WHITE PAPER

LUCIDUM SMART LABEL

LUCIDUM

NOW PART OF cyderes

SMART LABELS

As data volumes have exponentially increased, the need for efficient and scalable categorization methods has become paramount in modern data management and security. Tagging, which emerged in the 1990s and gained widespread adoption with the proliferation of Web 2.0 technologies, has been instrumental in indexing and organizing large datasets. This method is particularly valuable in environments characterized by rapid data growth and user-generated content. As data management systems have grown more complex, tagging methodologies have evolved, culminating in the development of dynamic tagging and, more recently, the query-driven, variable-based tagging framework from Lucidum: SmartLabels. This patent-pending advancement significantly enhances the ability to manage and control extensive resources, offering new levels of granularity and automation in data organization.

#Tags:Background

Just as hyperlinks disrupted and improved the ability to move between content, tagging improved our ability to organize the newly exploding volume of data. Beginning in the 1990s and exploding with Web 2.0 with the introduction of social media and user-generated content, tagging demonstrated unique value indexing and made large amounts of data useful and accessible. In the management and security of systems and identities, the key:value pair structure of tagging added a new facet to the control of sprawling resources.

#Tags:Use

Tags are simple to implement and highly customizable and allow the creation of a taxonomy for gathered information. Typically, individually applied and manual, tags permit unlimited customization and data fit. Systems can be tagged by system type, use, compliance category, user groups, and more.

LUCIDUM

#Tags:Drawbacks

Tagging's strength introduces its detriments. Manual tagging is necessarily slow to respond to changes in environment. Identifying systems missing tags is often a predicate to mature management and security practices. In many cases, misspellings and variances are more harmful than missing tags, and the manual creation of tags increases the risk of incorrect tag assignment. It is also impossible, in practice, to apply tags globally or consistently.

#Tags:Drawbacks

Tagging's strength introduces its detriments. Manual tagging is necessarily slow to respond to changes in environment. Identifying systems missing tags is often a predicate to mature management and security practices. In many cases, misspellings and variances are more harmful than missing tags, and the manual creation of tags increases the risk of incorrect tag assignment. It is also impossible, in practice, to apply tags globally or consistently.

#Dynamic tagging:Background

Dynamic tagging emerged following the escalation of complex content and data. E-commerce platforms and recommendation engines pioneered the use of dynamic tagging that now is integral to many hyperscalers and system brokers. Dynamic tagging system provide default tags and suggested key:value pairs which, in turn, are importable by many management and security platforms. These tags can be automatically assigned and improve management, visibility, and prioritization.

#Dynamic tagging:Use

Dynamic tags can be used to group hosts by region and type, categorize services by function, and assign or identify the system and service owners. Dynamic tagging adapts to changing content but the tags themselves remain static.

Dynamic tags permit reliable segregation of hosts and services, reducing noise at support and response centers. The ability to filter out non-production service alerts from production alerts depends upon accurate and comprehensive application of dynamic tagging at the source.

#Dynamic tagging:Drawbacks

Dynamic tags are relatively easy to implement and manage but nearly impossible to customize consistently. Though they provide increased management and security operation discrimination and visibility, they do so at a foundational level, requiring a robust manual tagging process or extensive customization to fine tune. The algorithms driving dynamic tags degrade transparency and user input. Though valuable and necessary, there is a hard limitation on that value and extensibility, limiting the enterprise to low-level functionality even when imported into management and security systems.

LUCIDUM SMART LABELS

#SmartLabels:Background

SmartLabels were pioneered by Lucidum in 2023 with its patent pending in the United States. SmartLabels provide formula, query, machine learning, and AI-driven tagging of systems and identities. SmartLabels are applied dynamically based on the present condition of the system or identity and its match with the SmartLabel formula. SmartLabels can drive other SmartLabels using nested if- then-else statements with unlimited tagging functionality with values that include arithmetic operations and text management (concatenation, redaction, entry). SmartLabel rules are applied consistently and comprehensively, leaving no blind spots.

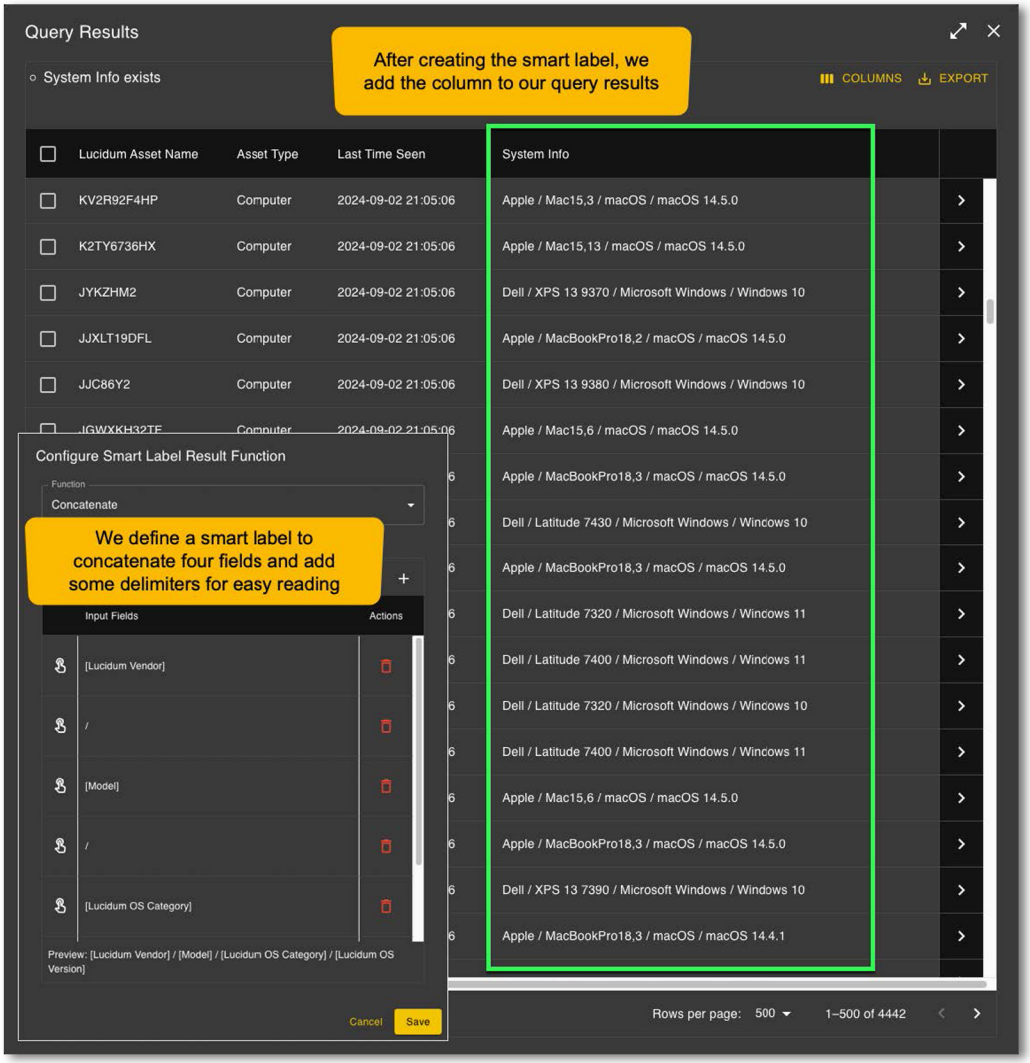
#SmartLabels:Use

Use cases range from the simple to the complex. At the foundational level, SmartLabels can be used to identify untagged or misspelled tagged assets, match their

characteristics (user, application, adjacency, originating image or pipeline) with a known-good tagged asset, and then generate and apply the standard tag to that previously untagged asset. One SmartLabel results in the immediate correction of an enterprise's tagging posture.

#SmartLabels :Example1

Simple SmartLabels can be used to standardize operating system and application manufacturers, products, and versions from infinite source descriptions without removing the original data.
Dynamic tags permit reliable segregation of hosts and services, reducing noise at support and response centers. The ability to filter out non-production service alerts from production alerts depends upon accurate and comprehensive application of dynamic tagging at the source.

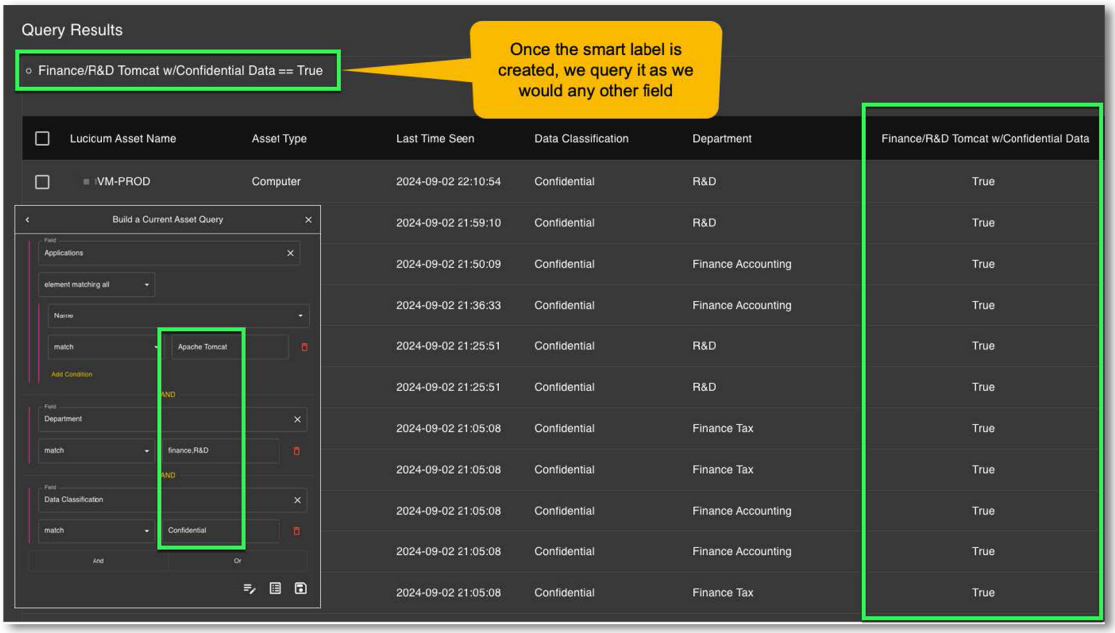


LUCIDUM

#SmartLabels :Example2

SmartLabels can be used to apply custom risk inputs derived from departments, information classification, adjacency, and security configurations.
Risk management is a combination of quantitative and qualitative. Quantitative measures can be derived from security configuration, vulnerabilities, information classification, and more. Qualitative measures are just as important to risk management and include the assessment of the relative risk of a department, role, location, application, and other factors.

In this example, the enterprise determined that the departments 'Finance' and 'R&D' were of inherently greater risk than the others. Further, owing to a temporary setback in system updates, those systems running the 'tomcat' application have increased risk. Finally, systems that store, transmit, or process confidential information also have increased risk. This SmartLabel formula identifies those systems that fall within the Venn overlap of these three qualitative variables and add weight to their risk score. The function of SmartLabels is such that if a system no longer meets the requirements of the SmartLabel formula, it no longer receives the concomitant increase to its risk score.



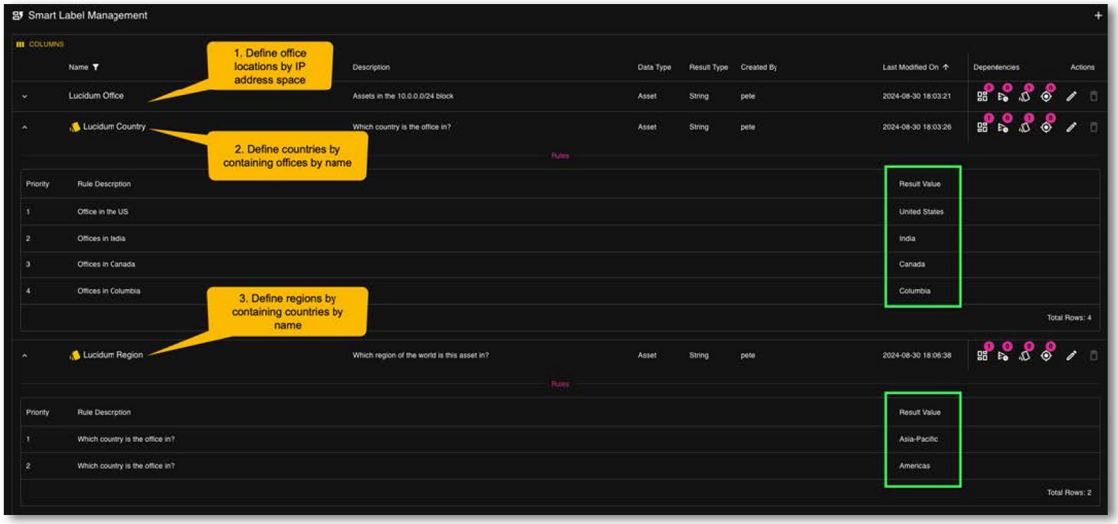
Lucicum Asset Name	Asset Type	Last Time Seen	Data Classification	Department	Finance/R&D Tomcat w/Confidential Data
iVM-PROD	Computer	2024-09-02 22:10:54	Confidential	R&D	True
		2024-09-02 21:59:10	Confidential	R&D	True
		2024-09-02 21:50:09	Confidential	Finance Accounting	True
		2024-09-02 21:36:33	Confidential	Finance Accounting	True
		2024-09-02 21:25:51	Confidential	R&D	True
		2024-09-02 21:25:51	Confidential	R&D	True
		2024-09-02 21:05:08	Confidential	Finance Tax	True
		2024-09-02 21:05:08	Confidential	Finance Tax	True
		2024-09-02 21:05:08	Confidential	Finance Accounting	True
		2024-09-02 21:05:08	Confidential	Finance Accounting	True
		2024-09-02 21:05:08	Confidential	Finance Tax	True

LUCIDUM

Useful SmartLabels include: the ability to determine system criticality and priority, during its use or ephemeral duration, by its users, applications, IP range, and over 200 other variables; identify 'crown jewels'; assign primary security analyst or support analyst; identify executive and departmental ownership; and more.

#SmartLabels:Value

SmartLabels are configurable through the Lucidum UI or through JSON files. Their configurations are fully transparent and manageable. The SmartLabels are themselves infinitely nestable enabling many layers of SmartLabels to drive superordinate SmartLabels .



The SmartLabel framework is driven by a user-friendly query structure that negates the need to learn a complex query language. The query structure is intuitive and conforms to technology and business logic, unlocking the ability to build a custom abstraction layer that fits your needs. Clean, well-managed data structures aren't a prerequisite to SmartLabels , they are the result.modern enterprises.

LUCIDUM

The progression from traditional tagging to advanced query-driven dynamic tagging systems illustrates the ongoing innovation in data categorization techniques. Traditional tagging provided the foundational structure necessary for basic data organization, while dynamic tagging introduced automated adaptability to evolving datasets. The advent of SmartLabels represents a significant leap forward, enabling highly customizable, formula-driven tagging that aligns with complex system requirements and business logic. As data continues to expand in scale and complexity, the capability to effectively categorize, manage, and secure it will be critical. The release of SmartLabels equips data management frameworks with robust, adaptable, and capable functionality to exceed the demanding needs of modern enterprises.

LUCIDUM