2/22/2021

Digital Guardian On-Premises Implementation Specification

Table of Contents

Introduction

This document details the **Digital Guardian On-Premises Implementation** (**OnPrem**) solution for the ***Digital Guardian Endpoint Data Loss Prevention Suite (eDLP), Network Data Loss Prevention Suite (nDLP), Analytics & Reporting Cloud (ARC) (****DG Hosted****)*** and various setup services provided. This document contains an outline of the requirements the **Client** is expected to provide in order to run the **OnPrem** solution as well as the **Service Level Agreement (SLA)** for the (DG Hosted) offering. A definition of services offered by Digital Guardian during the **setup phase** of the implementation is also included. The **Setup Phase** is considered to be the time spent scoping, developing, testing, training the client and deploying the Digital Guardian system until the agreed upon use cases are implemented. This document does not address **Support Terms** and requires the client to have already signed the **Digital Guardian Master Agreement** (**DGMA**) and relevant addendums which contains a full scope of terms and conditions that apply to this Service.

DG On-Premises Implementation Specification Overview

Digital Guardian OnPrem Implementation is a software delivery model in which software is licensed on a subscription basis and the system is managed by the client on client hosted infrastructure within the clients datacenter or cloud provider of their choosing. Services to assist the client during the implementation and operational preparations phase are available for purchase include the following:

1) **Infrastructure** – The client will provide and facilitate all back-end infrastructure support and software systems that are required to run the Digital Guardian solution. This includes the eDLP DGMC infrastructure as well as any of the nDLP Manager & nDLP Inspectors components. Procurement of all necessary third party software, such as windows operating systems, Microsoft SQL Licensing, etc., are the clients sole responsibility. The client will be required to provide sufficient database space on a supported version of Microsoft SQL Server and conform with the configuration requirements as stated in the Digital Guardian Installation and Upgrade manual as well as the Server Requirements document.

2) **Installation Process –** Digital Guardian will assist with the installation and configuration of the **Digital Guardian Management Console** (**DGMC**) and **nDLP** infrastructure. The installation process will consist of several steps outlined below.
    - Delivery team kickoff call to introduce the team, provide a product overview, and review the deployment process
    - Define the sizing and architecture requirement for the infrastructure required
    - Provide the client with the prerequisite security application exclusions documentation
    - Provide an installation readiness check list to assist the client in preparing for the implementation
    - Perform the Installation via remote sessions or onsite, supporting the client where needed during the production deployment. Travel schedules and logistics to be mutually agreed upon
    - Travel and related out of pocket expenses are not included. Digital Guardian will invoice the client for such travel and related out of pocket expenses (See MSA for terms)
    - Perform any post install environment cleanup and customizations
    - Create required Digital Guardian Agent install packages and validate successful installation and registration
    - Pilot the deployment of the solution to a limited number of targeted test systems for user acceptance testing
    - Provide transfer of knowledge sessions to enable the client to run the system independently

3) **Infrastructure & Application Monitoring** – The client will provide infrastructure and application monitoring including critical usage, fault and stress indicators for the DGMC Infrastructure. The client will maintain a secure and stable infrastructure by regularly monitoring, auditing and testing the environment for vulnerabilities.

4) **Agent Installation Packages** – DG Professional Services will build the initial installation packages for OnPrem deployment environments as well as modify all initial resource files required for proper system implementation. The client is responsible for Agent installation packages after initial creation is performed by DG personnel during setup. The intention during this phase is to train the client on the proper procedure required for future agent package creation and deployment.

5) **Upgrades** – If the client has purchased ARC services they must maintain their DGMC on a current compatible version with the ARC environment. For DGMC to ARC connectivity to function properly the client must perform regular updates of the DGMC infrastructure as updates are made available by Digital Guardian. Updates to the ARC environment are handled by Digital Guardian and are not the responsibility of the client. Typically ARC updates happen every 6 weeks and are dependent on the DG engineering release cycle.

6) **Digital Guardian DLP Policy Packs** – DG will provide access to standard content packs for eDLP and nDLP standard use cases for the clients consumption and reference purposes. eDLP Content is made available through the DG Content Server while standard nDLP content is provided in the Appliance release. DG Professional Services will assist with the implementation of the standard content packs and will attempt to train the client in the optimal use of the provided content. It is the client's responsibility to enable and customize this content going forward to meet any specific use cases the client requires.

7) **DG ARC Content** – Digital Guardian will provide access to included workspaces, analytics rules, and reports provided as standard content. This also encompasses advanced endpoint system information, advanced analytics across the enterprise, threat vector mapping, and SOC workflows for investigation and remediation. Additional details can be found in the DG ARC product documentation and literature. The DG ARC Content comprises:
    a. Cyber and DLP Rules in DG ARC
    b. Security Analysis Driven Dashboards
    c. Reporting & Analytics
    d. Detailed Process Tree Investigation Capabilities
    e. Endpoint Forensic Artifact Collection
    f. Configuration for the clients specific environment is included as part of the service.
    g. Clients will have access to continuous updates that are published and announced on the **Quarterly Customer Update**.

8) **Operations & Support** – DG will enable the clients access to Digital Guardian's ticketing and CRM system (based in SalesForce) for issue and change control tracking, knowledge base access , general training content and for product issues reporting and tracking or for any items requiring Digital Guardian intervention. This system is available around the clock facilitating access to the DG Support and Operations team via Web Portal, email, and phone (7 x 24 x 365).

9) **On-Demand Training Library -** DG will provide access to on-demand training which consists of self-study eLearning topics on conceptual/process information, "how to" software video demonstrations, labs including step-by-step documentation to practice, and knowledge checks. Content areas include Supporting and Troubleshooting, Administration, Security Policies, and Analytics and Reporting.
    - Supporting and Troubleshooting content includes all installation, configuration, and troubleshooting topics for the Endpoint and Network DLP solutions.
    - Administration content includes topics for administrative tasks performed in the DGMC and nDLP Manager.
    - Security Policies content includes topics for creating policies in the Endpoint and Network DLP solutions.
    - Analytics and Reporting content includes topics for incident management and reporting for the endpoint and network DLP solutions.

10) **High Availability and Disaster Recovery** - Various High Availability ("HA") and Disaster Recovery ("DR") solutions can be implemented depending on the risk tolerance of the particular client. Implementation of an HA (High Availability) solution is dependent on the clients' needs and capability to run an HA implementation. The required recovery time objective (RTO) and recovery point objective (RPO) defined by the client will determine the solution requirements.

11) **Backups** – The client will provide backup and resiliency for components including DG event bundles generated by the DGMC bundle archiving feature (if it is implemented). At a minimum, Digital Guardian recommends the client implement Daily backups of the SQL database for DR purposes. DG professional services can assist with implementing included SQL full and differential backup.

12) **SIEM Integration** – DG will set up configurations required for data exports to the client's SIEM for all DG supported SIEM platforms. DG will not be responsible for configuration activities on the clients SIEM required for data processing. Custom development using DG Application Programming Interface ("API") are the clients responsibility.

13) **Bundle Playback** – For eDiscovery event requiring the playback of Bundle Archives, The client will need to either; build a DGMC server dedicated for forensic playback purposes (additional license required) and then use the Archive Restore tool to play back any data into the forensic DGMC; or contract with Digital Guardian to store Bundle Archives in ARC for playback and investigation purposes, requiring the self-service playback feature available in the ARC platform. For specific service level commitments please see the Service Level Agreement Section below.

14) **idP SAML Integration** – DG will provide idP SAML integration for identity authentication into the ARC. This will require the implementation of a PingIdentity Access Agent on the clients OnPrem DGMC. Note: The client should have an idP capable of SAML authentication for proper ARC support. **Multi Factor Authentication (MFA)** support is available in various scenarios. See the client's requirements section for further details.

15) **Penetration Testing** – DG will conduct penetration testing on all DG hosted ARC infrastructure on a scheduled basis for compliance and security purposes. The client is responsible for validating the OnPrem environment meets any required **Security Technical Implementation Guides ("STIG").**

16) **Audit Compliance** – all certifications will be maintained by DG infrastructure support team for all DG hosted ARC infrastructure. The client is responsible for validating the OnPrem environment meets any required certifications.

DG OnPrem Setup Services

In order to get the client up and running as quickly as possible, DG has built predefined OnPrem Setup Services that should be purchased to help deploy the DG OnPrem environment. Setup Services are sized and defined based on a variety of factors, but primarily are done by the size (number of agents), scope of deployment (target systems, use cases, operating systems, etc.), and project deployment timelines. The Setup Services includes all time and effort spent by the Digital Guardian deployment team; meeting with the client, documenting any modifications to the solution; developing and testing configurations; knowledge transfer and training the client's personnel; transitioning the deployment to the operations team for ongoing management. These setup services are meant to be a good starting point to get the environment operational for an initial deployment. Further assistance, project specific work, additional use cases, all must be defined and require purchased additional professional services.

Digital Guardian offers standard setup services covering the various solutions for DG Data Loss Protection platforms. This section below describes how services packages are sized and selected for the appropriate deployment. Any deviation from the standard setup services defined in this document may require a separate **Statement of Work (SOW)** and may incur additional fees.

Client Commitment

Although Digital Guardian can provide complete back end management and support of its cloud hosted products and services as well as expert guidance on setup of the key components of a successful **Data Loss Prevention (DLP)** program, there are still elements which require client personnel to be engaged and guide the overall implementation of a properly run DLP program. The two main areas clients must address are

- Maintaining the Agent and servers deployed internally within the client environment
- Supervising and managing the implementation of DLP controls on the client devices.

The level of client commitment (how many people and how much time they spend) depends on the client's size and the complexity and depth of the DLP program developed. Like all critical corporate functions, it's important to plan for some level of redundancy and backup for these, so personnel shifts or departures do not adversely affect the on-going operation of the DLP program.

This is a key client responsibility, which is frequently overlooked. Unplanned loss of key client personnel without proper redundancy and cross-training may require client to purchase additional services time and support from DG to fill the gaps, bring the replacement personnel up to speed, and keep the DLP program running efficiently.

OnPrem Endpoint Setup – (DG-SU-LOW)

- **Infrastructure** - This setup includes single DGMC and ARC environment
- **Operating Systems Supported: Windows & MacOS** (If Linux operating systems are required, additional cost will apply).
- **Number of Agents/Users:** Less than **5,000** endpoints.
- **Use Cases:** the setup phase includes the standard out-of-the-box DLP Use Cases from the content server as outlined in the DLP Use Case Spreadsheet. ***This setup package does not include custom policy development***.

  Additionally, the following conditions apply:

  a. Cloning of PII/PCI/PHI/SRC GIT/ITAR/Context Classification Policies found in DLP Content Pack Use Cases - in total no more than 3 cloned policy sets.
  b. Cloning of Control Rules from the Digital Guardian DLP Content Policy Pack - in total no more than 3 cloned policy sets.
  c. Standard out-of-the-box Digital Guardian Analytics & Reporting Cloud ("ARC") or Digital Guardian Management Console ("DGMC") reports/dashboards/workspaces.
  d. Outside of US deployments - Cloning of PCI/PII Classification Policies up to 3 additional languages (pre-defined list of countries).
  e. Customization of Prompts/Skins (The client is responsible for translation of prompt text into local languages) - in total no more than **2** Prompts/Skins.
- **Project Timeline**: The setup phase is considered complete once the content pack and agreed (in-scope) use cases are implemented and the system is handed over to the client. The setup phase from kickoff to hand over to the client is to be completed within **160 hours** of PS effort and within **60 calendar days** from the date of the kickoff meeting**.** Details on what is provided are described in this document. The setup phase must be completed within **one (1) year** from the date of the Order Schedule.
- **Training:** Client is required to take all online training courses in order to run the environment post setup. Training to begin before Production deployment commences.

OnPrem Endpoint Setup – (DG-SU-MEDIUM)

- **Infrastructure** - This setup includes single DGMC and ARC environment
- **Operating Systems Supported**: **Windows & MacOS** (If Linux operating system are required, additional cost will apply) – (DG-SU-Linux)
- **Number of Agents/Users**: Up to **10,000** endpoints.
- **Use Cases:** the setup phase includes the standard out-of-the-box DLP Use Cases from the content server as outlined in the DLP Use Case Spreadsheet. Additionally, the following conditions apply:
  a. Custom Classification & Control Rule Development - not supported by the Digital Guardian Content Policy Packs - **in total not to exceed 3 custom use cases.**
     - Client use cases should be identified during the sales process and documented in detail for the implementation team.
     - All custom use cases must be within the supported capabilities of the product and the ability of the implementation team to craft a working solution via rule, policy and custom configurations solution via rules, policies and custom configurations capable of being deployed at the desired scale within the client's environment.
  b. Cloning of Control and/or Classification Rules from the Digital Guardian DLP Content Policy Pack - in total no more than 3 cloned policy sets.
  c. Outside of US deployments - Cloning of PCI/PII Classification Policies up to 3 additional languages (pre-defined list of countries).
  d. Customization of Prompts/Skins (The client is responsible for translation of prompt text into local languages) - in total no more than **10** Prompts/Skins.
  e. Custom ARC or DGMC reports & workspaces - in total no more than 3 custom workspaces and/or reports.
- **Project Timeline:** The setup phase from kickoff to hand over to the client is to be completed within **260 hours** of PS effort and within **90 calendar days** from the date of the kickoff meeting**.** Details on what is provided are described in this document. The setup phase must be completed within **one (1) year** from the date of the Order Schedule.
- **Training:** Client is required to take all online training courses in order to run the environment post setup. Training to begin before Production deployment commences.

OnPrem Endpoint Setup – (DG-SU-HIGH)

- **Infrastructure** - This setup includes single DGMC and ARC environment
- **Operating Systems Supported: Windows, MacOS, and supported Linux operating systems.**
- **Number of Agents/Users:** Greater than **10,000** endpoints.
- **Use Cases:** the setup phase includes the standard out-of-the-box DLP Use Cases from the content server as outlined in the DLP Use Case Spreadsheet. Additionally, the following conditions apply:
    a. Custom Classification & Control Rule Development - not supported by the Digital Guardian Content Policy Packs - **in total not to exceed 10 custom use cases.**
        - Client use cases should be identified during the sales process and documented in a Design Specification for the implementation team so the effort level required for deployment can be estimated and if possible accommodated as part of this initial setup.
        - All custom use cases must be within the supported capabilities of the product and the ability of the implementation team to craft a working solution via rules, policies and custom configurations capable of being deployed at the desired scale within the client's environment.
        - If any use cases cannot be accommodated they will be deferred for subsequent reassessment and a later implementation effort, contracted for separately.
    b. Customization of Prompts/Skins - (The client is responsible for translation of prompt text into local languages) - in total no more than **20** Prompts/Skins.
    c. Outside of US deployments - Cloning of PCI/PII Classification Policies up to 5 additional languages (pre-defined list of countries).
    d. Custom ARC or DGMC reports & workspaces - in total no more than 10 custom workspaces and/or reports.
- **Project Timeline:** The setup phase from kickoff to hand over to the client is to be completed within **500 hours** of PS effort and within **180 calendar days** from the date of the kickoff meeting**.** Details on what is provided are described in this document. The setup phase must be completed within **one (1) year** from the date of the Order Schedule.
- **Training:** The Client is required to take all online training courses in order to run the environment post setup. Training to begin before Production deployment commences.

OnPrem Network Setup – (DG-SU-NDLP)

- **nDLP Capabilities:** each nDLP function requiring a separate setup fee are:
  - Discovery (includes Cloud & CIFS)
  - Mail (MTA)
  - ICAP (Web)
  - Compliance Endpoint
- **Number of Locations:** Deployment to no more than (2) locations. (Large scale deployment with more than 2 locations may require additional DG professional services)
- **Use Cases:**
  - nDLP will be configured for the following network inspection items, as appropriate:
    - Network monitoring outgoing unencrypted traffic to be passively inspected and reported on (not blocking); SMTP (using MTA); HTTP (proxy using ICAP); FTP (proxy using ICAP); HTTPS (if SSL is intercepted through an ICAP-capable proxy)
  - Data Discovery will be configured for the following network inspection items:
    - On-Premises Discovery of confidential data on supported networks file servers and databases.
  - Cloud Data Discovery will be configured to:
    - Scan all files uploaded to supported cloud storage for confidential or regulated data on corporate owned cloud storage accounts using client provided credentials
  - Compliance Agent will be configured to:
    - Monitor (optional encrypt or restrict) files transferred from the client's endpoints for confidential data (USB drive, SD card, CD, DVD)
  - Traffic Monitoring Reporting
- **Project Timeline:** The setup phase from kickoff to hand over to the client is to be completed within **40 hours** of PS effort and within **60 calendar days** from the date of the kickoff meeting**.** Details on what is provided are described in this document.. The setup phase must be completed within **one (1) year** from the date of the Order Schedule.
- **Training:** The Client is required to take all online training courses in order to run the environment post setup. Training to begin before Production deployment commences.

OnPrem ARC Connection Setup – (DG-SU-ARC)

- **Environment Request:** MSP Operations will raise a new DG Environment record under the client's account. *The purpose of this is to generate a unique ID for the ARC environment that can be associated with the client account.*
- **ARC Provisioning:** MSP Operations will create an ARC tenant appropriately sized for the client. A tenant secret and connection details will be provided to the project team for use on the client's DGMC.
- **Authentication:** If **Single Sign on (SSO)** is required then MSP Operations will set up DG side SSO configuration and organize a remote session with the client and Project team to configure DGMC side parameters for SSO, allowing the client to authenticate as with their enterprise identities to the ARC.
- **SSO Specific Requirements:**
    - ARC doesn't perform authentication itself, instead it relies on an external federation service to provide it SAML authenticated tokens. In order to facilitate login to ARC the simplest method is to use the DGMC to authenticate a session that ARC then permits.
    - In order to achieve this the OnPrem DGMC has to meet the following criteria:
        - The DGMC must be able to communicate outbound on port 443, this covers communication to ARC and to Digital Guardian's SSO service.
        - The DGMC must be version 7.5.1.0020 or higher.
        - The DGMC must have a Ping Access™ Agent module installed within its IIS modules. DG will provide the module and the configuration information.
          Reference: https://www.pingidentity.com/en/resources/downloads/pingaccess.html
          The Ping Access™ Agent module redirects inbound DGMC logon requests to DG for 'tokenization'. Once authentication is then completed by the DGMC, DG's Ping infrastructure provides a token that can be used for entry into ARC using DGMC credentials.
- **Bundle Archive:** The Archive Restore functionality is included as part of the ARC subscription. It will include 1 year of retention unless additional storage has been purchased. The ARC tenant will be configured for retention as part of the deployment process. For specific service level commitments please see the Service Level Agreement Section below.
- **Project Timeline:** The setup phase from kickoff to hand over to the client's operations team is approximately **5 days.** Details on what is provided are described in this document. The setup phase must be completed within **one (1) year** from the date of the Order Schedule.
- **Training:** The Client is required to take all online training courses in order to run the environment post setup. Training to begin before Production deployment commences.

DG Deployment Methodology Phases

The implementation process follows the proven Digital Guardian Deployment Methodology. The phases are detailed below. Upon completion of the Setup phase, the client will be turned over to the clients operations team for ongoing management, maintenance, and usage. The phase descriptions encapsulate the entire DG platform of services and depict a general overview of the deployment process. Additional details will be provided during the project kickoff. The setup phases are as follows:

- The **Planning and Requirements phase** focuses on designing and defining client's detailed requirements based on client's business objectives for information protection. This includes defining the target uses cases, project schedule, technical details, and resource plan.

- The **Qualification phase** includes building and testing agent deployment packages for each operating system and verifying agent compatibility within client's standard operating environment. For network only deployments, this phase will be skipped.

- The **Deployment phase** focuses on configuring, testing, and deploying the Digital Guardian Management Console (DGMC), the Digital Guardian Appliance, provisioning the tenant in the DG Analytics and Reporting Cloud (DG ARC), and assisting in the deployment of the core Digital Guardian Agent, including enabling any additional licensed modules.

- The **Use Case Implementation phase** focuses on reviewing and implementing the necessary data loss prevention (DLP) rules and policies. This could also include fingerprinting of sensitive data sources where appropriate if nDLP is being deployed.

- The **Transition phase** focuses on assisting the client with the definition of their internal DG operations and support processes, as well as facilitating a knowledge transfer to ensure a smooth transition of regular operations to the **Client's Operations Team**. Additionally, Digital Guardian will provide support, governance, and strategic oversight during this phase to ensure the solution is adopted within client and to ensure that client has a successful deployment. *The handover process is discussed later in this document.*

The Planning and Requirements Phase

This phase focuses on designing and defining the client's detailed requirements based on the clients business objectives for information protection. This includes defining the target uses cases, project schedule, technical details, and resource plan.

- When the project begins, Digital Guardian will conduct a project kickoff session to:
  - Introduce the Digital Guardian professional services team.
  - Review the client's main security objectives and expectations.
  - Review Digital Guardian's Data Protection Suite.
  - Review architecture design and sizing requirements.
  - Review high level deployment process and best practices.
  - Define next steps which will include defining a custom deployment plan and baseline schedule.
- As part of this phase, Digital Guardian will begin conducting workshop sessions with the client to collect and document use cases and security requirements which may vary across the clients various departments. Services to collect and define requirements will be conducted throughout the project and will be part of the on-going lifecycle management of the deployment. In preparation for these sessions, Digital Guardian will work with the clients Project Manager to identify appropriate attendees to participate in each workshop session.
- From a general perspective, during this phase, Digital Guardian will work with The client to document the requirements and develop use cases that describe the data use in terms of:
  - Users (e.g., employees, partners).
  - Systems (e.g., business applications, web applications, email).
  - Data Type (e.g., PCI, PII, CAD diagrams, sensitive documents).
  - Data Usage (e.g., email, prints, USB, Web transfer).
- The goal of this phase will be to finalize:
  - Initiate the project and familiarize the client with Digital Guardian's deployment methodology and best practices.
  - Begin collection of security use cases and requirements to incorporate into the Solution Design Documentation.
- Once approved, the Solution Design Documentation will become the controlling definition of scope for the remainder of the project. Changes to the design will require approval through the process described in the Change Control Management Section below. The design must be compliant with the setup level purchased as defined above.

The Qualification Phase

This phase will include building and testing Digital Guardian Agent deployment packages for each required operating system and verifying Agent compatibility within the client's standard operating environment. For network only deployments, this phase will be skipped. As part of Agent Qualification, the DG Agents will be installed on a limited number of test workstations configured with the client's standard hardware and software, including typical applications. These machines are used to ensure the DG Agent's compatibility with the configuration. Testing will include verification of the installation itself, functionality of the core Digital Guardian capabilities and the additional modules licensed by the client.

- Digital Guardian will assist the client in:
  - Installing one DGMC in a testing environment (license permitting), for the purposes of training the client in the proper implementation procedure for the deployment of the client's production environment. Digital Guardian is only responsible for only deploying a single environment. The expectation is that the client is trained during the process and are able to install the production system on their own.
  - Building required DG Agent deployment packages. Initial deployments focuses on core functionality. Subsequent deployments will incorporate combinations of the additional modules required for the specific situation or user groups.
  - Validating Agent installation packages and performing compatibility testing in a lab or Quality Assurance ("QA") test environment.
- The client agrees to:
  - Provide the necessary test workstations with representative build images.
  - Distribute the agent installation package to the test workstations.
  - Assist in the qualification of the agent.
  -

The Deployment Phase

This phase focuses on configuring, testing, and deploying the DGMC, nDLP virtual or physical Appliances, and assisting in the deployment of the DG Agents. This includes all pre-installation actions such as verification of ports, insertion points, routing, and proxy changes; as well as system level configurations (e.g., configuration of management interface, MTA, and ICAP). The client's team will take responsibility for agent install planning and phased deployments; as well as shadow the DG team on the environment build out.

- In the deployment phase, Digital Guardian will assist The client with:
  - Installing one DGMC in either a test or production environment as requested by the client. Digital Guardian is only responsible for only deploying a single environment. The expectation is that the client is trained during the process and are able to install the production system on their own.
  - Installing agents on a set of pilot machines and performing validation testing.
  - Starting the phased deployment of Digital Guardian Agents in the production environment.
  - Performing the nDLP Pre-installation verification
    - Verify IP address, gateway and DNS for network interfaces:
      - Management
      - MTA
      - ICAP
      - Discovery Cloud/Network
    - Verify switch ports for interfaces
    - Verify insertion point for network tap
    - Verify physical location for VMWare ESXi for Virtual
    - Identify SMTP routing changes:
      - MTA access list
      - Forwarding MTA
      - Re-routing MTA
    - Verify ICAP-capable proxy
    - Verify initial content for registration (unstructured files, database parameters, CSV files, or regular expressions)

- Digital Guardian will assist the clients IT resources with the following services
  - Configuration of Microsoft SQL Server Database Server.
  - Installation and configuration of DGMC(s).
  - Optionally installation and configuration of **DG Archive and Restore** for backups and archive retrieval.
  - Building deployment packages for necessary end-user workstations (Windows, Linux, and MacOS based on agent-types purchased).
  - Validating Agent installation packages and performing compatibility testing on pilot groups in production environments.
  - System Level Configuration of nDLP appliances including:
    - Management interface
    - DNS settings
    - Time zone settings
    - NTP and verify NTP synchronization
    - Hostname and Alert SMTP email address and server
    - SNMP if available
    - Syslog (if alerting to external syslog server is desired)
    - Creating administrative users
    - Network Inspection
      - Verify the network inspection interfaces on the TAP
      - Verify inbound/outbound direction and tap operation
    - MTA
      - Configure the MTA IP address and verify connectivity
      - Configure forwarding and re-route server parameters
      - Configure MTA access list
      - Configure internal SMTP server to route a single test domain to the CGN VMWare ESXi for Virtual (e.g. gmail.com or other non-critical domain)
      - Configure a test policy and verify an email to gmail.com causes an incident and is successfully sent to the final destination
    - ICAP
      - Verify the ICAP IP address and verify connectivity
      - Enable proxy interception for a single workstation
      - Configure a policy for ICAP inspection for the single workstation
      - Enable site-wide ICAP inspection based on current ProxySG configuration
      - Verify SSL interception and HTTPS over ICAP on a single workstation
      - Plan rollout strategy for further SSL interception
    - Data Discovery
      - Plan/configure data discovery on network, file servers and databases.
    - Cloud Data Discovery
      - Plan/configure data scan strategy for files uploaded to cloud storage

- The client agrees to provide the following items and support to the Digital Guardian Implementation Team
  - Provide hardware and/or virtual servers that conform to the requirements described in the DG Server and Agent Requirements document as published for the appropriate agent and server version.
  - Arrange for Digital Guardian personnel to have the necessary access to the server equipment to assist with performing the installation.
  - Digital Guardian will assist the client in the deployment of the agent on workstations during the early deployments of the first 25 systems.
  - Deploy DG agents via the clients' standard software deployment platform (e.g., Microsoft SCCM).
  - Agent compatibility testing will be carried out on representative sample workstations / workstation images to adequately represent the deployment environment.
  - Rollout to production machines, only the DG Agent version and configuration that has been successfully qualified (on lab and pilot machines) and proven to work within the software/application environment agreed.
  - Identify the agent populations to be implemented and schedule the implementation waves.
  - Distribute the installation package to the first 25 systems receiving the agents according to the schedule described in the project plan. This support is limited to and will end once the install package is determined to be viable for deployment to the entire production environment.

The Use Case Implementation Phase

This phase focuses on reviewing and implementing the necessary data loss prevention (DLP) rules and policies. This could also include fingerprinting of sensitive data sources where appropriate if nDLP is being deployed.

- Digital Guardian will assist The client in:
  - Configuring, testing, and deploying the standard classification and control policies and rules included in the current published policy packs.
  - Designing, developing, testing, and deploying any required custom classification and control policies and rules as defined by the setup level chosen.
  - Designing and deploying legacy custom reports and dashboards or DGARC workspaces as defined by the setup level chosen.
  - This support is limited to and will end once the policies are determined to be viable for deployment to the entire production environment.
- The client agree to:
  - Provide access to the workstations necessary to execute functional tests.
  - Execute the functional tests specified in the Solution Design Documentation.
  - Provide the necessary personnel to implement and test the policies and rules. The Analytics and Reporting Console Phase (if purchased)

The Analytics and Reporting Console (ARC) phase (if purchased)

- This phase focuses on setting up and connecting the cloud-based ARC environment with the client OnPrem DGMC environment. In addition, all reporting, dashboards, alarms and forensic incident management will be customized per the project analysis and reporting requirements depending on the setup level.

The Transition Phase

This phase focuses on assisting the client with the definition of the client's internal DG operations and support processes, as well as facilitating a knowledge transfer to ensure a smooth transition of regular operations to the clients operations Team. Additionally, Digital Guardian will provide support, governance, and strategic oversight during this phase to ensure the solution is adopted within the client's organization and to ensure that the client has a successful deployment. *The handover of the completed project is discussed later in this document.*

- At the end of the Transition phase, The client will:
  - Will have completed all provided Training Material (online or other) in preparation for Client to take over responsibility of administering and managing the DG implementation.
  - Be able to operate its "level one" help desk.
  - Know how to interact with Digital Guardian Technical Support to request assistance.
  - Be trained in the use of Digital Guardian's Client Support portal.

ARC Cloud Connection requirements for OnPrem DGMC Setup

DGMC Deployed OnPrem Using PingAccess Agent for ARC Cloud Connection

- This solution leverages the user identity hosted in the clients Active Directory or the local DGMC to log in to the DGMC for access validation.
- Requires the OnPrem DGMC to have Local DGMC Accounts created or The client has to established an LDAP Sync with The clients OnPrem Microsoft Active Directory for authentication purposes.
- DGMC acts as the federated idP eliminating the need to for a Federated idP connection to The clients ADFS or equivalent environment for DGMC authentication.
- Install and configuration of the Ping Access Agent is required on the DGMC server.
- Internet connectivity is required for the DGMC to access the DG cloud ping infrastructure accessible using the following appropriate URL:
  - https://accessagent.msp.digitalguardian.com – US Based Access
  - https://accessagent-de.msp.digitalguardian.com – EU based access
  - https://accessagent-preprod.msp.digitalguardian.com – Test environment access

Project Administration

Digital Guardian Team Roles and Responsibilities

Role	Responsibilities
Digital Guardian Account Manager	• Responsible for all aspects of the partnership and engagement between the client and Digital Guardian
Digital Guardian Program Manager (PM)	• Overall progress of the Digital Guardian project and day-to-day project management • Ownership of the Digital Guardian project delivery, quality, and timely execution of the project • Business requirements gathering and use case definition • Risk identification, analysis, response, monitoring, and control • Communication management and conflict resolution • Management of the Digital Guardian resources
Digital Guardian Technical Consultants	• Digital Guardian infrastructure requirements definition • Digital Guardian installation/configuration • Policy and rule development, testing, and deployment support of all modules • General technical support for the duration of the project

The clients Team Roles and Responsibilities

In addition, the following the client's team members will be expected to participate in the project (some more than others). It is understood that multiple roles may be filled by a single person:

Role	Responsibilities
Decision Maker (CSO, CISO, etc.)	• Makes broad-reaching decisions that may be outside the scope of the other participants • Clarifies business opportunities, drivers, and high-level security considerations
Project Steering Committee	• Commits the necessary cross-functional resources to the project • Ensures project stays aligned with business and corporate strategy • Champions project effort and monitors overall project progress • Resolves issues outside of the responsibility and authority of the Project Manager
Project Manager	• Serves as the main contact point for day-to-day project-related issues, including project timeline, deliverables, and issue escalation • Involved in all stages of the engagement • Arranges and coordinates the participation of other the clients team members
Data Protection Officer (or similar role)	• Responsible for overseeing the clients data protection strategy and implementation to ensure compliance with various data requirements such as GDPR • Individual has authority to grant the clients users access to DG systems that contain the clients data
Business Analysts / Data Analysts	• Identifies business use cases and has a good understanding of the clients business process and security needs • Understands end-user behavior • Perform analysis on data provided by DG to manage risk within the organization

Role	Responsibilities
The clients DG Administrator	• Has a thorough understanding of security architecture and strategy • Understands DG policy, rule, report, and deployment support for the DG environment • Has full administrator authority and access to change system parameters as necessary. • Will operate the DG system after hand-over from the Setup Phase.
IT / IT Security	• Ensures compliance with external regulations and the internal security policy • Has a strong understanding of all aspects of the clients security needs • Has details on the Active Directory integration/VPN Setup as required • Manages desktop environment & agent deployment solution • 2nd line DG agent support and troubleshooting • Assists in any lab and production agent setup/deployment
Network Administrator	• Assists with the diagnosis of network-related issues, including those involving network cards, routers, hubs, switches, LANs, WANs, load balancers, firewalls and external ISPs • Has a thorough understanding of the network architecture
Database Administrator (DBA)	• Assists in the monitoring of database server-related tasks, including backup, maintenance planning, performance monitoring, and all related administration tasks • Has a thorough understanding of the database server architecture • Able to use the database server console for problem diagnosis with full administrator authority and access to re-index tables, change system parameters, and to reboot systems as necessary
Help Desk	• 1st line DG Agent & Appliance support

Scheduling

To permit effective management and mobilization of both project teams, this engagement will commence no sooner than two weeks and no later than six weeks after the execution of the Digital Guardian Master Agreement and an Order Schedule.

Project Status and Progress

Digital Guardian **Program Manager (PM)** and the clients Project Manager will have regular status meetings at agreed upon intervals to review progress against assigned milestones, cost estimates, timelines, deliverables and any issues or risks that may affect the project. As part of these status meetings, the Digital Guardian Program Manager and the clients Project Manager will evaluate whether the estimated cost to complete the project has changed since the previous meeting. If it has, they will work together to escalate this issue as required by the client. During that time, adjustments may be made to activities, deliverables, timelines and/or resources pursuant to the Change Control Management section to ensure that the effort is meeting the clients business and technical needs. In addition, the Digital Guardian Program Manager will be responsible for ensuring that those project management artifacts (e.g., project plan, Solution Design Documentation) managed by Digital Guardian are properly maintained.

Change Control Management

Throughout this project there may be requests from the client that were not originally contemplated and estimated in this document. Digital Guardian will manage all project changes through the project's Change Management process. Additional work will be estimated and priced by Digital Guardian, after which Digital Guardian and the client will evaluate the scope changes on the basis of the client's impact on the project schedule and cost justification. Cost estimates and schedule impact analysis will be presented to the clients Project Manager for approval prior to implementation of any Change. Changes are broadly defined as any work activities or work products not originally planned for in this **Implementation Specification**. They include but are not limited to:

- Participation in any substantial activities not included in this document.
- Developing any deliverable products not included in this document.
- A change in responsibilities as defined in this document between the client and Digital Guardian.
- Investigative work to determine the impact of changes.

The Digital Guardian **Program Manager (PM)** will maintain a Change Control Log of all changes considered along with the client's details and dispositions. Changes will be made by the implementation of a SOW signed by the client and Digital Guardian before being incorporated into the project plan/schedule.

Risk and Issue Management

All project team members will be made aware of the importance of identifying risks and issues and getting prompt resolutions. The steps below will be followed to ensure that risks and issues are dealt with effectively:

- Identify risks and issues.
- Document the risk or issue.
- Evaluate the risk or issue.
- Assign responsibility for resolution.
- Monitor and control progress.
- Communicate resolution.

The Digital Guardian Program Manager will maintain a central risk and issue log. If a risk or issue cannot be resolved in a reasonable period of time, it will be escalated to the next level of management and project control.

Project Completion

At the completion of the setup phase, the DG Services team will turn-over to the client the On-Premise environment to operate. While a project plan of tasks will be provided to outline the implementation, the following tasks will be complete prior to hand over to the client for full operations to take place.

DG Responsibilities by Group

1. DG Solution Architecture / Sales
    a. Prerequisite Checklist to the client
    b. Complete delivery handoff document to Services
    c. Create DG Software License Request
2. Infrastructure & Operations Implementation
    a. DG assists with the Environment Buildout
    b. Configures AD/LDAP Sync
    c. Configures SIEM Data Integration
    d. Coordinates data exports
    e. Installs environmental monitors
    f. Transitions environment to DG Services team for Setup Phase
3. Services
    a. Professional Services Group Schedules Kickoff Meeting with the client
    b. Agent Package Development & Deployment Support
    c. Endpoint Agent Tuning and Configuration
    d. Deploys Content Packs
    e. Installs and configures nDLP Manager & Inspectors
    f. Assist with Agent packaging / AV exclusions
    g. Completes Setup Phase & Custom policy work as defined in the setup specification
    h. Completes handoff and enablement to the clients operations team
4. Support
    a. Provides 24/7 DG product help desk support
5. Steady-State Operations
    a. Project is complete. .

Completion for OnPrem eDLP Deployment Project

Tasks to be completed for transition for an Endpoint OnPrem deployment:

- Access to DG Training on-demand Portal will be provided
- Implementation Plan (includes project steps, timelines and resource plan)
- Solution Design Document (outlining use cases and initial policies)
- Review prerequisite DG Installation requirements outlining AV and security product exclusions
- Agent Deployment Package, Agent Testing & Tuning
- Default content packs will be deployed and configured as requested
- Initial default reports and workspaces will be deployed and operational
- An initial review of the data analysis process will be performed for onboarding
- Project Closure Meeting will be conducted, and the OnPrem environment will be handed-off to the client's operations team.

Completion of OnPrem nDLP Deployment Project

Tasks to be completed for transition for a Network OnPrem deployment;

- Appliance installation and administration of the nDLP Appliance(s)
- Network Packet Monitoring configured, as requested:
  - Outgoing unencrypted traffic to be passively inspected and reported (not blocking)
- Mail configured, as requested:
  - SMTP (using MTA)
- Web configured, as requested:
  - HTTP (proxy using ICAP)
  - FTP (proxy using ICAP)
  - HTTPS (if SSL is intercepted through an ICAP-capable proxy)
- Data Discovery configured, as requested:
  - On-Premises Discovery of confidential data on supported networks file servers and databases.
  - Scan all major databases and find rows where confidential data is being stored, including in "text" fields.
  - Scan a network share and produce a detailed audit report listing location and frequency of confidential data.
  - The following protocols/systems are supported for scanning:
    - CIFS, NFS, SMB, and WebDAV
    - Oracle, Microsoft SQL, MySQL, PostgresSQL, DB2, Informix, and Sybase
- Cloud Data Discovery configured, as requested:
  - Scan all files uploaded to supported cloud storage for confidential or regulated data on corporate owned cloud storage accounts using the clients provided credentials.
  - Audit files that are uploaded or changed.
  - Control cloud content for leading Cloud storage providers – see product information for latest support.
- Compliance Agent configured, as requested:
  - Perform pre-deployment testing of Compliance Agent image to verify application compatibility. This includes creating the Windows installer package for deployment.
  - Monitor files transferred from the client's endpoints for confidential data (USB drive, SD card, CD, DVD)
  - Prompt the user to provide justification before allowing the transfer of sensitive data
  - Optionally encrypt sensitive data as it is written to USB drives
  - Restrict device use to authorized users and devices
  - Provide detailed activity logging and audit reporting of all files containing sensitive data
- Policy Creation
  - Development and deployment of relevant custom patterns
  - Register PCI/PII/PHI data
  - Create policies using the content and custom actions
  - Test currently running policies
  - Policy Tuning
  - Extend and create new regular expression-based policies for custom patterns as needed
- Remediation configured, as requested:
  - Various remediation actions are available and can be discussed
- Knowledge transfer focused on:

    - Identify anomalous activity in logged events and reports
    - Best practices recommendations
    - Filter, rule, and report tuning
- Active Directory integration for user and group assignment naming and for identification of users in policy violations where available.
- Reports configured:
    - Generate reports of confidential data, frequency, and location to determine high-risk users
    - Administrators will receive all standard reports as well as access to custom reports creation as part of the service.
- SIEM Integration/Log Management configured, as requested:
    - Provides necessary effort to connect to the clients provided SIEM and maintenance work to ensure data feed is operational for supported SIEMs
    - Custom integration or non-supported SIEMs will require an additional Standard of Work.

The clients Requirements for DG OnPrem Deployment

There are a variety of requirements to run the Digital Guardian solution as an OnPrem deployment. These requirements are detailed here.

Client Technical Requirements for OnPrem Deployments

The following are the technical requirements to effectively manage and operate the DG OnPrem Endpoint and Network Data Loss Protection solution.

- **Load Balancers** – If a large scale deployment requiring more than a single DGCOMM server or nDLP appliance is required the provisioning of a load balancer or other such load distribution service is the client's responsibility. Digital guardian will provide general guidance on the proper configuration and implementation of a load balancer for DGCOMM and nDLP traffic.
- **SMTP Services** – If email notifications are required the client must provision an SMTP server for mail relay purposes. The DGMC will be configured to use this system for all mail forwarding tasks.
- **VMware Virtualization Infrastructure** - If images are provided, the client is responsible for provisioning a compatible VMWare, Hyper-V or such other equivalent environment to support the deployment of any nDLP or DGMC components.
- **LDAP Sync** – If the client requires additional user metadata for reporting and previsioning purposes, the system can be configured to leverage the DGMC's ability to LDAP sync with the clients Microsoft Active Directory domains. This method expands the capability for the DGMC to target groups for policy and rule deployment, reporting activities and other such administrative tasks dependent on this information being available in the DG system. We support LDAP over SSL and can connect to the client's environment via Secure VPN or externally accessible LDAP connection which bypasses the need for a VPN tunnel.
- **ARC Access and SSO Configuration** - If the client wishes to use the clients own company idP credentials for the DGMC and ARC authentication, then they will require one or more of the following solutions:
  - An active LDAP sync to The clients Microsoft Active Directory Domain
  - A SAML connection to the clients idP for account authentication (ADFS, OKTA, DUO, etc.).
  - If SAML Authentication is the only method allowed by the client , only users with DG Agents installed on the clients endpoint systems will be able to be granted access to the DGMC and ARC environments
- **SQL Infrastructure** – A dedicated SQL Server is recommenced with a requirement of a dedicated named SQL instance for the Digital Guardian databases

The clients Responsibilities

- Best effort to ensure the accuracy, quality, and legality of the data being provided to DG either as documents or data from endpoints.
- The client has the sole responsibility of the reviewing, monitoring and triaging of forensic incidents.
- The client must comply with current technical documentation, including API and developer guides. Documentation is updated and available from the Help link in the DG Support Portal.
- The clients designated administrators is responsible for granting or revoking access to employees
- Client must provide Digital Guardian with, accurate, detailed and complete information of any functional issues requiring DG support involvement.
- nDLP Manager & Inspectors (VM servers) – The client will be responsible for maintaining the VM servers that host our nDLP Manager & Inspectors in the clients network
- It is the client's responsibility as to not exceed the clients allocated storage limits, as well as monitoring the agent/appliance health and connectivity to the DG infrastructure.
- Provide reasonable efforts to prevent unauthorized access or use of the DG ARC.
- If desired, enable Data Privacy to prevent DG admins from accessing client data in the DG ARC.

DG OnPrem Service Level Agreement

The Service Level Agreement pertains to all the Digital Guardian ARC infrastructure listed above. However, because different types of technologies are utilized (e.g., onsite DG Appliance vs. a DGMC and ARC in our data center) some terms and conditions will be modified. This document does not address the Support Services Terms on product software support, response times, and priority definitions, as these can be found in the **Support and Managed Services Terms** located here: https://digitalguardian.com/contracts/DG_Support_and_Managed_Services_Terms.pdf

Definition of Infrastructure Components

The following are the definitions of key systems and services:

- **Analytics and Reporting Cloud (ARC)** – this technology is used for providing reporting and analytics services.
- **Application Servers** - Windows application servers hosting the DGMC, Bundle Processor, Job Scheduler, DG Communications and Distribution Servers.
- **Authentication** – A Microsoft Active Directory Domain is required for authentication, client access and administration.
- **Authentication Service (PING Federate)** – this is used to provide access to various components within the cloud architecture.
- **DGCOMM** – the DGCOMM system is the HTTP based connector used by the Digital Guardian Agents for connectivity with the DGMC.
- **Digital Guardian Management Console (DGMC)** – this is the management console for Policy and Configuration management.
- **Firewalls (Network Access Controls)** – used to segment the clients environment from other supporting technology and other client environments. This also includes the technology used to establish client specific connections like VPN connections.
- **Load Balancers** – required for traffic communication to the DGCOMMs and DGMC.
- **NAGIOS** – used for monitoring the infrastructure for availability and functionality.
- **SIEM Export Technology** – technology deployed on the DGMC Application Servers to stream the data to client's SIEM.
- **SQL Server** – DG utilizes a SQL Instance for the Collection and Reporting Databases.
- **System Outage** – a system outage is defined by a loss of network connectivity or system availability resulting in the DG ARC being unavailable as defined above for any period outside of a scheduled maintenance window.

Availability Definition

DG Cloud Availability – Digital Guardian commits that our DG Cloud Service will be available **99%** of the time, excluding scheduled maintenance.

DG Cloud Uptime – Digital Guardian designated components (for example data ingestion, search functionality, web services access) of the DG Cloud service deemed critical are measured for uptime availability as follows. [1]

- **DG ARC** – Uptime availability is defined as the DG ARC logon system being up and available to process user logon requests to access the administrative interface from the authorized administrative networks.
- **System Services** - availability monitoring is made up of, but not limited to, the following critical system metrics:
    - DG ARC, Firewall, and Load Balancer status checks (DG ARC URL)

Uptime Calculation – is determined using a monitoring solution that tests the DG ARC application for valid responses at predefined intervals. If the validation test fails a specific number of predefined consecutive connection attempts, an outage will be reported, and an alert will be sent to the operations team for remediation. Calculations of service availability can then be measured based on the recorded history of system availability.

Downtime Measurement – is defined as the amount of time the system was down outside of an allowed maintenance window.

Scheduled Maintenance –Schedule Maintenance shall be defined as:

- **Digital Guardian Scheduled Maintenance Windows** - modification or repairs to shared infrastructure, such as core routing or switching infrastructure or platform patching and upgrades that Digital Guardian has provided notice of at least seventy-two (72) hours in advance **or** that occur on Saturdays during the hours of 6:00 am to 10:00 am in the time zone where the data center is located.
- **Scheduled Environment Maintenance** – maintenance of the systems hosted by Digital Guardian that are either scheduled with the client in advance (either on a case-by-case basis, or based on standing instructions), such as hardware or software upgrades.
- **Emergency Maintenance** – critical unforeseen maintenance needed for the security or performance of the clients configuration or the Digital Guardian's network.

Response Time Definitions

Response Time – is defined as the elapsed time between the first contact by an authorized support contact to report an issue and the target time within which Digital Guardian personnel report back to the designated support contact authorized to address the issue. Digital Guardian is not responsible for a missed response time SLA if the designated support contact is unavailable and does not respond to the acknowledgement of the receipt of the reported issue. A Response Time is a guarantee of communication timeframes only; Digital Guardian does not guarantee a problem fix, workaround, or other final disposition within these timeframes.

Desktop Health and Availability – The client is responsible for managing and supporting the client's desktop environment. As outlined in the Service Description, Digital Guardian will complete a thorough quality assurance process to ensure that the Digital Guardian Agent and associated rules function correctly on the client's desktop image. Digital Guardian provides to the client via the console information on the functioning of the Digital Guardian Agent. The agent alerts the clients support staff of Digital Guardian Agent related issues via Operational Alerts. The training provided by Digital Guardian includes standard support processes and procedures.

Service Requests Response Commitments – the following matrix covers response and resolution levels for typical client requested actions related to ongoing support and maintenance of the Digital Guardian solution environment.

[1] Supporting infrastructure outside of the DG Cloud control are exempt from this calculation (Client VPN, AD, SIEM, DGMC, nDLP, etc.)

DG OnPrem Request SLA Matrix

Category	Description/Examples	Response*	Resolution
Request New License Keys	Renew and create new Product License Keys. Install keys on requested Server	Same Day	Next Business Day
Upgrade the DGMC Server	The client is responsible for upgrades of the DGMC. If the client requires assistance, a SOW will be required to engage DG Professional Services to assist.	One (1) Week for a SOW	Coordinate with the client to upgrade the clients DGMC based on the negotiated requirements outlined in the SOW. (Typically twice per year or as needed with a MSP approved DGMC release)
Enhancement Requests	Document enhancement request and submit to DG Engineering for review and feasibility assessment	One (1) Week	TBD
Data Replay Request for OnPrem	The request to replay bundles for clients eDiscovery requests for the purposes of a forensic investigation of historical data (greater than the online retention period in the DGMC).	One (1) Week for a SOW	This work requires a SOW with an estimate and scheduling. (NOTE: A self-service playback interface is available in ARC if purchased)
Additional Storage / Capacity Expansion for ARC	Clients can purchase additional online storage in additional 100GB and 1TB increments	Next Business Day	Next business day. Per mutual schedule if a reboot is required.

**Response is the confirmation of receipt, initial evaluation of the request and acceptance or request for more information.*

Archive & Restore

Digital Guardian sets up Digital Guardian's Archive & Restore functionality for all On-Premise environments to provide playback functionality for investigations of events older than the DGMC or ARC retention settings as outlined in the applicable Master Services Agreement for the purchased Service. The main objective of this capability is to provide Archive & Restore with playback functionality of OnPrem environment metadata using either a forensics DGMC or an ARC tenant instance so that selected archives can be restored and played back for targeted investigations without any disruption of the production environments.

Archive & Restore usage guidelines:

- Digital Guardian can restore data that is older than the environments online standard retention period to an ARC tenant in its original format (Events/Alerts on ARC)
- Restorations are performed only upon client request or can be performed by the client if the self-service bundle playback feature is available and has been purchased and for data replay.
- If the self-service bundle replay feature is not available, clients may request up to four (4) AR restorations per calendar year at no charge. Additional restorations may result in additional fees as per Digital Guardian's current price list or a pre-negotiated price established by Client and Digital Guardian.

- Archives backups are performed daily and can be restored to an ARC tenant for specific date ranges of archived events for forensic investigation purposes.
- Client can request what is restored on a "per date, per user, or per machine" basis.
- 150GB of storage are allocated for bundle playbacks in ARC.
- Current retention settings and storage limits on the ARC environment remain unchanged.
- If additional storage is required for bundle playback additional charges may apply.

Data Retention Commitments for DG Analytics and Reporting (ARC)

The client's ARC tenant will have its Live Data Retention Defaults configured according to the following guidelines. Increases to this default will be made based on the clients retention requirements and purchased storage volumes. Any purchased storage amount will be outlined in the **DG Order Schedule**. The following section defines the data retention guidelines governing how much data is stored and for how long that data is available within the ARC before it is deleted from the system.

- **Retention** - Digital Guardian will store data in the ARC based on the allocated storage volume purchased by the client. The client can purchase as much storage as they like in either **100Gib (Gigabyte)** and **1TiB (Terabyte)** increments. The default amount of storage that will be allocated to a client environment will be 100GB and can be increased from that point.
- **Estimates** - An estimation on the amount of data typically collected on a per agent basis will be provided during the sales cycle based on the use cases and retention periods required by the client. This is an estimate only based on Digital Guardian experience. Once the maximum amount of storage is agreed upon and the client purchases the required amount, it will be configured within the ARC.
- **Monitoring** - Digital Guardian Operations team will not monitor or warn on storage overage for **OnPrem** clients but storage usage dashboards and warning notifications can be configured in the system to alert the client when limits are reached.
- **Alerting -** Predictive alerts on early pruning can preemptively warn the client before data will be purged. Clients are encouraged to monitor the system for data consumption and tune their rules, policies and configurations to adjust the rate of data consumption accordingly.
- **Pruning** - The system will be configured to purge the oldest data first following a FIFO (First in, First Out) methodology based on the amount of storage allocated or optionally the number of days the data should be retained.
- **Filtering** - Data Filtering can be used to reduce the overall quantity pf data being collected. This can be achieve by various means including; configuration changes on event capture settings; adjustments to rules and policy deployment; adjustments on process flags; application of filtering rules on the ARC; application of filter rules on the agent.
- **Deleting** - Data that has already been collected **cannot** be selectively deleted from the system. We are unable to delete data for a single user, system, process, explicitly to eliminate only the unwanted data during a specific time window.
- **Expansion** - Additional storage is always available for purchase if the client wishes to retain more data for longer periods of time. Only DG operations personnel can modify the data retention and volume settings.
- **Time** – The ARC system can also be configured to prune data out of the system based on a maximum amount of time data is stored based on its date of original collection. The system can be configured by the number of days data should be kept up to the amount configured.

NOTE: Digital Guardian reserves the right to reduce any data flows / ingest that are causing instability in the cloud environment.

Data Type	Default Retention Settings	Description
Tenant Live Data Retention Defaults	100GB Default Storage	The default amount of storage that a tenant is allocated for live data processing and reporting in the DG ARC. Additional storage can be purchased in 100GB or 1TB increments. Data Lifespan can also be configured by days of retention, so data is purged on a specified age.
Incidents and Attachments	365 Days of Retention	Incident Details, Notes, Alerts, Alarm, Events and Attachments uploaded to Incidents (NOTE: Bundles are retained based on Bundle Archive settings)
Events, Alerts, Alarms	Tied to Tenant Live Data Retention Defaults	Metadata related to DG Agent collected events, alerts, DG Appliance Incidents and Server-side rule detections that generate an Alarm
System Scan Search	30 Days or up to a max limit in gigabytes based on tenant size	Parsed System Scan data for Workspace searching and filtering. Raw scans are available for 30 days by default
System Scan History	60 Days or up to a max limit in gigabytes based on tenant size	Scan zip files that result from running the system scanner. Full or partial scans in raw, downloadable form
Component Lists	Permanent Retention	List definitions and contents
Incident Attachments	Permanent Retention	Attachments uploaded to Incidents
Email Attachments & Report History	Tied to Tenant Default (60 days)	Files that result in email attachments for Notifications or Executed Reports. (Report History)
Process Inventory	60 Days	Data that results from process launch and Virus Total reputation scoring.
DG ARC - Agent Data Bundle Archive Retention (Available for Purchase)	1 Year	Offline Archived Bundle storage for up to 12 months of agent data for recovery and forensic analysis (Longer term storage available for a fee). May require manual intervention to reload by PS Engagement.
Bundle Replay data in ARC	Unlimited by time or up to a max limit of 150GB by default	Offline Archived Bundles played back into ARC for eDiscovery purposes.

Data Type	Default Retention Settings	Description
Legal Hold	Greater than 1 Year	Please contact the MSP operations team for available options.

Protection and Privacy of Client Metadata - (Optional ARC Capability)

DG maintains administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of the client's recorded telemetry. Each client's tenant environment is provided segregated logical data stores for their metadata which is not accessible by other clients.

An optional Tenant level data privacy feature is available to clients to prevent DG employees from accessing client recorded metadata. *This must be enabled by the client*. Once enabled DG employees will not have access to that clients metadata unless it is necessary to maintain the service or comply with governing bodies.

Additional Products and Services

Items that may require an **additional fee**, custom sizing, or additional agreements include the following:

1) **Custom Data Extracts** – clients requesting custom data extracts or custom reporting outside of the Digital Guardian system that require additional configuration and data storage/bandwidth will require a sizing effort and possibly additional fees due to the extra infrastructure requirements and time to setup the custom operation.

2) **SIEM Integration** – clients that want to integrate an unsupported SIEM may require additional Professional Services depending on target SIEM. DG will not host the clients SIEM software in the cloud. Supported SIEMs include: QRadar, Splunk (Classic and Cloud), LogRhythm, Solarwind, ArcSight, FireEye (Helix Cloud), Alienvault

3) **Investigation Module** – the Investigation Module provides enhanced File Capture capabilities into the core Digital Guardian product. To utilize this service the client must purchase the Investigation Module license; purchase additional Professional Services for implementation services.

4) **Additional Servers / Additional Storage / Server Agents / Development Environments** – clients that require more environments than our standard production and/or require data separation from a data privacy perspective or Server Agent storage requirement will need to be sized and properly priced.

5) **Custom Threat Feeds** – DG Threat Team will configure agents to utilize custom threat feeds. Additional Professional Services may be required based on complexity of integration.

6) **Ongoing Professional Services Packages (DG-PS-24 or DG-PS-40,etc)** – A variety of additional professional services delivery options are available for purchase. Examples are included below. Please speak to your DG Account Manager for details.
    a. **Custom Installers –** remain the clients responsibility, and DG will only provide standard installation files unless contracted for via additional Professional Services.
    b. **Rule Writing** – all rules will be developed by the client unless contracted for via additional Professional Services or delivered as part of the initial setup phase defined by the implementation specification.
    c. **Advanced Use Case Development** – DG is very flexible and can be used to meet a variety of requirements. The client is not limited in the number of use cases that they can implement, but support for the development and maintenance of the custom use cases must be contracted via additional Professional Services if the client is unable to develop the solution and maintain it.
    d. **Report Writing** – all reports will be developed by the client unless contracted for via additional Professional Services for delivery. Default reports are provided via the DG Content Server or in the DG ARC.
    e. **Workflow Integrations** – Integrations with third-party systems using API interfaces are not supported unless contracted via additional Professional Services for delivery.
    f. **Intelligence Feed Maintenance** – The client will maintain data feeds required for system operations (such as Custom Threat Feeds) unless contracted for via additional Professional Services.
    g. **Incident Response Services** –All incidents will be addressed by the client unless otherwise contracted with DG for remediation via additional Professional Services.

h. **Custom Training Delivery** – If additional training is requested by the client the Professional Services team can develop and deliver custom training required for Digital Guardian related content. Questions on what topics can be covered and what prerequisites are needed should be directed to the DG delivery team for proper assessment and estimation.

i. **Health Checks** - Following completion of the Client Health Check, recommendations for improvement will be provided by the PS team for review and approval by the Client. After approval, an estimate for completion of the recommended changes will be provided along with any estimated fees required for delivery. The Health Check can include the following:
   - Review existing policies to ensure they adhere to current policy best practices and that no policy conflicts are occurring
   - Confirm Policy assignment accuracy
   - Confirm DGMC user access accuracy
   - Identify opportunities to decommission old, unused or infrequently triggered policies
   - Identify opportunities to leverage out of the box (content server) policies in place of existing custom policies
   - Conduct Dynamic Group, Custom Configuration, Scheduled Task, Agent Version, OS version and Resource Review to identify opportunities for enhancement or cleanup.

7) **Technical Account Management (TAM)** – a named resource and client contact within DG Client Service Organization who understands the client's environment and provides priority support for any technical issues. This offering is generally consumed by large organizations (10k endpoints and up). Please see the TAM Offering Document for more information.