WHITE PAPER

Last MSSP Standing: Innovate. Disrupt. Win

LUCIDUM

NOW PART OF cyderes

Introduction

Lucidum is the industry's only comprehensive, intelligent, and efficient security data fabric pipeline that includes:

- 750+ connectors to security, IT, cloud, and other sources of data;
- Significant, user-friendly transformation machine-learning functions with five patents (four pending);
- Integrations with SIEM, Risk, Threat, Data, Ops platforms and all cloud providers;
- Set up, configuration, and integration within minutes, not weeks or months.

Imagine being the first MSSP in your vertical to cover everything in your customer's environment from Day Zero. Be the only MSSP your customer has ever seen that knows about adds, moves, and changes in the customer on premise and cloud environment – identities and systems – as it happens, not six months later. Innovate. Disrupt. Win. It's that simple.

As of 2024, there were over 3800 MSSPs in the United States. The growth in MSSP offerings far out paces the 11%+ CAGR demanded by the market. Standing out amid a stadium full of seemingly identical MSSPs is not just a marketing problem. As cloud environments and interconnected devices proliferate, threats increase in number and sophistication, and compliance tasks multiply, organizations require the services, coverage, and expertise that is more than a commodity offering.

The urgency to compete, scale, and offer a broad portfolio of products and services is frustrated by the already low operating margin. MSSPs struggle and fail every week, but you didn't get into the business to be average. You need high margin without sacrificing net promoter score. You need operational efficiency and the ability to improve your analyst/customer ratio without limiting your competitive offerings.

Lucidum delivers security data fabric to MSSP platforms, consolidating and simplifying customer source data, threat intelligence, cloud data and injecting the result into your platform. With over 700 data connectors and more being built every week, there is no product your customer has deployed that Lucidum cannot simplify, enrich, and inject into your platform. We deploy in less than an hour, reduce the volume of data in your platform,

LUCIDUM

We deploy in less than an hour, reduce the volume of data in your platform, speed queries, reduce costs, all within your current platform and using your existing workflows. No additional agents, no custom code, just one pipeline, transformed data, and your platform becomes a single pane of glass.

Lucidum MSSPs Delight Customers

On day-one, Lucidum MSSPs automatically generate a complete view of each customer's assets, users, asset ownership and data ownership, data classifications, security risks, threats, vulnerabilities, compliance posture, and more.

Lucidum is agentless and ingests read-only API data from IT all solutions in your environment, including operations, development, business, network, security, and HR solutions, and data lakes.

Lucidum applies rules-based algorithms, ML algorithms, network graph analysis, and NLP text mining to:

- find all assets
- find all users
- find all applications
- find "invisible" assets and users
- normalize ingested data
- deduplicate ingested data
- find and classify all data in data stores
- find relationships between assets, users, and data
- build enriched records for assets. Each asset record includes all the ingested data about the asset across all applications and also includes inferred data from Lucidum's ML.
- build enriched records for users. Each user record includes all the ingested data about the user across all applications and also includes inferred data from Lucidum's ML.

Using machine learning and AI to fill the gaps between security solutions, Lucidum MSSPs detect and classify all assets, users, data, configurations, and security configurations, **even those not detected by the solutions in the environment.**

LUCIDUM

Lucidum MSSPs see traditionally "invisible" assets and users including ephemeral assets (containers, serverless functions, and VMs) unmanaged assets (shadow IT, IoT and OT devices, and development and testing environments), zombie users (accounts with no directory management but still have access to applications or assets) and non-human users/system accounts (accounts that have access to applications or assets but do not appear in HR systems).

Among other ML tools, Lucidum uses Network Graph Analysis to find "invisible" assets. This ML tool finds connectivity patterns and communication patterns within the network that reveal unknown assets like IoT devices and OT devices and unmanaged users, like zombie users or non-human accounts. Network Graph Analysis also finds isolated subgraphs in the network graph that frequently indicate shadow IT.

As customer environments change and grow, and as new threats emerge, Lucidum MSSPs offer new services or enhance existing services. For example:

- Find all ephemeral assets and unmanaged assets, determine if those assets are missing agents or other security applications, create an automated action to remediate each asset, and bill the customer accordingly. The customer is covered continuously. Your service and billing continually fit the customer's growth and elasticity.
- Find zombie users and non-human users, apply security policies to those accounts, create an automated action to install security software for the accounts, and bill the customer accordingly.
- As a customer embraces cloud transformation, moving to hybrid-cloud or multi-cloud architecture, the Lucidum MSSP has a detailed view of the customer's infrastructure and can both accelerate these migrations and capture opportunities to upsell cloud products and migration services. Your customer? Completely covered in all the paths they take.

Customers seek MSSPs for their expertise and deep security knowledge and skills. Lucidum MSSPs include additional offerings, all derived from the same Lucidum feed into their platform. These include:

LUCIDUM

• Compliance auditing, gap analysis, and strategic planning services
• Data transformation and cloud 'lift and shift' projects
• Lucidum's detailed view of the customer's infrastructure and Lucidum's patented SmartLabels provide an opportunity for MSSPs to offer customized levels of service (bronze, silver, and gold) for each customer. For example, MSSPs can use SmartLabels to offer fully customized, automated tagging of assets to meet compliance requirements.

Automate, Consolidate, Simplify.

Lucidum MSSPs have their existing management tooling and workflow supercharged with streamlined, enriched Lucidum pipeline data. They are constantly updated with every customer's full population of systems and identities. Investigations, remediation, reporting, and even QBRs benefit from Lucidum's automation. The result is a product-driven MSSP that creates operational efficiency, not friction and complexity.

• **Automated monitoring.** At least daily and more frequently as required, Lucidum performs ingestion and applies ML algorithms to ingested data. Lucidum then updates asset records and user records that have changed and updates the vulnerability reference tables. Lucidum also keeps a record of changes for each asset, user, and vulnerability. With Lucidum, technical staff no longer manually audit customer's assets and security posture.

Lucidum MSSPs have an automated, detailed view of each customer's environment. As customer environments change and grow, Lucidum MSSPs automatically keep up with the changes:

- new assets (including invisible assets),
- new users (including zombie users and non-human accounts),
- new vulnerabilities,
- new threats, and
- new compliance issues.

LUCIDUM

- **Automated Security Tasks.** Lucidum includes a feature called Actions. Actions are no-code automations based on query results. Actions are built upon webhooks and APIs. Because Lucidum includes powerful automations, Lucidum MSSPs automate installations, upgrades, patching, and other security maintenance tasks, freeing up technical staff. In addition, Lucidum puts the data that SOCs and NOCs use most in the places where they need it most, like ticketing systems, communications platforms like Slack and Teams, and in platforms and data warehouses, like SIEMs and SOARs.

- **Automated Prioritization.** Lucidum's centralized visibility and analytics, patented risk measurement, and patented SmartLabels automatically prioritize and triage work, ensuring that technical staff concentrate on the tasks that matter most to the customer and the business.

- **No Switch Tax.** Lucidum includes pre-built integrations with 700+ security and IT management products, platforms, and sources. Lucidum MSSPs focus on core business tasks instead of integration. And Lucidum runs headless, using no-code webhooks to feed your existing platform and workflows. There's no new product to learn or screen to distract.

Lucidum MSSPs onboard customers quickly (hours not weeks), keep a constant pulse on changes to the environment, and do it all from their existing platform tooling and workflow. As a result, they win larger, more complex customers, scale their client base, and enter new markets without increasing headcount or overhead.

Want NPS? Because that's how you get NPS.

When the customer signs the contract, they expect that they're covered before the digital ink dries on the DocuSign. The fact that customer can't tell you what they're using, how much of it, or where immediately becomes your problem, your risk, and your reputation. Lucidum MSSPs not only know everything in scope from Day Zero but also show prospects what their existing provider doesn't see and can't secure. NPS from Day Zero includes:

LUCIDUM

- **Time to Onboard.** Lucidum MSSPs reduce onboarding work to hours. Lucidum MSSPs see all assets, all users, all relationships, and the current security posture of the customer, including risks, threats, vulnerabilities, and misconfigurations on day-1.

- **Time to Notify for Zero-Day Vulnerabilities.** Lucidum's detailed view of each customer's environment includes all applications, their versions, and where they reside. Lucidum MSSPs automatically and immediately identify all systems affected by zero-day vulnerabilities.

- **MTTQ (Mean Time to Quarantine).** Lucidum's detailed view of each customer's environment helps MSSPs immediately identify unprotected assets and unprotected users that do not meet security and compliance standards before the threat executes. Lucidum's automations can automatically quarantine these assets and users before remediation.

- **MTTR (Mean Time to Resolution).** Lucidum helps MSSPs immediately identify CVEs (common vulnerabilities and exposures) and KEVs (known exploitable vulnerabilities) that have fixes or workaround and then automate installations, upgrades, patching, and other security maintenance tasks. All without additional subscriptions or additional agents.

Lucidum MSSPs offer a bespoke but scalable experience for each customer using both the detailed view of each customer's environment and Lucidum's patented SmartLabels. Centrally managed, variable-driven, dynamic tagging and transformations that feel built to each customer's unique needs.

- During QBRs (quarterly business reviews), Lucidum MSSPs report not only security vulnerabilities and threats handled but also patching status, identity misconfigurations (shared accounts, missing MFA, etc.), and security maturity scores.

- Customers view detailed dashboards on security improvements and risk remediation in Lucidum dashboards. If the MSSP prefers to use Lucidum headless, the MSSP sends and displays Lucidum data in their reporting tool or the customer's preferred application.

LUCIDUM

- In addition to basic cybersecurity. Lucidum allows MSSPs to become trusted advisors, helping customers mature and improve their infrastructure through tagging policies, balancing assets across availability zones, and implementing DLP policies for confidential and restricted data.

Show the prospect that you see everything they (and their current provider) do not, cover the entire environment from Day One, continuously cover changes to the environment, have QBRs that matter: all without changing your platform or your workflow. NPS like no one's seen. It's that simple.

Conclusion

Customers want one thing: keep them safe from the moment they sign the contract. Keep them safe when they add new cloud resources. Keep them safe when they buy new laptops. Keep them safe when they open new offices. How hard could this be?

Of nearly 4000 MSSPs in the United States, only Lucidum MSSPs deliver completely and continuously. Lucidum's security data fabric connects to every and any security and IT data source in your customer's environment without agents, without custom configuration, without a change to your workflow.

Then Lucidum's machine learning and AI transform the raw data into consolidated, contextualized, and enriched results. Lucidum feeds your platform tooling with these results and you see all systems, all identities, their applications, configuration, condition, and risk. One hour, complete control of the customer environment, no switch tax.

See how Lucidum can help your MSSP. Contact us for a demo today.

LUCIDUM