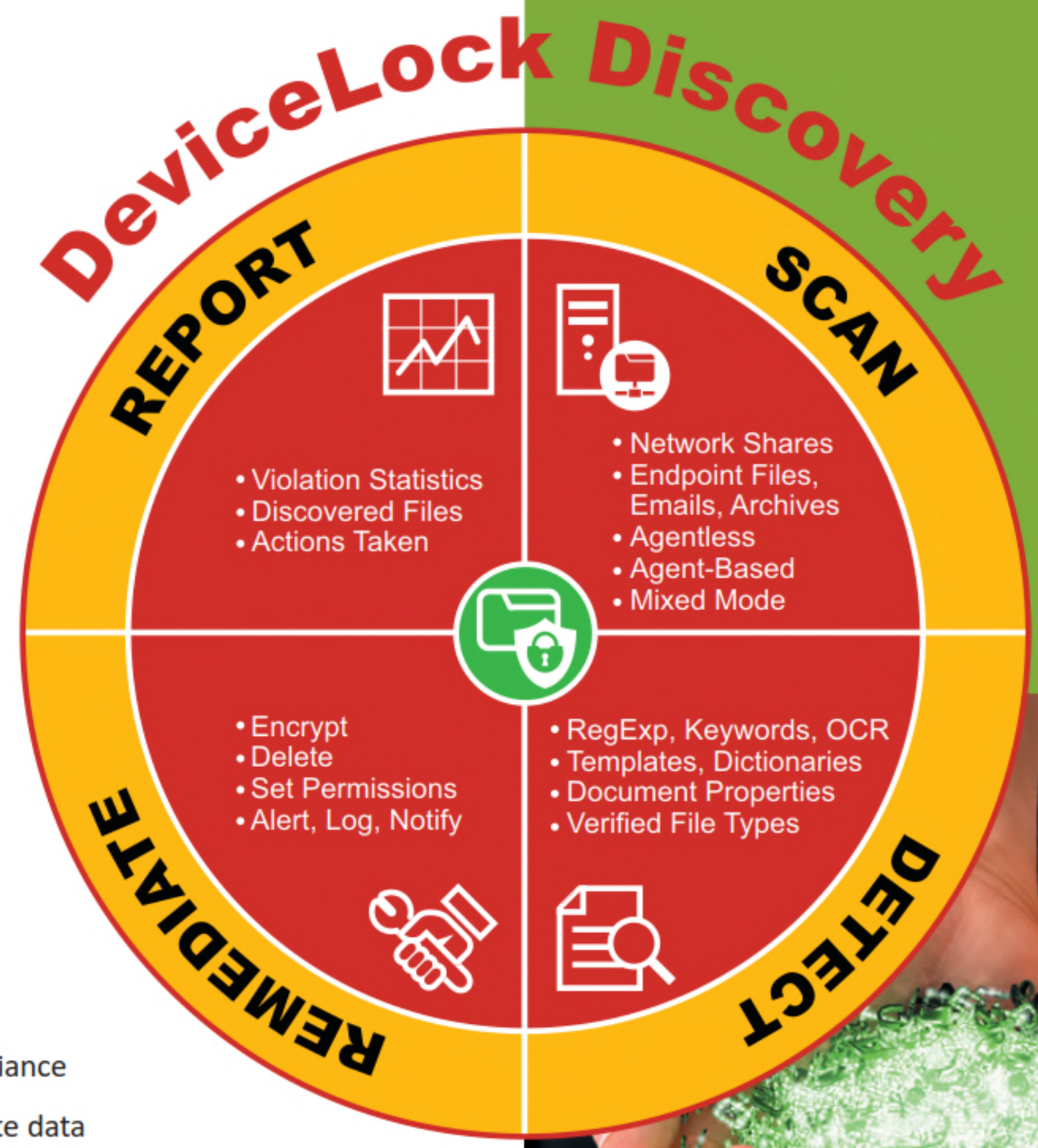
DeviceLock®

DISCOVERY



A functional component of the DeviceLock DLP Suite, DeviceLock Discovery enables organizations to gain visibility and control over confidential "data at rest" stored across their IT environment in order to proactively prevent data breaches and achieve compliance with regulatory and corporate data security requirements.

By automatically scanning data residing on network shares, Windows Servers, storage systems and Windows endpoint computers inside of the corporate network, DeviceLock Discovery locates documents with exposed sensitive content and provides options to protect them with remediation actions, as well as can initiate incident management procedures with real-time alerts sent to Security Information and Event Management (SIEM) systems and data security personnel in the organization.

DeviceLock

Structure

When deployed as a standalone solution, DeviceLock Discovery consists of the following components:

DeviceLock Discovery Server – a content discovery server software service that remotely scans files on network shares via the SMB/CIFS protocol, as well as deploys and manages DeviceLock Discovery Agents on target computers. Structurally, DeviceLock Discovery Server is an integral part of DeviceLock Content Security Server.

DeviceLock Discovery Agent – a lightweight content discovery client software for scanning accessible network shares and local file systems on endpoint computers (desktops, laptops or servers) that are not otherwise protected by full-function DeviceLock Agents.

Management console – a graphical user interface (GUI) for centrally managing all DeviceLock Discovery components. Depending on customer requirements and deployment specifics, DeviceLock administrators can choose two types of management consoles that include the DeviceLock Management Console (MMC snap-in) and the DeviceLock WebConsole.

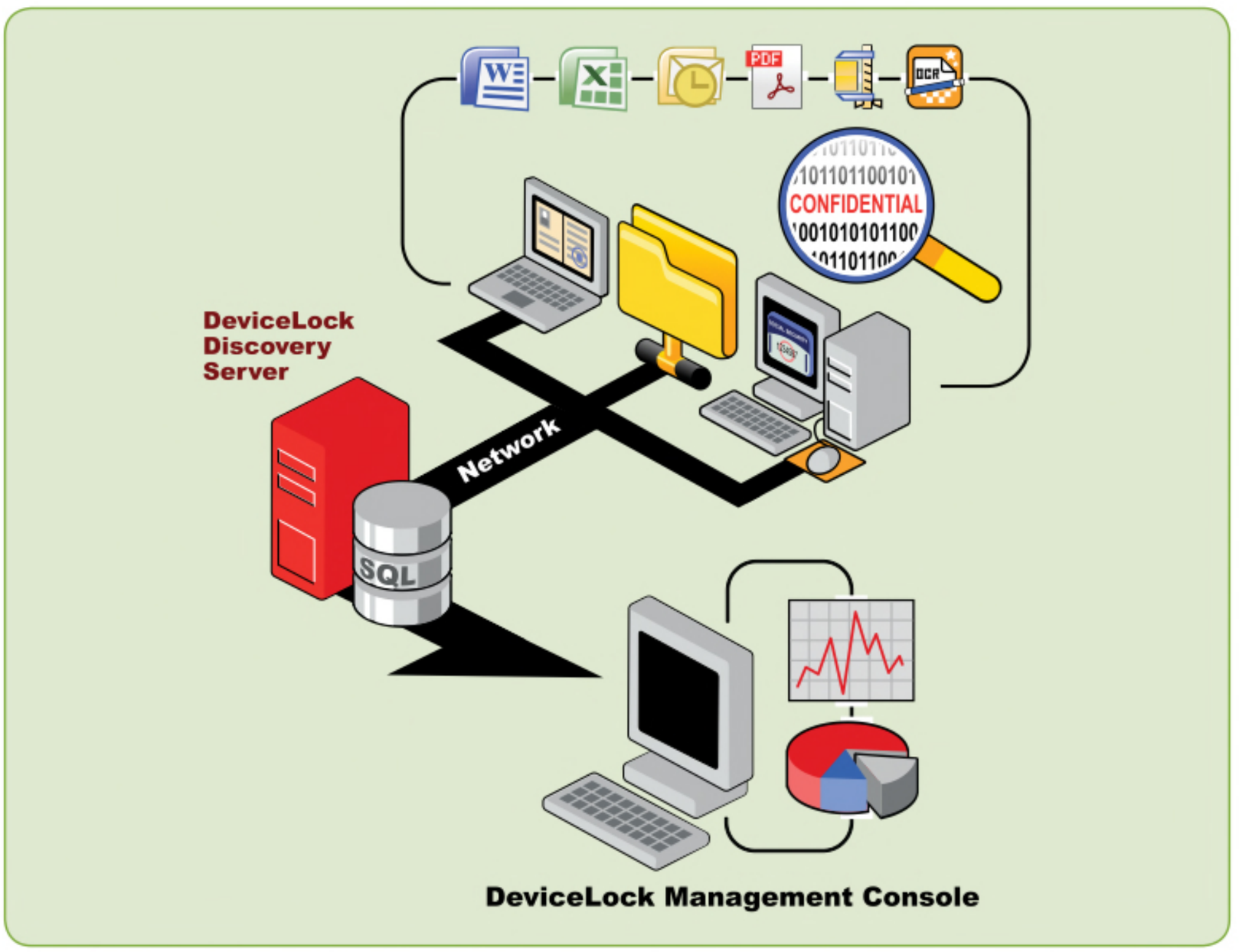
Where used together with other DeviceLock DLP components, DeviceLock Discovery can also utilize the built-in discovery capabilities of DeviceLock Agents for scanning data stored on their host computers and accessible network shares.

Operations

Depending on the network topology and other specifics of the protected IT environment, DeviceLock Discovery can perform scans in several scanning modes: agentless, agent-based, and hybrid scanning.

The agentless mode is used by DeviceLock Discovery Server to scan network shares and network-based storage systems accessible via the SMB/CIFS protocol. In this mode, the files are downloaded to the server where content inspection and detection take place, which is then followed by remediation actions that are enforceable over the SMB protocol.

The agent-based mode scanning is performed by DeviceLock Agents and DeviceLock Discovery Agents to scan local file systems on the computers where they run, as well as network shares accessible from these computers. In this mode, the content of local files is inspected locally by the Agent, which then enforces pre-configured remediation actions depending on the content discovered. Files accessible on network shares are downloaded to the endpoint computer where the Agent inspects their content, detects violations and remediates them per policy rules. Besides the critical ability to scan local file systems on corporate computers, the agent-based scanning delivers considerable performance advantages. First, local file system scans do not require sending files to the central server across the network. Second, spreading the CPU-consuming content inspection processing across many distributed endpoint agents reduces the load on Discovery Server.



▶ **DeviceLock Discovery: Locates documents with sensitive content and provides options to remediate them.**

The hybrid scanning mode combines both agentless and agent-based scans that are performed simultaneously by relevant DeviceLock Discovery components. In addition to enhanced data security with this hybrid method, the variety of scanning modes allows DeviceLock administrators to efficiently configure content discovery tasks in order to reduce network bandwidth consumption while achieving greater performance benefits.

DeviceLock Discovery scans can be initiated by administrators manually or can be configured to run on a schedule. Scan targets can be defined as computers and their groups, as well as network shares and storage systems in the corporate network. DeviceLock Discovery Agents can be remotely installed on and removed from target computers by the DeviceLock Discovery Server in a fully automatic and transparent to end users process.

Content Detection

DeviceLock Discovery can identify and inspect three general categories of content: textual data, binaries, and various other data/metadata types.

For detecting structured and categorized textual content, DeviceLock Discovery uses "keywords" (singularly listed or whole word phrases) and Regular Expression (RegExp) patterns, which can be combined with numerical thresholds and other parameters to specify triggering conditions in DLP rules. To ease the task of specifying data patterns, the product ships with hundreds of pre-built industry-specific, topic-specific, and country-specific keyword dictionaries, as well as RegExp templates for common sensitive information types, such as Social Security Numbers, credit cards, bank accounts, addresses, driving licenses, etc. In addition, customers can develop their own keyword dictionaries and templates, as well as modify pre-built ones for customized filtering needs. The accuracy of content detection is increased by morphological analysis of keywords in English, French, German, Italian, Portuguese, Russian, Spanish, and Catalan Spanish.

For detecting unstructured textual and binary content, DeviceLock Discovery uses data fingerprinting. The set of data fingerprints of an object, for instance a document, uniquely identifies both the entire document and its contents. By using data fingerprinting for content inspection, full copies or parts of textual and binary content can be reliably detected in scanned documents and files. The percentage thresholds of detected sensitive content that trigger DLP rules can be configured by security administrators to optimally fit the data security policy of the organization. In addition to textual and binary content detection, DeviceLock Discovery uses data fingerprinting to detect exact copies of any non-text files – such as images, design drawings, multimedia, and more. To simplify the data fingerprinting process for content inspection, DeviceLock Discovery supports automatic classification of corporate data into pre-built or user-defined classification levels. The database of classified data fingerprints is automatically populated by processing examples of sensitive documents when DeviceLock administrators place them into the folders of their relevant classification levels. There are five basic classification levels pre-built int the product, but customers can add or define their own categories as well. The built-in categories include "Unclassified", "Restricted", "Confidential", "Secret", and "Top Secret", but customers can use a combination of pre-built classifications and any of their custom-built ones in DLP policies.

A built-in optical character recognition (OCR) engine allows DeviceLock Discovery to extract and inspect textual data from images in graphical files of more than 30 formats, as well as from pictures embedded in documents and other data objects, such as emails, instant messages, posts to social networks, etc. With 30+ written languages recognized, this highly efficient OCR engine delivers to DeviceLock customers the ability to discover and protect exposed confidential data in information assets presented in graphical form. Unique to DeviceLock Discovery is that the OCR module runs in each of its enforcement components: the DeviceLock Discovery Server, the DeviceLock Discovery Agent, and the Devicelock Agent. This distributed OCR architecture tremendously improves the overall performance, functional scope, and reliability of the solution. Because graphical objects on endpoints are scanned and inspected locally by agent-resident OCR modules, this dramatically reduces the load on the Discovery Server and the scan traffic in the corporate network.

Verified File Type detection is another content-aware method used in DeviceLock Discovery, independently or in combination with textual patterns and data fingerprints. A binary content signature-based method is used to reliably detect the actual file type regardless of its displayed file extension or header. In addition, a wide set of file and document properties can be used to select a document, or class of documents, in order to enforce DLP controls over documents meeting only these criteria. Further extending its built-in content analysis techniques, DeviceLock Discovery can also recognize and use the classification labels assigned to documents and files by Boldon James Classifier products as detectors in DeviceLock DLP rules.

The flexibility of content-aware detection rules is further improved with compound content definitions that can significantly reduce non-sensitive, or "false", content detections. Multiple content matching criteria with different detection methods and content types can be logically combined together by using Boolean (AND/OR/NO) operators in order to create content definitions of practically unlimited granularity.

Remediation Actions

Once confidential content has been detected in a file stored in the wrong place, the following preventive actions can be enforced to remediate the exposure: Delete, Safe Delete, Delete Container (if a violation found in a file inside the container/archive), Set Permissions (for NTFS files), Log, Alert, Notify User, Encrypt (with EFS for NTFS files only).

DeviceLock

DeviceLock Discovery Specifications

Infrastructure (Installable) Components

- DeviceLock Discovery Server (a component of DeviceLock Content Security Server)
- DeviceLock Discovery Agent
- DeviceLock Agent (when used together with DeviceLock Endpoint DLP)
- DeviceLock Management Console (MMC snap-in) or DeviceLock WebConsole w/Apache

Targets

- Windows endpoint computers (file systems, email repositories, mounted peripherals), network shares, Windows Servers, storage systems

Discovered Content

- **Content Types Controlled:** textual content, binary data, data types
- **Textual Content Objects:** parsable file formats (100+) & archives (40+), images (OCR processing), Oracle IRM-sealed documents, files classified by Boldon James Classifier
- **Textual Content Detection Methods:** keywords and keyword dictionaries (160+ prebuilt, user-configurable) with morphological analysis (English, French, German, Italian, Russian, Spanish, Catalan Spanish, Portuguese, Polish), RegExp templates (90+ prebuilt, user-configurable), data fingerprints (partial/exact document matching) within Data Classifications
- **Binary Data Detection Methods:** data fingerprints
- **Controlled Data Types:** verified file types (5300+), file/document properties, embedded image properties, security contexts of Oracle IRM-sealed documents, data objects classified by Boldon James Classifier
- **OCR Features:** server and endpoint-resident OCR processing, 30+ languages, integrated DeviceLock keyword dictionaries and regular expressions, rotated/mirrored/inverted images

Scan Modes

- Agentless, agent-based, hybrid

Scan Operations

- Manual, scheduled automatic task execution

Remediation Actions

- Delete, Safe Delete, Delete Container, Set Permissions (for NTFS files), Log, Alert, Notify User, Encrypt (using EFS for NTFS files)

Other Features

- Static & dynamic target list configuration, discovery reports, automatic on-demand Discovery Agent installation/removal

System Requirements

- **Discovery Server:** Windows Server 2003-2019 (32/64-bit), Microsoft RDS, Citrix XenServer, VMware vSphere Desktop; 2xCPU Intel Xeon Quad-Core 2.33GHz, RAM 8GB, HDD 800GB (if hosting SQL DB, less if not); SQL Express or MS SQL Server 2005-2017
- **Agents:** Windows NT/2000/XP/Vista/7/8/8.1/10/ Server 2003-2019 (32/64-bit); Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View; VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC; CPU Pentium 4, 512MB RAM, HDD 400MB
- **Consoles:** Windows 2000/XP/Vista/7/8/8.1/10/Server 2003-2019 (32/64-bit); CPU Pentium 4, 512MB RAM, HDD 1GB

Licensing

Further extending the flexibility of DeviceLock DLP incremental licensing, DeviceLock Discovery can be purchased separately and used independently of other DeviceLock DLP products – so that customers do not have to purchase the basic DeviceLock component in order to deploy DeviceLock Discovery. At the same time, it can be licensed as an upgrade to existing DeviceLock DLP Suite or derivative DeviceLock module installations. Alternatively, customers who have initially purchased only DeviceLock Discovery can enhance it with other DeviceLock DLP functional components. New customers also have the choice of licensing the full DeviceLock DLP Suite solution that includes DeviceLock Discovery for a discounted price.