Desktop Encryption

Synoptek

Table of Contents

Introduction

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Desktop Encryption (the "Service").

The service definitions found herein reflect Synoptek standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect Synoptek's best practices or industry standards at its sole discretion with or without notice.

Service Offerings

Synoptek's Desktop Encryption is designed to provide the customer with a comprehensive managed encryption solution. The service provides data encryption for endpoints to ensure theft or loss of data to malicious actors cannot be utilized.

The service includes encryption enforcement, key management, as well as additional safety settings to offer enhanced data protection. A complete list of the included components is included in the Service Components table below.

Upon signing of a Service Order, Synoptek and customer will jointly schedule to deploy this service to subscribing devices. During this transition phase, and before Synoptek can transition services to supported technology platforms, Synoptek's service levels will be best effort.

This service is priced per endpoint (device).

SOLUTION PURPOSE

Good security hygiene calls for the protection of sensitive data. Many industry and governmental regulations now require encryption and have penalties for the release of unencrypted personally identifiable data, often making recovery from unintended data access arduous. However, user productivity is often impaired with traditional encryption software, and implementation can be difficult. Once implemented, there is a need for homogenous management of PCs and Mac's. Synoptek's Desktop Encryption solves for these issues.

Through Desktop Encryption, Synoptek enforces unobtrusive encryption and data security for all company and employee-owned devices in use within the customer's organization. Synoptek handles every aspect of the solution on the customer's behalf, from deployment to management. Desktop Encryption's remote cloud-based management allows troubleshooting and remediation to be handled remotely as well, translating into less downtime and maximizing employee productivity.

SERVICE CAPABILITIES

This service provides management for the Customer's Office 365 environment, text-based chat functionality, document management, video/audio conferencing (meetings), and collaboration.

FEATURE	DESCRIPTION	INCLUDED
ENCRYPTION ENFORCEMENT	Synoptek will provide and enforce full encryption for endpoints that meet requirements of various federal regulations where encryption is specifically mandated (e.g. HIPAA, HITRUST, PCI DSS, GDPR, CCPA, FEDRAMP, NIST 800, ISO 27001, etc.). While drive encryption is in scope of this service, file-based encryption is not.	Yes
ENCRYPTION KEY MANAGEMENT	Synoptek will house and manage all BitLocker recovery keys, even after endpoint is removed from system, Synoptek will keep keys until this service is terminated.	Yes
REMOTE DATA DESTRUCTION CAPABILITIES	The encryption key will be deleted remotely at customer request when an endpoint is marked as "lost". The Master Boot Record (MBR) and files will be securely destroyed when an endpoint is confirmed as "stolen" by the customer.	Yes
ENCRYPTION FOR PORTABLE MEDIA	Synoptek will provide encryption for portable media, such as USB drives/disks.	Optional Service – Additional Charges Apply

Service Deployment

Synoptek's Service Deployment team is responsible for the onboarding and offboarding of Desktop Encryption.

EXPECTATIONS DURING ONBOARDING

Architecture and Environment Requirements

- Synoptek will require the following of the customer during onboarding:
  - Question and Answer meeting with customer to set expectations during rollout and verify alignment
  - Previous encryption solution(s) on endpoints must be removed prior to assessment
  - Each endpoint must have a Trusted Platform Module (TPM) chip
  - User Acceptance Testing (UAT) group for testing the policies/rules settings
  - Endpoints must have operating systems that are supported by the OS vendor (e.g., Windows 7+, MacOS 10.13+, etc.)
    - *Note: Customer endpoints with Windows 7 Pro operating systems cannot be supported.*

Synoptek Deliverables:

- Synoptek will deliver the following to the customer after requirements (above) have been met:
  - Design policy tailored to customer objectives and need
  - Deployment Schedule
  - Follow up remedial actions
    - For systems that do not respond appropriately, Synoptek will reach out individually to those endpoints for troubleshooting
  - Reports on success of ongoing deployment

Service Support

Customer acknowledges and agrees that Synoptek may directly or remotely communicate with the agents we install on Customer's Devices for purposes related to the security and management, including, (i) Bitlocker recovery keys, (ii) issuing reports and alerts such as automated support requests and alert messages; (iii) providing support and maintenance services; (iv) applying policy and configuration changes; (v) extracting usage information, service performance information and event logs; and (vi) solution patch and update management.

SCOPE AND LIMITATION OF AUTHENTICATION AND ACCESS MANAGEMENT

This service includes the management of the following existing native operating system encryption capabilities:

- BitLocker (Windows 7+; Windows 7 Pro excluded)
    - Windows 7 may be subject to limited functionality due to its EOL as of January 2020.
- FileVault (MacOS 10.13+)

Specific Capability Limitations:

- Remote Data Destruction Capabilities: Remote deletion can only occur if the endpoint connects to the Internet once marked as "lost" or "stolen".
- Anomalous Log-In Detection: This is capability is not an intrusion detection & prevention system. It is simply a capability of the encryption management agent. Any remediation required by Synoptek requires ITaaS User subscription.

Exclusions: Unsupported Incidents:

These services are not intended as consulting, design, or implementation services. The following items and functions are not supported under Synoptek's Desktop Encryption:

- Administration of Customer's Servers or Network equipment (including server set up and enterprise server configuration changes unless otherwise noted in this service definition), On-site desktop support, Data backup and file restoration, Printer RMA issues, Smartphone, PDA and tablet applications, and devices and applications not provided by Synoptek unless specifically identified in a Statement of Work ("SOW") signed by the Parties.
- Strictly a workstation product. No PDA's, mobile phones, or servers.

Communication of Out-of-Scope Issues:

- Out-of-scope issues identified by Synoptek will be documented and communicated to the Customer.

- The customer will be responsible for management of its systems and must work directly with its manufacturer or vendor for assistance with unsupported, third-party applications and devices.
- The customer also is responsible for failures caused by viruses, user abuse, environmental conditions and other causes not within Synoptek's control.
- Out-of-scope can be remedied with Synoptek Professional Services on a time and material basis.

Requirements for this Service

The following specifications are required for Synoptek's Desktop Encryption:

- Customer endpoints must support BitLocker or FileVault in order to receive appropriate level of support for Synoptek's Desktop Encryption service.
- Customer managed endpoints must have an Internet connection. There may be additional required ports and protocols required in order to provision and enforce encryption.
- An authorized business contact must call Synoptek with any incidents, encryption problems, requests for remote data access elimination 'quarantine,' or 'kill,', etc. In order to receive appropriate service from Synoptek's Client Delivery Team.
    - Recovery keys can be made available to customers for their own assigned endpoint.
    - *Note: Synoptek requires written correspondence or ticket creation from the authorized technical contact prior to any lost or stolen status change.*
- The customer must follow set processes, as necessary, regarding any changes.
- The customer must notify Synoptek regarding any devices that need to be added or removed from management.

SYNOPTEK RESPONSIBILITIES

Synoptek can provide reporting on devices and associated encryption and security status. Synoptek will require the following to do so:

- Specific components to report on, scheduled interval of the report (weekly, monthly, etc.), and an email address for Synoptek to send report to, once generated.

CUSTOMER RESPONSIBILITIES

- The Customer must not perform any action on the System which would interfere with Synoptek's ability to monitor or manage the Service including, but not limited to the following actions:
    - Disabling or changing any user or service login accounts used by Synoptek for monitoring or managing the System.
    - Removing or changing any monitoring agent software settings.
- The Customer is responsible for notifying the Service Desk (Support@Synoptek.com) when affecting the System, or when performing any other activity which would result in an "outage" as seen from the monitoring system.
    - As security is application-dependent, the Customer is responsible for the overall security of applications and data. Synoptek is not responsible for the security or the integrity of software or data installed on the System or any applications which it is running.

Appendix

Synoptek provides optional services that the Customer may purchase for additional service management fees.

COMPARISION CHART: BITLOCKER (ALONE) VS. DESKTOP ENCRYPTION

Comparison Chart			
Desktop Encryption	**BitLocker (alone)**	**Desktop Encryption (w/ BitLocker)**	**Media Encryption: Additional Add-On**
Encryption Enforcement			
Encryption of Endpoint Data (FIPS 140-2 compliant), uses AES encryption algorithm in CBC mode with a 128-bit or 256-bit key	✓	✓	✓
Full disk encryption	✓	✓	✓
Remote enablement of encryption on user devices (no user interaction necessary)		✓	
Remote enablement of encryption on all other internal fixed drives		✓	
Encryption Key Management			
Key Restoration to protect lost/stolen device		✓	
Remote Data Destruction Capabilities			
Remote deletion of the encryption key and deletion of files based on pre-defined policy		✓	
Anomalous Log-In Detection*			
Alerting of invalid log-in attempts		✓	
Security Policy Setting *(Microsoft OS Only)**			
Security policy setting for customers without an Active Directory Domain		✓	
Encryption for Portable Media**			

Encryption of USB storage devices			✓
Device Decommission			
Secure, remote device decommission		✓	✓

** Optional Service*

*** Optional Service - additional charges apply*