oomnitza

USE CASE

Enterprise Technology Orchestration as the Touchstone for Cybersecurity

Introduction and Context

One of the first questions asked by security operations after a severe compromise indicator is, "What asset was compromised?" The answer to this question shapes the response and remediation steps. Similarly, a CISO must always be prepared to answer the core "Ws" security questions; who controls what assets, and where they are located (physically or in which cloud)? Unfortunately, for CISOs and security teams, answering these questions has become progressively more challenging:

- An increasingly larger percentage of employees are working remotely, connecting via VPNs, or worse, connecting through unsecured home wifi.
- BYOD has blurred the line between personal and business use of devices.
- Business applications have moved from on-premise to SaaS, meaning they live in the Cloud and are controlled and secured by third-parties.
- Cloud infrastructure is dynamic, distributed, and highly transient.
- SSO and employee directory systems are frequently circumvented by employees just trying to "get stuff done."
- The sheer number of assets requiring management across laptops, servers, mobile devices, on-prem software,
- SaaS, and cloud infrastructure, is increasing rapidly.
- Shadow IT is still an issue creating additional risk, and the new remote working model makes this even more difficult to control.

Given the increased attack surface, hackers are ramping up their activities across the board. Beyond these seven trends, CISOs and their security teams now face a barrage of connected peripherals (keyboards, monitors, mice) and the rapidly expanding Internet of Things. As a result, they must guard a broader and ever-shifting asset attack surface populated with "dumb" connected devices that may lack key security measures such as hard-to-guess default admin passwords, updated operating systems, and enterprise-grade encryption. Keeping an accurate inventory of all these new assets is a tall order. Each new asset class generates a new asset silo that must be managed independently, including CMDB, MDM, SAM, UEM, CSB, Cloud Infrastructure Management, and more. Maintaining proper system patches and security controls for all asset types requires automatic asset discovery and automated validation that patch controls are in place. Lastly, IT security teams are normally distinct from IT teams and often rely on their own separate systems. Creating collaborative and integrated workflows and workspaces is key to ensuring that both teams can perform their core tasks effectively with a minimum of manual or redundant efforts.

Use Case: Leveraging Enterprise Technology Orchestration to improve IT security

A key use case for Oomnitza is helping IT security teams track assets more efficiently, respond to problems more quickly, and maintain security compliance and data hygiene. Oomnitza also allows the flexible integration of IT security workflows with other tools in IT, Finance, and HR, such as anomaly alerting and workflow automation for complex multi-stakeholder security response tasks. This is in contrast to dedicated cybersecurity asset management products that are specific and limited to IT security processes.

USE CASE 1: AUTOMATED IT ASSET DISCOVERY AND INVENTORY

Autodiscovery allows deal teams to quickly survey and visualize the entire IT asset state across all silos of assets. This discovery includes laptops, mobile, on-prem software, cloud infrastructure, and SaaS. Oomnitza leverages existing agents in sub-systems (ITAM, CMDB, MDM, SAM) to discover and continuously update all assets attached to corporate networks. By tapping into existing ITAM capabilities and aggregating the information, Oomnitza lets security teams instantly answer critical questions such as:

WHO
owns a compromised asset or account?

WHERE
is the asset located?

WHEN
was the asset last used?

Equally important, Oomnitza reconciles asset counts and identification across silos to ensure accurate accounting. Oomnitza continuously generates and updates the following:

- *A comprehensive breakdown of IT assets in use by OS, device type, and location*
- *Recency of purchase to track end of life and refresh eligibility*
- *Upcoming end of warranties*
- *Deployed assets without an assignee*
- *Devices without an asset tag*
- *Lost or stolen devices by location*
- *Anti-virus compliance by location*
- *Last check-in for known devices*
- *Unencrypted devices by location*
- *A tally of the number of assets that are unaccounted for*

This capability is critical in incident response when IT security teams require confidence that they have the right data and are not dealing with duplicated or inaccurate asset owners, location, and status data.

USE CASE 2: AUTOMATED COMPREHENSIVE ENTERPRISE-WIDE PATCH AND CONTROL VALIDATION

Alongside asset discovery, as a second step Oomnitza also collects and aggregates patch and security control information. This saves security teams the hassle of reconciling patch and control status across multiple systems. It also allows security teams to create automated workflows and rules based on patch and control anomalies, such as out-of-date patch status or security controls being turned off on assets. Oomnitza helps security teams identify asset security coverage gaps either through rapid queries, automated reports, or conditional triggers to generate validations. Oomnitza can detect and instantly report on the following:

With a flexible and extensible API and connection framework, Oomnitza allows security teams to write their own connectors and workflows in Python to create bi-directional reporting and updating between Enterprise Technology Orchestration (ETO) systems and security management platforms like SOARs and SIEMs.

USE CASE 3: COORDINATED AND AUTOMATED CROSS-FUNCTIONAL INCIDENT RESPONSE

One of the most challenging aspects of IT security is mitigating business and compliance risk once an incident has been reported. Systems at risk might include "crown jewels," such as access to company financial accounts, PII and customer account data, and health records. Oomnitza simplifies the set-up and automation of workflows to ensure the fastest possible cross-functional response to an incident.

- Extensible APIs that can be quickly programmed to integrate systems across finance, HR, operations, and software development
- Visual workflow creation that allows IT security teams to create and set triggers for cross-functional responses to an incident

These features transform IT security planning into a holistic exercise that augments agile response and effective management of incidents.

Building a business case for Oomnitza for IT Security

To calculate and demonstrate the value of Oomnitza for IT security, create a business case and elaborate on the expected benefits. A list of benefits might include:

- More comprehensive and automated IT asset discovery
- Integration of multiple IT asset data repositories into a single source of record for querying and reporting
- Increased accuracy of IT asset databases
- Rapid mapping of any IT asset to an owner and location
- Rapid identification and mapping of security gaps
- Automated workflows to enforce security policies
- Visual workflow engine to set policy enforcement
- Extensible connectors to allow IT security to customize their own environment without code or integration contractors
- Bi-directional syncing of updated IT asset data into IT security platforms such as SOARs and SIEMs
- Cross-functional security incident response enablements
- Faster incident response and remediation times

Secondary benefits to IT security teams gained through the adoption of Oomnitza are also likely to be significant and might include the following:

Improved **IT SECURITY**	*Better* **ENTERPRISE-WIDE**	*More* **PROACTIVE**	*Simplified* **ASSESSMENT**	*More* **USER-FRIENDLY**
stance	security hygiene and awareness	planning for security events across teams	of the cost of mitigation IT security risks and improving security stance	environment for cross-functional collaboration and workflow design

To best illustrate the potential benefits in aggregate, paint a simple "before vs. after" picture that includes estimates of key metric improvements. Metrics might consist of a reduction in staff hours on manual tasks, reductions in incident response and remediation times, improvement in security coverage across the enterprise, and reduced number of breaches or Indicators of Compromise. This exercise should paint a definitive picture of the value of Oomnitza for IT security. Beyond these calculations, make sure to value the improved trust in systems and peace of mind resulting from creating a single, accurate, reconciled system of record as a foundation underpinning the most critical IT security tasks.

About Oomnitza

Oomnitza is an agentless enterprise technology orchestration solution for digital business. By consolidating technology asset data from siloed systems into a single pane of glass, our customers are able to optimize their technology spend, automate their governance processes to meet compliance and auditing requirements, protect from security risks, and ensure great employee experience and productivity. Oomnitza is headquartered in San Francisco.

www.oomnitza.com