryption and inventory encrypted and unencrypted data saved on the GLOCO network.	• GLOCO approved external devices should be encrypted. • Encrypted data should not be allowed to be copied to a non-GLOCO approved device.
Data Classification & Fingerprinting	U3.1	As a manager I should be able to flag data that I am responsible for as sensitive.	• A tool should allow management to flag or classify data as sensitive. • Provide granularity based on departments,roles and permissions.
	U3.2	As a security team member, I should be able to fingerprint databases for security purposes.	• Fingerprint databases and data for sensitive information. • Have the ability to see which databases are not fingerprinted yet.

1.5 NON-FUNCTIONAL REQUIREMENTS

Table 1.5 Non-Functional Requirements

Epic	User Story		Acceptance Criteria
Capacity	1	As a security officer the solution must be able to process a large volume of concurrent requests in a timely manner.	• There should be minimal degradation in network performance. • Solution must support up to 20,000 concurrent sessions.
Usability	2	As a security office, the solution must be configurable and accessible by security staff.	• Ability to view current network status. • Ability to create customized dashboards.
Performance	3	As a security officer, the solution must be able to timely identify and process threats and non-threats.	• All network data must pass through the DLP appliance quickly. • An alert should be sent to the Incident Response team within 30 seconds of threat detection. • Non-threats should be processed and allowed to leave the network within 30 seconds.
Scalability	4	As a security officer, the solution must be able to grow and support expanding systems, networks, endpoint devices, and processes.	• Solution should be able to support future growth including new physical site locations. • Solution must support up to 20, 000 endpoints.
Cost Reduction	5	As a security officer, I should see a reduction in the cost of an insider threat incident.	• Reduce the cost of insider threats by at least 20%.

1.6 BUSINESS BENEFIT JUSTIFICATION

Preventing insider threats does not generate revenue directly, but instead prevents losses that could be much more extensive than the cost of setting up and maintaining a good DLP system. Intellectual property and company data need to be safeguarded to maintain an edge over the competition. Looking at the cost of a data leak and comparing it to the cost of a DLP solution is the best way for us to determine the value of such a system.

According to a study done in 2016 by the Ponemon Institute, 68% of all insider incidents are due to employee negligence, not malicious intent. This can be an employee who accidentally forwards an email to the wrong person or attaches the wrong file when sending something outside of the company. These cases of negligence cost companies an average of nearly $207,000 per incident. Additionally, criminal or malicious insider breaches account for another 22% of incidents, which can include a disgruntled employee releasing or e-mailing data outside of the company on purpose. Incidents like this cost companies an average of $347,000 each, a 68% increase over employee negligence. Finally, the last 10% of incidents are credential thieves, which can be an outsider attacker who gets an internal employee's account information through methods such as phishing. These are the costliest attacks, since they are premeditated, and cost companies on average $493,000 per incident, a 138% increase over employee negligence and a 42% increase over malicious breaches.

These costs are also averaged across different size companies, but larger companies will pay much more. Companies with more than 75,000 employees could pay over $7 million per incident. Also, since negligence is the largest segment of threats, even though they cost the least, they will on average account for the largest amount of financial damage to a company. Using the averages stated previously, annualized costs for employee negligence average nearly $2.3 million. Companies in the Industrial and Manufacturing sector, which GLOCO is part of, experienced an average of $5 million in costs per year due to these insider breaches. Minimizing the damage caused by these types of threats is the goal of this proposal.

Data loss prevention tools are one of the methods for reducing risk and preventing data leaks. According to Ponemon, on average, companies that employ DLP tools and solutions find a reduction of 16.3% to the costs associated with insider threats. This is just one tool that can be used but will be layered within other tools and processes. Mandatory employee training on insider threats can reduce costs by 7%. User behavior analytics can reduce costs by nearly 26%. Threat intelligence systems can reduce costs by nearly 19%. Combining these different techniques can provide a much stronger system and mitigate the risks of insider threats and data leaks at GLOCO.

PART 2:TECHNICAL SPECIFICATION

2.1 Architecture Overview

Protech_t Security Consulting proposes a customized insider threat technical solution to be deployed on-premise and consists of the following vendor components:

1. Digital Guardian Network Appliance
2. Digital Guardian Endpoint Agents
3. Digital Guardian Management Console
4. Symantec SSL Visibility Appliance

GLOCO systems to be protected by insider threat solution are:

1. IPv4 Network TCP/IP Protocols - HTTP/HTTPS, FTP/SFTP, SMTP
2. Compute & Storage Hardware - Physical & Virtual servers, SAN storage
3. Enterprise Applications - ERP (Employee data), Sales (CRM) and Marketing Portals
4. Clients/Endpoints - Desktops, laptops, network printers

2.2 Vendor Selection

Gartner's 2017 Magic Quadrant for Enterprise Data Loss Prevention (DLP) cites Forcepoint, Symantec and Digital Guardian as the market leaders in enterprise DLP solutions. These three vendors were considered in the vendor review process based on GLOCO's data security requirements, integration with existing enterprise systems and costs. Digital Guardian is the best fit due to the product's capabilities, cost, and ease of integration.

DLP Vendor Comparison

Table 2.2.1 DLP Vendor Comparison

GLOCO On Premise DLP Requirements	Vendor		
	ForcePoint DLP	Symantec DLP	Digital Guardian DLP
User & Entity Behavior Analytics - Risk warnings and threat detection	Yes	Yes	Yes
Automatic content and context data classification and user based (manual) data classification and engine training	Yes	Yes	Yes
Data discovery and classification support for Structured (databases), Unstructured (documents), Binary (non-textual files)	Yes	Yes	Yes
Sensitive Data in transit on the network should be inspected /protected with encryption (network DLP)	Yes	Yes	Yes

Sensitive Data in use should be inspected/protected with encryption (network and endpoint DLP)	Yes	Yes	Yes
Sensitive Data at rest should be inspected/protected with encryption	Yes	Yes	Yes
Alert and block sensitive data transmission violations	Yes	Yes	Yes
Alert and block sensitive data copy to unapproved hardware	**No**	Yes	Yes
Management console with ability to view dashboards	Yes	Yes	Yes
Integration with existing systems - SIEM (Splunk), LDAP, Email	**No**	**No**	Yes
Regulatory and Intellectual Property protection requirements (HIPAA, GDPR, PCI-DSS policies)	Yes	Yes	Yes

Digital Guardian's licensing model includes a perpetual software license for the on-premise appliance and up to 20,000 supported endpoints, with annual support and maintenance. Digital Guardian also offers a managed services option, which GLOCO could consider in the future to accommodate expansion.

Licensing costs & models

Table 2.2.2 Licensing costs & models

Component	ForcePoint	Symantec	Digital Guardian
Managed services option	No	No	Yes
Appliance, Software, Support & Maintenance costs (year 1)	$43,000	$65,000	$61,000
Appliance, Software, Support & Maintenance costs (year 2)	$21,000	$22,000	$11,000
Projected Total Costs (implement and service solution (2 year)	$64,000	$87,000	$72,000

Symantec SSL Visibility Appliance

While using SSL is a positive development for overall internet data privacy and secure communications, it means that any DLP implementation that cannot inspect TLS/SSL traffic is effectively useless. Symantec offers an appliance to mitigate this risk by securely inspecting TLS/SSL LAN traffic. Symantec SSL Visibility Appliance purchase and licensing costs are $30,000.

The overall purchasing cost of the insider threat solution is $100,000. No additional labor costs will be incurred as GLOCO's IT and Security teams will configure and deploy the solution.

2.3 Software/Hardware Solution

The insider threat solution offered by Digital Guardian consists of several components (see below).

Table 2.3 Software/Hardware Solution

Component	Hardware/Software	Functionality
Digital Guardian Network DLP Appliance	Hardware	Scans and Protects transport protocols: HTTP/HTTPS, FTP/SFTP, SMTP, etc.
Digital Guardian Endpoint DLP Software	Software	Access control, file encryption, removable media encryption, UEBA
Digital Guardian Management Console	Software	Set rules for network appliance and endpoint agents, generate reports
Symantec SSL Visibility Appliance	Hardware	Decrypts SSL/TLS encrypted network traffic on the fly

2.3.1 Digital Guardian Network DLP Appliance

Network security will be handled by the Digital Guardian network appliance installed into the GLOCO network stack to provide DLP for all network traffic. False positives will be minimized by fingerprinting all file types. The Database Record Matching (DBRM) tool will target all file transfers attempting to transmit sensitive data outside of the network. The DBRM runs in the background and can scan and categorize structured data, like fields in a database, and unstructured data, such as a Word document. Email will also be monitored with the ability to specify keywords and rules for real time matching. A training set of data is supplied to the DBRM to help it learn what kinds of data are sensitive, and to help limit false positives. The DBRM scans the data and creates a hash using a mathematical algorithm to identify each instance of secure data. Then it can use that to scan the network for files containing this data and classify them. A classification tag is appended to the host file or email and can then be tracked as it moves throughout the network.

The network appliance uses a switch port analyzer to monitor all traffic and enforce policies. Policies come preconfigured to cover some specific data restrictions, such as PCI-DSS, PII, and PHI data. This includes e-mail (SMTP), web (HTTP/HTTPS), and file transfer protocol (FTP/SFTP). A single appliance can support all the needs of the GLOCO location where it will be installed. The device supports Lightweight Directory Access Protocol (LDAP) integration and communicates with GLOCO's existing Active Directory (AD) server. All traffic traversing the network is monitored using the permissions set within AD to allow or disallow file access. The appliance can handle IPv4 and IPv6 TCP/IP communication protocols and can work within multiple types of storage repositories and databases (see table below).

Table 2.3.1 Readable Storage Repositories

Readable Storage Repositories	
Windows CIFS & SMB	Oracle
NFS File Shares	DB2
MS SQL / MySQL	Sybase
PostgreSQL	Informix

Below is the current network architecture, followed by the proposed architecture with the DLP solution in place.

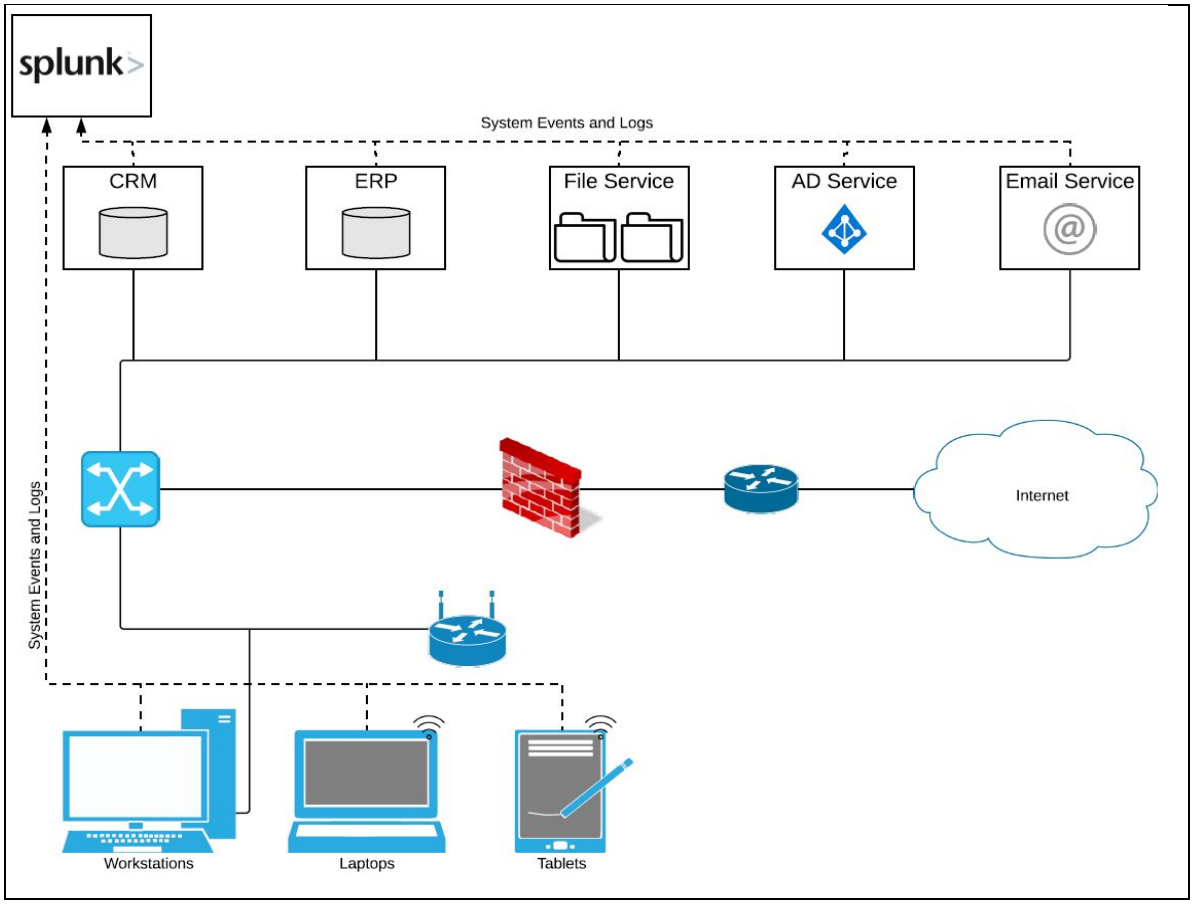

Figure 4. GLOCO Corporate Network and Service Layout (AS-IS)

2.3.2 Digital Guardian Endpoint DLP Agent

Endpoint security will be handled by software from Digital Guardian in the form of an Endpoint DLP Agent. It will be deployed using GLOCO's current software deployment solution, System Center Configuration Manager (SCCM), to all GLOCO owned devices. The software runs as a service in the background. Rules in the management console will allow the Endpoint DLP to be configured appropriately and fingerprint the data on all GLOCO devices. "Fingerprinting" is the process of creating a hash of sensitive data within a file and then appending that hash to the file. It helps the DLP software to classify and track the data. Access and permissions to data are granted by integrating the Endpoint DLP with the current permissions that users have in AD. Sensitive data are automatically tagged and can persist even if the data are copied to another file format, such as a screenshot of sensitive data being sent in picture format. Digital Guardian will tag the screenshot with the same classification as the data that was on the screen at the time. Actions taken can range from warnings to blocking the data entirely, depending once again on the rules that will be set in the console. This covers data that is attached to emails, transferred to removable hard drives, or uploaded to the web or FTP. Data can be logged, blocked, automatically encrypted, or require the user to submit justification to the security team prompting a manual override.

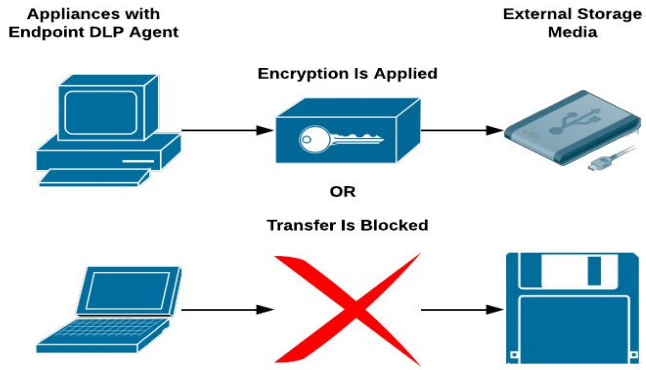

Figure 5. Enforcing Encryption on Removable Media

The User and Entity Behavior Analytics (UEBA) software is deployed as part the Endpoint DLP Agent, but it will be monitoring what users do on a normal basis and building a log of their normal activity. This will be used to track when an employee account or machine behavior deviates from the norm. UEBA software will alert the security team of this threat, which decreases the reaction time to respond to these issues.

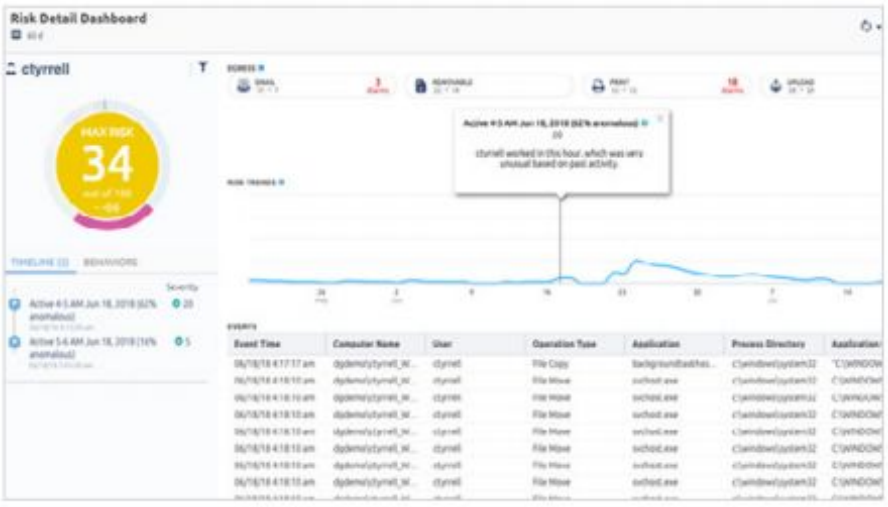

Figure 6. Example of a UEBA Risk Dashboard
(Courtesy of Digital Guardian)

2.3.3 Digital Guardian Management Console

The Digital Guardian Management Console (DGMC) will be deployed on a server running Microsoft SQL, which stores the system configuration including policies, rules, DMGC accounts, a registry of agents installed on endpoints, and events. The DGMC requires two databases: Collections and Reporting. The collections database stores daily event information, while the reporting database will store historical data for reports. The DGMC connects to the LDAP server, the DLP agents, the DLP network appliance, and the SMTP server for email notifications. The server that the DGMC is installed on requires Microsoft IIS, .NET Framework, and a copy of Windows Server 2008 or newer. We recommend Windows Server 2016. Separate dashboards can be configured for management and incident response security team.

2.3.4 Symantec SSL Visibility Appliance

GLOCO will utilize a dedicated appliance for TLS/SSL inspection purposes, the Symantec SSL Visibility Appliance.

Figure 7. The SSL Visibility Appliance model SV2800B. Symantec

The SSL Visibility Appliance is deployed as a "bump in the wire" and will be completely transparent to both end systems and intermediated networking elements. There is no need for network reconfiguration, IP addressing or topology changes. (SSL Visibility Appliance Administration & Deployment Guide)

The appliance can decrypt all types of SSL traffic, regardless of port, via deep-packet inspection. This is essential since data exfiltration typically occurs using non-standard ports. It is often as important to exclude traffic from decryption for privacy mandates. For example, sites classified as containing personal financial information or private healthcare information might need to be excluded from interception. This is achieved by configuration of rule sets within the appliance. The appliance comes with a pre-categorized list of websites for easy policy management.

Figure 8. Screenshot of pre-categorized list
Host categorization allows for easy configuration of TLS Inspection bypass to protect privacy, for example when employees access financial services or private health sites.

The Symantec SSL Visibility appliance contains all the tools GLOCO will need for implementing policy-based TLS interception with security best practices, including support for the latest TLS protocol TLSv1.3, and no degradation of end-to-end TLS security. The intercepted data will be redirected through the Digital Guardian network appliance unencrypted for scanning.

An added benefit of implementing the TLS interception via a dedicated device is that it allows GLOCO to add more security scanning solutions in the future without having to decrypt the data multiple times. For example, in addition to adding the Digital Guardian network DLP device to the flow of data, a IDS/IPS or passive forensic device could be added to the existing infrastructure with minimal impact.

2.4 Integration with existing systems at GLOCO

GLOCO currently uses Splunk Enterprise software for log analysis and monitoring of their web servers, database servers, and firewalls. GLOCO's IT team uses Splunk for problem and anomaly detection in existing systems with great success. Digital Guardian's event and alerts data will be sent to Splunk for inclusion in its powerful data analytics and search tools. This allows GLOCO's existing IT team to continue to use the familiar Splunk console for monitoring these new sources of data from DGMC, via the use of the Digital Guardian App for Splunk Enterprise.

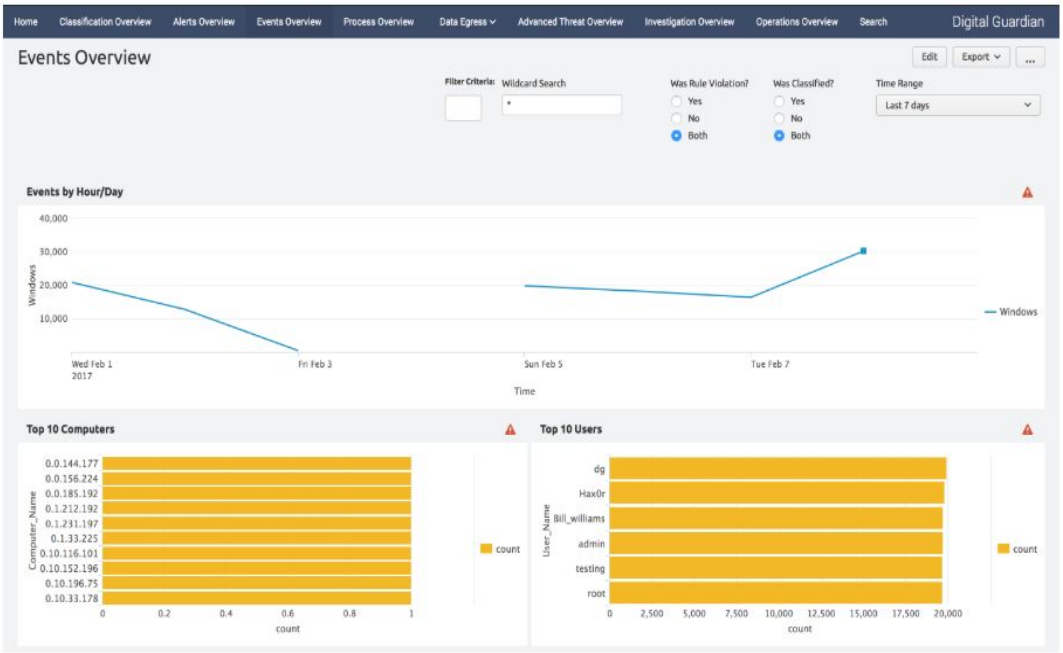

Figure 9. Digital Guardian app for Splunk
(Courtesy of Splunkbase)

2.5 Data Design and Management

Data management will encompass definitions of data entities, how and why they are stored, the extent of use, and how the data flows through the solution and other systems. The Digital Guardian DLP solution has three primary data entities:

Table 2.5 Data Design and Management

Data Entity Type	Description
User / Role Profiles	• Data sets that outline permissions for job function requirements • Allows DLP solution to understand hierarchical design of privileges • Includes: name, position, department, employee ID, and scope of work
Classifications	• Identification and sensitivity tagging of digital assets • Allows for controlled access rights (view, edit, manage) for that asset or asset group.
Logs / Archives	• Record all permission based – and DLP governed – access flows, profile changes, and trends. • Data that is collected includes: timestamps, actors, process, access levels, request, change orders, employee ID, IP addresses, MAC address, geolocation data, etc.

User Profiles: Includes employee record information, as well as privileges that will be added on these profiles by the employees themselves – to be approved by their hiring manager. Privileges are structured in three primary verbs on all assets or asset groups: View, Edit, Manage. Once a Profile has been created, privileges can be retroactively added or removed per the approval of immediate supervisors. These privileges, alongside the rest of a user profile, are saved in a dedicated DLP System of Records (SQL database) to ensure the further protection of the system.

Classifications: Includes asset tagging using pre-included flags. Examples of default tags are Low Priority, Moderate, Sensitive, Critical, and Common. These tags can be overridden by an organization's security team. Classification data drives the privileges that can be added to a user profile. Classification tagging is designed with a hierarchical access flow in mind, for example an asset cannot have contradictory classifications tags of being low sensitivity and critical. These classifications are to be added to all new assets, and retroactively added to existing assets. Classification tags can be applied to groups of assets; however, this will apply the classification on a file level basis as well to safeguard future movement and modification of assets. Like user profiles, classification data are stored in a dedicated database – DLP System of Records – to protect against tag modification attacks or injection attacks.

Logs and Archive: Data entities store all relevant information to employee behavior on all internal corporate systems and network. Logs are appended to any given user action. An example would be the requesting of an updated user privilege for an asset. The logs would not only record the previous and new access change, but also the requester and approver information. In addition, this example would result in recording new trends in the system. Logs will help to identify deviations of access rights and other peculiar occurrences for the sake of proactive DLP. Like the User Profiles and

Classification data, Logs and Archived activity will be stored in a dedicated database as well, accessible to only the security personnel in the organization.

Analysis tools, including artificial intelligence and machine learning scans, will be run on the System of Record containing the desired data set. These scans will result in patterns and trend identification that will be sent as periodic digests and/or immediate alerts to the security teams responsible for incident response.

2.5.1 Data Flow Diagram

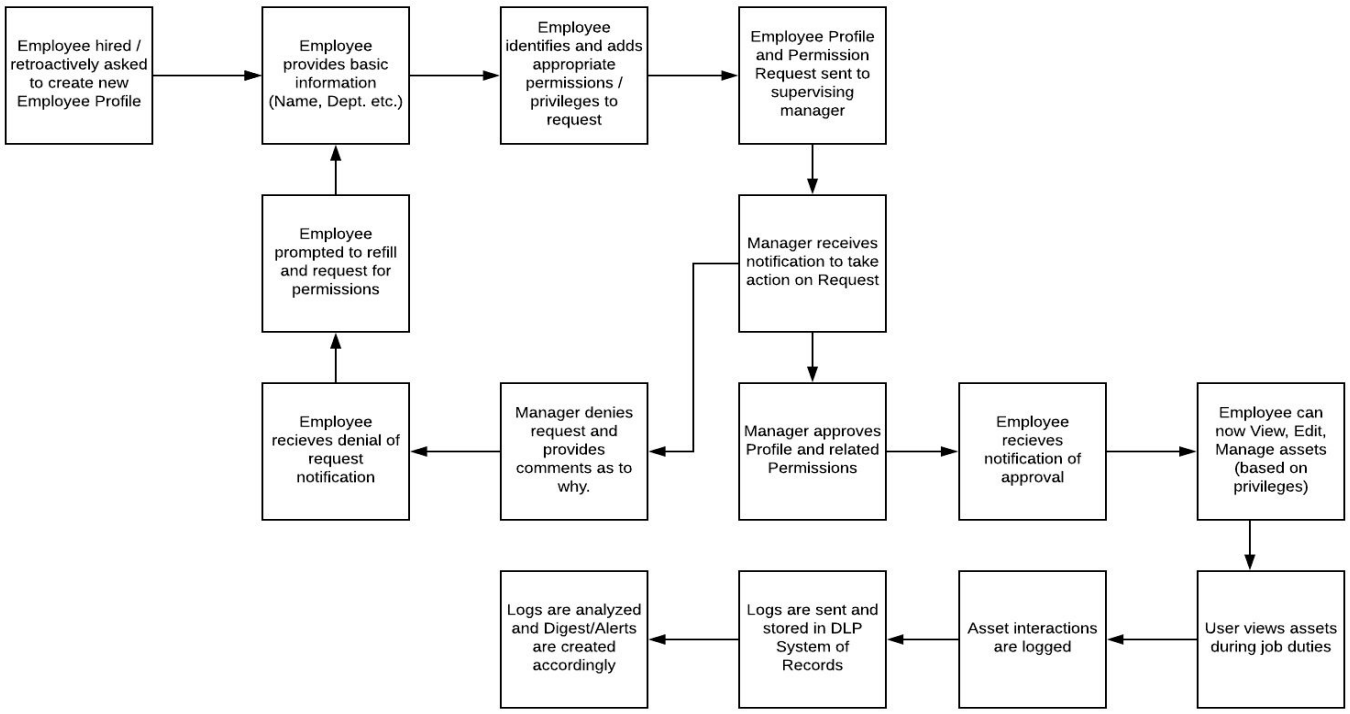

Figure 10. Data Flow Diagram

Creation of User/Role Profile for new hires/existing employees - in addition to logging of asset interactions.

2.6 Solution demonstration

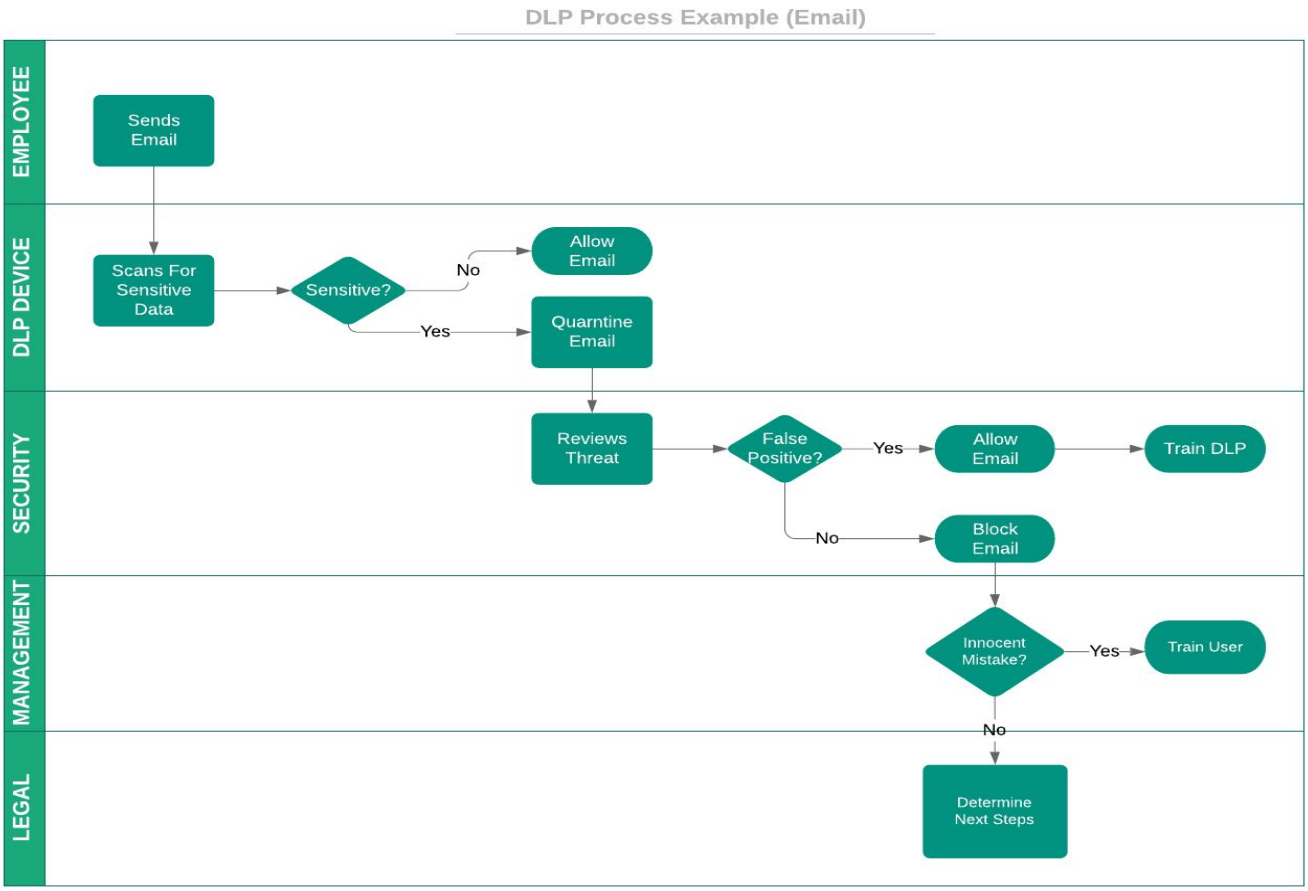

Figure 11. DLP Process Example (Email)

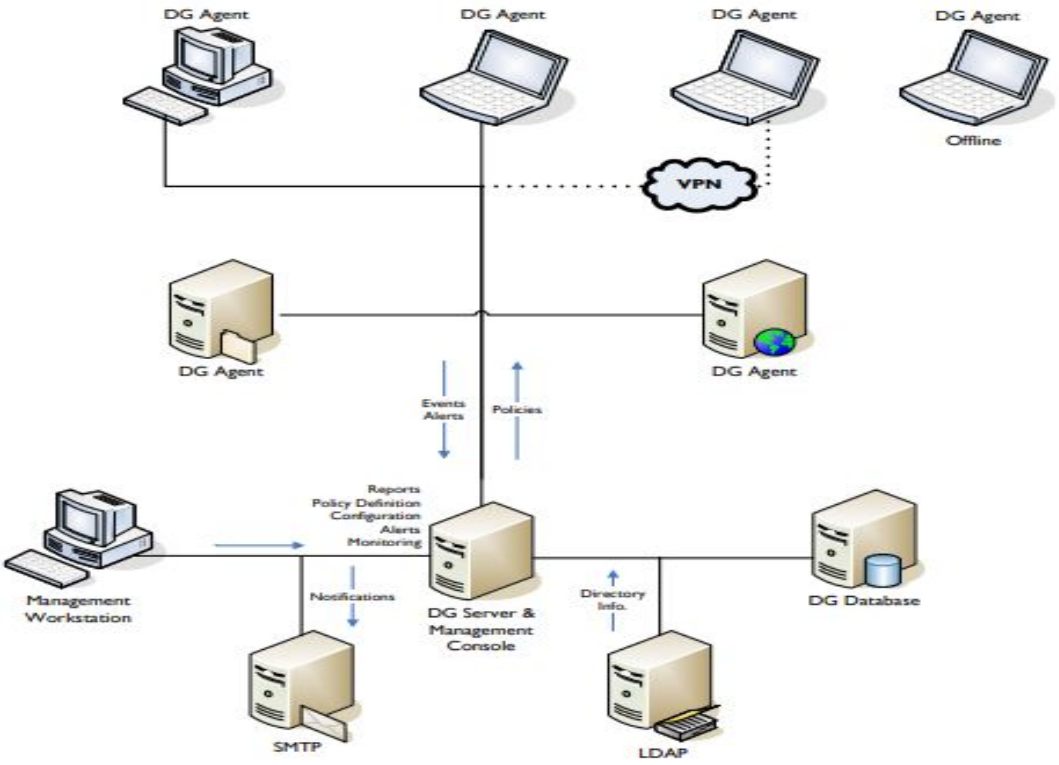

Figure 12. DLP Process Example (Email)
Image courtesy of Verdasys/Digital Guardian

Risk Dashboard - Executive (CSO)

Figure 13. Screenshot of Risk Dashboard
Image courtesy of Digital Guardian

Risk Dashboard - Incident Response Team

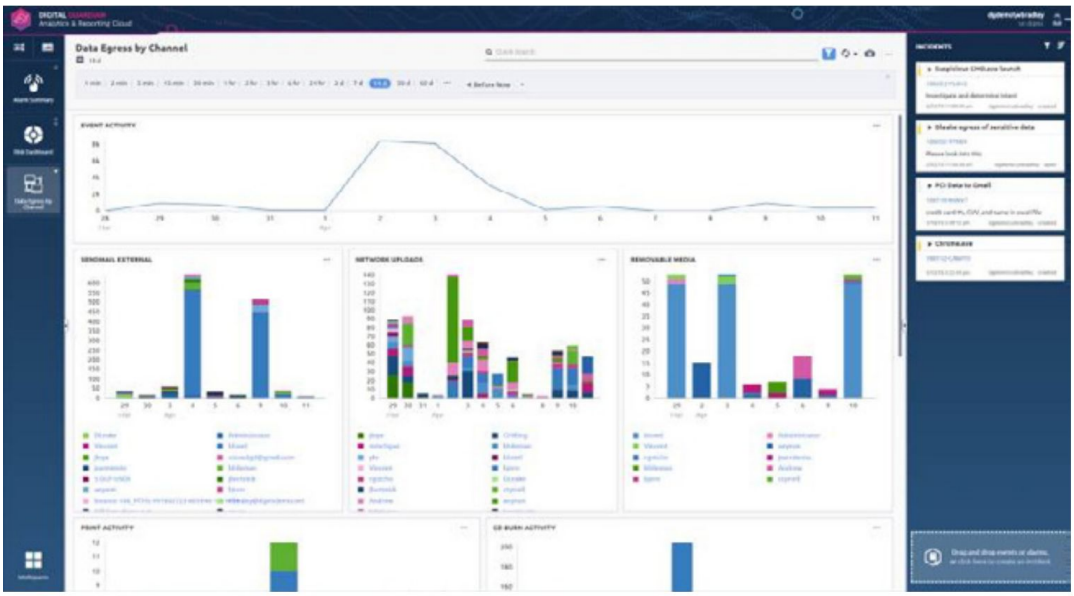

Figure 14. Screenshot of Data Egress by Channel
Image courtesy of Digital Guardian

Roles and Policy Definition

The DGMC server enforces role-based access control. System Roles are provided:

- Alert Manager – Access to view and resolve DG Alerts.
- Classification Policy Manager – Creates Classification rules, policies, and content patterns.
- Control Policy Manager – Creates and administers rules that apply used to govern user actions.
- Enterprise Report Viewer – Access to enterprise level reports;
- Filter Policy Manager – Creates and administers rules that apply filter, policies to users, groups, and computers.
- System Administrator – Assigns roles to other DGMC Users and receives emails in response to specific events.
- Trusted Process Policy Manager – Creates and administers rules that apply to Trusted Process Policies.

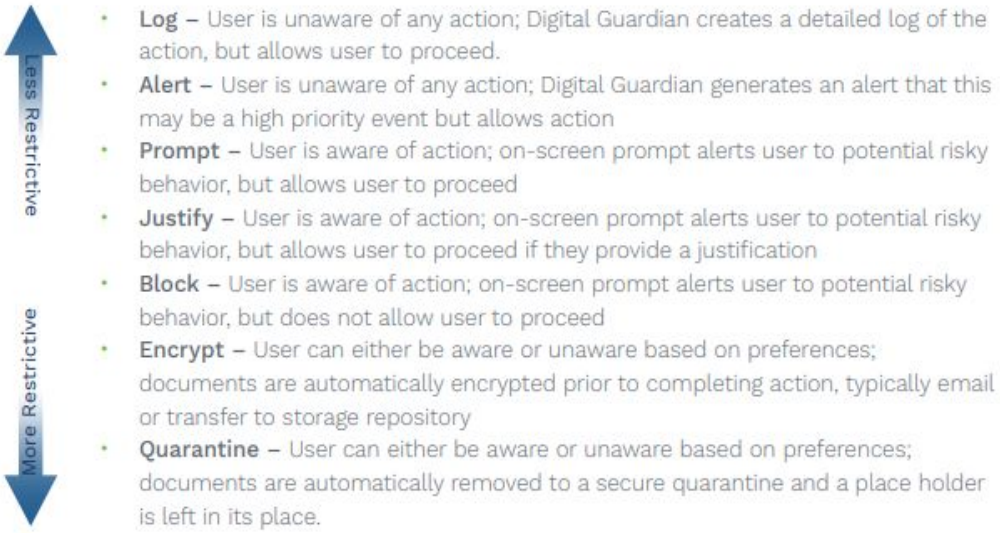

Figure 15. Screenshot of Policy Actions
Image courtesy of Digital Guardian

PART 3: IMPLEMENTATION PLAN

3.1 Solution Delivery Roadmap

DLP roll out will be managed by an agile multidisciplinary team with the VP of Security taking the role of product owner. For a successful implementation, the team will consist of stakeholders from Management, IT, Legal, Human Resources, and Finance who will be responsible for implementing and communicating the required changes that the team determines are appropriate for each department. Successful DLP implementation requires buy-in from all affected parties, and as such, communication is critical. The goal should be presented as a “safety-net” for the company. If mismanaged, a fear of “big-brother is watching” mentality may set in early and present serious challenges.

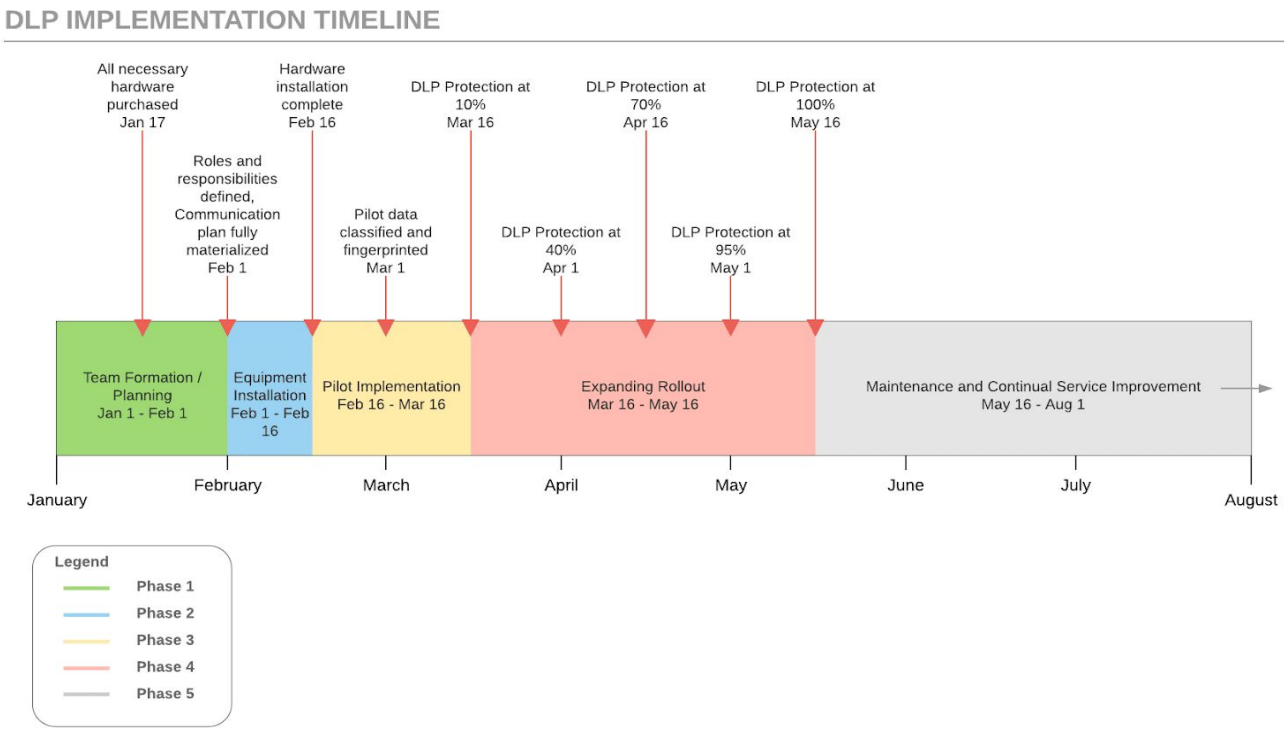

Figure 16. DLP Implementation Timeline

Phase 1: Team formation and planning

The DLP implementation team will meet to discuss and plan the departmental changes and roles that will be required for the project. These roles breakdown as follows:

- Executive Sponsor & Product Owner : VP of Security, Recommendation CSO
- Management: Get buy-in from the employees, establish procedures related to DLP violations
- IT: Install appliances, install endpoint software, establish help desk procedures related to DLP problems
- Legal: Legal counsel considering data privacy laws, establish procedures around serious DLP violations.
- IT Security: Establish procedures related to DLP event monitoring and alerts
- HR: Establish procedures related to DLP violations
- Finance: Project budget consultation

Phase 1 meetings will generate a series of user stories related to each department's requirements. In addition to establishing departmental roles, during Phase 1 the team will identify a small set of sensitive company data with which will be the target of the DLP pilot implementation. While there will be no technical implementation during phase 1 (no appliances installed, no endpoint protection software installed), establishing departmental procedures related to DLP implementation and events should occur. The culmination of Phase 1 will be a series of presentations describing the goals of the project, how and when roll out will occur, and how it will affect employees. The primary goal here will be effective communication and getting buy-in from employees and dissuading fear. During this phase, the team will also decide which of the Digital Guardian managed services (if any) they will purchase in addition to the base package for the first year. Suggestions for roles and responsibilities are found in Table 3.1.

Deliverables: Roles, responsibilities, and buy in from Business Process Owners (BPOs), Procedures, Communication.

Risks: Need to make sure that CIO, BU managers and IT are all on the same page. Need buy in from executive leadership and ability to get the right people involved.

Dependencies: Purchasing of equipment and licenses. Initial training of IT team for deployment.

Table 3.1 RACI Chart (Roles and Responsibilities Matrix)

DLP Solution Implementation					
Process Description:	***Phase:***	**VP of Security**	**BPO's - HR, Legal, Finance**	**Security/Incident Response Team**	**IT Team**
Review and approve project, project budget	1	A	C	R	I
Oversee project communication (all phases) and solution deployment	1	I	-	A	R
DLP Solution purchase	1	C	I	R	I
Install new DLP network & SSL Visibility appliances & Management console	2	I	-	C	R
IT group test new DLP agents for deployment to endpoints	2	I	-	C	R
Define internal Help Desk procedure for end user DLP support using existing ticketing system	2	I	-	C	R
Define response procedures to DLP related escalations from IT team to support end users	2	I	-	R	C
Deploy verified DLP agents to pilot group endpoints (150 users)	3	I	-	C	R
Define GLOCO sensitive data for classification(departmental)	3	C	A	R	I
Configure data classification to sensitive GLOCO data	3	I	C	R	I
Define user permissions for classified data assets	3	I	A	R	I
Configure user profiles/permissions in DLP solution	3	I	C	R	I
Expanded Solution Rollout	4	I		A	R
User Training	4	I		R	I
Maintenance & Continual Service Improvement	5	I	-	A	R
R = Responsible, A = Accountable, C = Consulted, I = Informed					

Phase 2: Equipment Installation & Testing

IT will install the SSL Visibility Appliance and DLP Network Appliance into the corporate network. IP configuration is applied to the single network appliance which can support all 1500 devices included in this rollout. The Network team will assist as needed to configure the device to work on the network properly. The initial configuration will simply be in “bypass mode” disabling any scanning or interception. IT Security will install the SSL Visibility Appliance Root SSL Certificate on the protected endpoints. IT will also install and configure the DG Management Console and set up the necessary Oracle database for storing classification tags. IT will install an initial configuration to a few test machines and make sure that there are no conflicts. If any are discovered, the image will be adjusted accordingly. Help Desk processes for assisting users with DLP issues will be developed and the Help Desk will be trained on these.

Deliverables: Network installation of hardware complete, initial configuration complete, IT testing complete, DGMC dashboards created to monitor data usage on network, start fingerprinting the most sensitive data

Risks: Possible issues with network DLP configuration and other network devices to be handled by IT team

Dependencies: SSL appliance must be installed, then the network DLP appliance, and finally the endpoint DLP software to the IT test machines. Set up the DGMC to monitor and create reports on data access and use to start developing policies based on normal workflows.

Phase 3: Pilot Implementation (10% initial coverage)

Having planned out the required departmental changes and roles, and communicated the coming changes to employees, the stage will be set for the pilot implementation. Key employees from an interdepartmental cross section of the company will be included in the pilot DLP rollout program. Affected employees will be duly informed of their involvement in the pilot program before the enforcement begins. An SCCM user group will be created with the pilot members in it, and then SCCM will be used to push the installation package out to these individuals. The package will be configured based on the testing done by the IT team in phase 2. It will require a Windows Installer file (.msi) that resides on the network and is accessible by the SCCM server. This will allow a silent push to all pilot machines. IT Security will then enable TLS interception and DLP scanning for the systems taking part in the pilot program. IT will fingerprint the targeted sensitive data. IT Security will track and generate reports based on what the DLP detects, and this will be used to set up the workflows for daily work for employees.

Deliverables: Pilot group created and trained on process, Endpoint DLP deployed to all pilot group machines, continue fingerprinting data, adjust DGMC dashboards as needed

Risks: Endpoint DLP interaction with existing applications and security software to be handled by IT security team

Dependencies: SCCM installer and pilot group set up properly, dashboards and reports will be used to start adjusting the workflows

Phase 4: Expanding Rollout (30% every 2 weeks over 6-week period, plus 2 weeks for outliers)

The DLP implementation team will target new datasets for protection in order of sensitivity, with the goal being to reach the high-impact data first. Using everything that was learned during the pilot program as a guide, the team will begin to expand DLP protections to these new datasets and install endpoint protections on affected endpoint systems. Endpoint DLP will be pushed out to expanding rollout systems via SCCM in waves.

In addition to targeted endpoint deployment based on targeted data protection, IT will make plans for company-wide endpoint protection deployment, including automatic installation on new systems, and implement that rollout. As more systems come under DLP management, more edge cases and false positives may occur. It is important that if the IT or IT Security departments become overwhelmed with DLP alerts, rollout must pause while work is done to re-train systems or employees on secure data management (depending on where the fault lies). At the end of Phase 4, all company endpoint systems will have DLP software installed, new systems will have it installed by default, and all sensitive company data will be under DLP protection.

Deliverables: Installation of endpoint DLP software onto all company assets, registering of USB storage devices, finish fingerprinting data if not already complete

Risks: Aggressive timeline to get all machines set up with endpoint DLP software

Dependencies: Management console must be configured from pilot group

Phase 5: Maintenance and Continual Service Improvement (CSI) (100% coverage)

The DLP Implementation team has completed its job and can be disbanded. The IT Security and IT departments manage the long-term health of the DLP system. Now that the DLP project is firmly established, IT Security can work interdepartmentally to identify opportunities for more advanced DLP protection. As issues are discovered, the IT security team will continuously adjust the DLP solution.

Deliverables: Continue to adjust DLP implementation until it fits GLOCO’s needs and workflows, continue to train employees on proper data management practices

Risks: Generating too many exceptions, making sure that configuration fits need

Dependencies: Continued support from employees and management through reports and training.

3.2 Operationalization

The IT Security team will administer the operation of the DLP through the Digital Guardian Management Console (DGMC) with oversight from the VP of Security. IT Security will monitor the DGMC for security incidents and take appropriate actions as needed. These actions will range from reviewing *Defend Notices*, reaching out to the offending employee to remind them of security policies, and escalating issues to the VP of Security.

The DGMC is used to monitor all incidents on the endpoints and network, set rules and data policies, and for performance reporting. The DGMC advance analytics engine provides in-depth analysis for executive reports, performance reporting, and forensics.

The VP of Security will be monitoring from a high level to determine if new rules or changes are needed. Approval for changes in rules and policies to be implemented in the DLP will come from the VP of Security. The IT Security can push those new rules or changes to every endpoint through the DGMC. Updates and patches for the DLP endpoint agents are applied via the DGMC as well.

The IT Help Desk will be provided with a limited access role to be able to see DLP blocks that have occurred and assist users by providing temporary access if approved by the affected user's manager. This temporary access will be removed after a set amount of time if the IT Security team does not upgrade it to a permanent permission. Tickets related to DLP will be forwarded to the IT Security team to address, either by adjusting the role permissions of the user if they are too low or adjusting the rules that the DLP system uses to block sensitive information if it is a false positive. Users will be referred to documentation and training if the access level that they are trying to upgrade to is not approved.

The performance requirements for the DLP solution is that users should not noticed DLP is in place unless an infraction is committed. There should be no perceived loss of speed for transferring files or sending emails. Along with the performance metrics provided by the DGMC, users will receive surveys gathering feedback on perceived effectiveness of DLP as well as feedback on how DLP effects workflow. Over the course of six months the goal is that the DLP is nearly invisible to the end user.

In the SLA agreement with DG and GLOCO, these are the highlights

1. Data Center Uptime: DG commits that their datacenter network will be available 99.99% of the time, excluding scheduled maintenance.
2. Downtime Measurement: Downtime is measured from the time a trouble ticket is opened until network availability is restored, or the affected device is powered back on, as applicable.
3. Maintenance: Categories of maintenance include Digital Guardian Maintenance Windows, Scheduled Customer Maintenance, and Emergency Maintenance.

4. Customer Desktop Health and Availability: Customer is response for managing and supporting its desktop environment.
5. Service Requests Health and Availability: Response and resolution levels for typical customer requested actions related to ongoing support and maintenance of the of the Digital Guardian solution environment.

The above SLA details are sourced from the Digital Guardian 7 Service Specifications document, specifically on pages 10 and 11, which is in the references at the end of this report.

3.3 User Enablement

Employees will be prompted to set up user profiles when trying to access their work stations and directories. The user profile will require basic information about the employee – such as name, title, department, and employee ID – as well as require them to request access permissions/privileges. Access permissions must be requested on an asset or asset group basis. Permissions will be categorized into the three primary verbs of View, Edit, and Manage respectively.

Once an employee has gone through the initial setup of the user profile, their daily work will continue almost as if nothing has changed. An important goal of the DLP solution is to effectively deploy while maintaining a frictionless environment for employees. Employees will notice a change if they attempt to access unauthorized assets. This will result in a *Denial,* defined as a notice explaining lack of rights or permissions to access the requested asset. Employees will now have access to create *Defend Notices*, defined as business and use justification in response to *Denial Notices*.

The Endpoint DLP Agent will be pushed silently, resulting in minimal employee hindrance in day to day work.

The DLP solution will require employees to attend initial and quarterly training sessions, consisting of basic procedural definitions and serve as a time for employees to ask any questions they may have. The training sessions will be offered as a dial-in video conference to allow for the easiest setup with minimal organization. Topics such as whitelisting financial and healthcare related websites and services, along with other privacy concerns, will be addressed. Descriptions of data classification, sensitivity criteria, and asset management will also be touched on. While existing employees will have the opportunity to attend the initial training session over a remote bridge, new hires will have this introductory training incorporated into their onboarding. This allows for the organization to set expectations from the very beginning.

3.4 Metrics and Measurement of Success

Metric 1: Number of databases and data residents not yet classified. Some data can be automatically classified through automatic data discovery tools, while other data must be classified manually. The goal then is to minimize this metric over time.

Metric 2: Number of databases not yet fingerprinted. One example of digital fingerprinting uses checksums of sensitive files, and as files pass through the DLP device, they are scanned, and the checksum is compared to a database of fingerprinted checksums. Databases that are classified, but are not yet fingerprinted, should be identified, measured, and minimized with time.

Metric 3: Number of unmanaged devices in the network handling sensitive data. The number of devices within an organization that are not under DLP management should be minimized, as each of these devices are a potential data loss risk. These devices should be identified and over time efforts must be made to minimize this number. This will be the primary metric for Phase 3.

Metric 4: Number of policy exceptions granted per period. There will be a period of training both the personnel, and the DLP machine learning mechanisms, regarding the new data policy. Exceptions will have to be granted, but these exceptions can be categorized and measured over time, with the eventual goal to get the system to the point that no exceptions are required.

Metric 5: Number of false positives generated per time period. A small number of false positives is manageable. Many false positives can grind a system to a halt and cause users to lose faith in the DLP solution. Therefore, it is important to measure, and work to minimize the number of false positives generated by the system.

Metric 6: Mean time to respond to any DLP alerts. DLP alerts must be prioritized by the security team as they are potential alerts of a major data breach. A system where the alerts are ignored for long periods of time is worse than no system at all, since in that scenario it only provides a false sense of security. Therefore, this metric should be measured and minimized.

Metric 7: Overall user satisfaction. At the completion of the implementation, users are surveyed to determine overall satisfaction with the new DLP system

References

Carnegie Mellon University. (n.d.). Guidelines for Data Classification - Information Security Office - Computing Services - Carnegie Mellon University. Retrieved October 3, 2018, from https://www.cmu.edu/iso/governance/guidelines/data-classification.html

Common Criteria Portal. Digital Guardian Product (2012, October 2). Retrieved October 25, 2018, from https://www.commoncriteriaportal.org/

Digital Guardian. (2018) Digital Guardian 7 Service Specifications. https://digitalguardian.com/contracts/Digital_Guardian_7_Service_Specifications.pdf

Digital Guardian. (2018). Digital Guardian Technical Overview [Whitepaper]. https://digitalguardian.com/resources/whitepaper/digital-guardian-technical-overview

Digital Guardian. (2018). Digital Guardian Endpoint DLP Retrieved October 26 from https://info.digitalguardian.com/rs/768-OQW-145/images/DG-Endpoint-DLP.pdf

Digital Guardian. (2018). Digital Guardian User & Endpoint Analytics Retrieved October 26 from https://info.digitalguardian.com/rs/768-OQW-145/images/DG-UEBA-datasheet.pdf

Ernst & Young. (2011, October). Data Loss Prevention Keeping your sensitive data out of the public domain. *Data Loss Prevention*. Retrieved October 3, 2018, from https://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf

Kish, D., Reed, B. (2017). Magic Quadrant for Enterprise Data Loss Prevention. Gartner G00300911 Retrieved from *https://www.gartner.com*.

Ponemon Institute. (2016, September).2016 Cost of Insider Threats Report. Retrieved September 28, 2018, from https://learn.dtexsystems.com/rs/173-QMH-211/images/2016%20Cost%20of%20Insider%20Threats.pdf

Ring, M., & Stevens, M. (2015, Jan 20). Deploying a Data Protection Program Quickly – Best Practices for Success [webinar]. Retrieved from https://www.brighttalk.com/webcast/12317/139807

Singh, A. (2017, June 08). 6 Key Metrics to measure the success of your Data Loss Prevention (DLP) Program. Retrieved October 1, 2018, from https://www.firecompass.com/blog/top-6-metrics-data-loss-prevention/

Splunk Base(n.d.). Retrieved October 28, 2018, from https://splunkbase.splunk.com/app/1877/

SSL Visibility Appliance. (n.d.). Retrieved October 22, 2018, from https://www.symantec.com/products/ssl-visibility-appliance

Symantec Corporation. “Symantec® SSL Visibility Appliance Administration & Deployment Guide.” Retrieved November 25, 2018, from https://support.symantec.com/en_US/article.DOC10950.html