WHITE PAPER

Transforming IT Asset Audit and Compliance Processes

Amid the ever-evolving compliance landscape, organizations struggle to track all their IT assets to ensure they're meeting standards and regulations. Enterprise Technology Management offers single-pane-of-glass visibility to minimize compliance risks—across data centers, devices, software, and the Cloud.

oomnitza

SPONSORED CONTENT InfoWorld FROM IDG

IDG COMMUNICATIONS, INC.

Regulatory compliance and auditing continue to grow in complexity—as do the risks of noncompliance. Organizations face fines, penalties, reputational damage, and security breaches when software, devices, and data are in violation of standards and regulations.

Yet, as enterprises expand their digital estates, the challenges in gaining visibility into all IT assets throughout their life cycle become daunting. Enterprises need granularity, certainty, and the ability to rapidly demonstrate compliance—no matter if the device or software is in the Cloud, data center, or a user's desktop.

Enterprise Technology Management (ETM) enables businesses to gain greater oversight and control over audit and compliance. This, in turn, mitigates the risk of violations that can lead to multimillion-dollar fines and other penalties, as well as bad press and a tarnished brand image.

Compliance is Much More Than a Checklist

At the heart of the problem is a simple fact: many organizations adopt a siloed and fractured approach to IT asset management. They often have limited visibility into systems, and they are unable to obtain a complete view of their assets, which exacerbates what are typically inefficient and error-prone—assets and data are typically misclassified or unaccounted for—compliance risks and liabilities grow substantially.

Making matters worse, it's not uncommon for organizations to view compliance as a check-box exercise. When specific regulatory provisions map to specific actions and tasks rather than taking an enterprise-wide approach, gaps are created. What's more, because compliance is broadly and deeply intertwined with cybersecurity and asset management, an organization will most likely lack the information it needs to achieve a high level of compliance with standards and regulations.

There's also the backdrop of consumer privacy. Regulations including the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have introduced strict privacy requirements and made it possible for consumers to control how and where their data is used. This challenge will grow; numerous US states and countries are considering new or more stringent regulations.

Organizations need a more granular way to identify IT assets in order to adhere to various standards and regulations. For example, one regulation may require consumers to opt in and another may require them to opt out. At the same time, the right approach would enable enterprises to seamlessly stay current with varying—and often quickly changing—requirements.

What's needed is a more holistic solution that orchestrates and manages compliance—while delivering a single view into all enterprise assets.

Critical compliance factors

A disconnected, piecemeal approach to IT asset management runs the risk of missing critical compliance factors, including:

- **Knowing which devices are active**
- **Identifying which devices are unaccounted for and therefore represent risk**
- **Knowing who is logging in from questionable devices or locations**
- **Determining whether software across the enterprise is up to date and patched**
- **Obtaining a complete inventory of Clouds, containers, software-as-a-service (SaaS) applications and licenses**
- **Identifying internet of things (IoT) devices and sensors, which may use cryptic device identifiers**
- **Determining which employees haven't read and accepted various documents, acknowledgements, and policy agreements, or undergone required training**
- **Keeping up with configurations. For example, mergers and acquisitions activity can complicate audits as assets from merging enterprises may be configured differently or in separate systems altogether.**

Filling the Gaps in Today's Asset Management Landscape

Achieving compliance improves when an organization can identify and monitor all IT assets from a central dashboard. This capability offers visibility into physical and virtual servers, Clouds and containers, SaaS and infrastructure as a service, desktop computers, tablets, IoT devices, and industrial control systems. It offers a coordinated approach to IT asset management, rather than a siloed one.

An orchestrated IT asset management solution also makes it possible to detect when a computer that was supposed to be decommissioned has just logged into the network, and identify devices in special economic zones that require specific disposal protocols.

Integrated management of IT assets can also identify logins and IP addresses spanning the entire organization and IT infrastructure. It finds devices, systems, licensing, users, and behaviors—and cross-references the data with various regulations such as HIPAA, Sarbanes-Oxley (SOX), GDPR or CCPA. This process delivers an accurate and real-time view of IT assets and spots situations that can lead to a violation, while knocking down data silos and moving beyond ad hoc point solutions.

Faster and more streamlined IT and SOC 2 audits also become possible with integrated asset management. An organization can see which assets are in use and detect what's not authorized. This includes shadow IT along with systems and devices that weren't authorized by the company. For example, an individual or line of business may have purchased and installed a SaaS app without IT's knowledge, thus putting control and governance at risk. Having this level of visibility streamlines audits—and can also help reconcile stolen or lost assets, or those not recovered after an employee left the organization.

A Next-generation Audit and Compliance Strategy

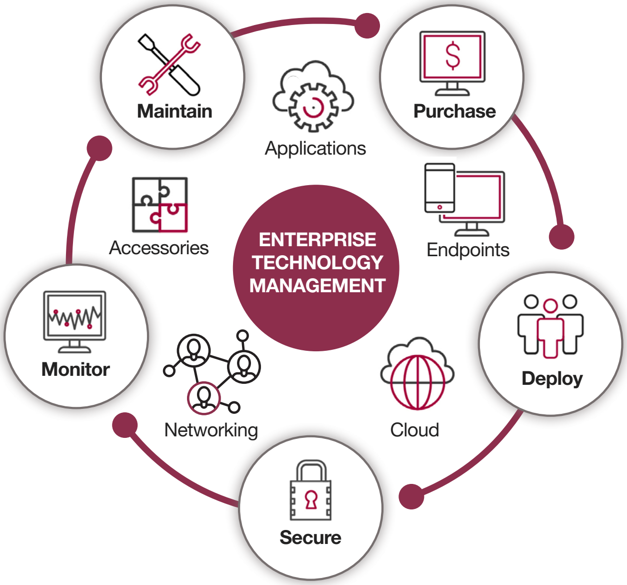
A single source of truth for IT assets makes it possible to more efficiently and effectively achieve compliance and governance. An organization moves beyond simply cataloging assets, and understands what data resides on specific devices and systems, how this data interacts with various systems, where it goes outside the organization, and who has access to it. IT has the ability to automatically define appropriate workflows and protections for specific devices and the types of data they hold.

An Enterprise Technology Management (ETM) solution achieves all of this by scanning the entire network—even out to APIs residing in a supply chain—to discover and identify all IT assets. It connects previously fractured asset management tools that typically resided in separate and siloed systems, with multiple interfaces and conflicting rules and audit processes that can lead to gaps and breakdowns. This includes tools like traditional IT asset management, software asset management, mobile device management, unified endpoint management, and configuration management database.

Using highly configurable workflows, it's possible to establish governance and controls through sound audit and compliance practices. ETM also constantly monitors the network and reaches out to the edge to spot changes and identify potential problems before noncompliance becomes an issue.

ETM reduces the challenges that extend across systems, offices, and geographies. In the end, it puts an enterprise at the helm of all of its various and constantly changing assets—and the sensitive data that continually moves around in them. This more advanced compliance solution ultimately locks down security and privacy controls—and data—to deliver audit and compliance capabilities that match today's business and IT needs. With a single pane of glass and real-time visibility, it's possible to identify vulnerabilities and catch potential violations through real-time alerts.

Figure 1. Technology Management for the Digital Enterprise



Oomnitza and ETM

Oomnitza is pioneering the ETM space while revolutionizing audit and compliance tasks. It eliminates silos and fragmentation while delivering visibility into sensitive data that must be tracked, audited, and managed effectively. With a broad and deep view into the enterprise—and out to business partners—an organization can construct an audit and compliance framework designed for today's world—with the flexibility and scalability to accommodate ongoing and sometimes abrupt changes.

Companies across multiple industry sectors have already embraced Oomnitza's software-as-a-service ETM offering, and are realizing a variety of cost-reduction, efficiency, and compliance benefits from its deployment.

As part of its ETM service, Oomnitza offers out of the box connectors to link to a full range of existing IT, Cloud, and security asset management systems. Once Oomnitza collects and rationalizes data from the underlying asset management systems, it enhances it with valuable metadata—such as an asset's projected lifetime, department, owner, and other information that device-centric asset systems rarely collect or exploit.

Oomnitza has worked closely with its customers to develop a large and ever-expanding collection of best-practice workflows, which the company includes as part of its core ETM offering. Most of the workflows involve asset life cycle processes such as on/offboarding, Cloud-instance instantiation and shutdown, and other common—yet formerly difficult to implement—management activities.

ETM represents the next step in asset management and security. It makes it possible to compress weeks of auditing into minutes or hours—and have far more accurate and detailed reporting in place.

Oomnitza offers three key capabilities

1

Data discovery and ingestion

Oomnitza's ETM solution looks to its supply chain via an API block to discover IT assets within minutes. It also ties together multiple point asset management tools and solutions. It collects, rationalizes, and then enhances this data with metadata such as an asset's life cycle, department, owner, and location.

2

Improved security, audit and compliance tracking

This robust asset identification process makes it possible to spot potential problems and take action based on classes of assets, department, geographic location, and much more. It also uses an ever-expanding collection of best-practice workflows to handle tasks such as employee onboarding and offboarding, Cloud-instance instantiation and shutdown, and device use and retirement.

3

Real-time monitoring

Assets and people come and go—and businesses are in a constant state of flux. An organization's current state of compliance is nothing more than a static snapshot of a precise moment. This is valuable but it doesn't guarantee that an organization will stay in compliance. Oomnitza offers dynamic monitoring—it updates assets continually and often in near-real time—which makes it possible to conduct spot audits and reporting at any moment with the push of a button.

Oomnitza ETM Audit and Compliance Features

- A central dashboard that serves as a single pane of glass
- Drag-and-drop configuration with built-in workflows, as well as the ability to customize processes
- A broad range of connectors to link to a full range of existing IT, Cloud, and security asset management systems (see the complete list here)
- The ability to account for all assets, including those that hold sensitive data
- One-click audit reporting
- A complete audit trail
- Automated and enforced governance processes
- Compliance with GDPR, CCPA, SOC 2, HIPAA and numerous other regulations
- Allocation of assets to the correct tax zone and cost center

Learn more about how Oomnitza's ETM solution can help your organization manage, secure, and optimize its full ecosystem of technology assets.

Visit **www.oomnitza.com.**

oomnitza