WHITE PAPER

Boost Security and Mitigate Risk with Enterprise Technology Management

Many organizations struggle to track and secure all their IT assets across the distributed enterprise. Enterprise Technology Management improves IT asset management and security to minimize risks—across data centers, devices, software, and the Cloud.

oomnitza

SPONSORED CONTENT CSO FROM IDG

IDG COMMUNICATIONS, INC.

The cybersecurity landscape has evolved dramatically as the digital estate has expanded. Sophisticated threats now target an expanded remote workforce as well as IT assets that are no longer in conventional places such as the data center.

Protecting the enterprise—including people, systems, and IT assets—has become a daunting task. Organizations face growing challenges tracking all the hardware, software, and systems they use. Too often, they're using siloed IT asset management systems to separately track devices, equipment, software licenses and other assets.

This fractured approach makes it difficult for IT and security teams to identify where risks exist, particularly in real time. A fully managed, centralized view of IT assets—across the organization, IT infrastructure, and even the supply chain—delivers the ability for organizations to not only mitigate risks, but also improve control, governance, and security posture. That's what can be achieved with Enterprise Technology Management (ETM).

Assets = Risks

As cybersecurity threats have grown, organizations have added more protection technology and tools. This is causing complexity and the potential for vulnerabilities through uncoordinated, unconnected systems and silos. This disconnect creates gaps, such as unsecured devices or the inability to apply controls and enforce policies. As a result, security teams find themselves flying blind, particularly when it comes to enforcing permissions and offboarding employees—and the devices they use.

Within a typical enterprise, massive numbers of devices are in use—computers, smartphones, tablets, servers, printers, and industrial controls, as well as IoT devices. It's often difficult to account for all these IT assets and verify that devices are configured correctly for users. It's not unusual for all these assets to wind up under the control of different applications and tools. These silos make asset management—and security—more difficult.

Yet, it isn't only physical assets that represent a problem. Enterprises must also account for operating systems, software, and firmware running on devices. Virtual machines, multiple and hybrid Clouds, and containers add to the challenge. SaaS subscriptions alone are overwhelming to manage, as the average company now uses 137 unique SaaS apps, according to a survey by Blissfully.

This complex environment makes it daunting, for example, to gain visibility into which patches and updates have been applied, whether users may have unauthorized access to devices, or to decommission a lost or stolen device.

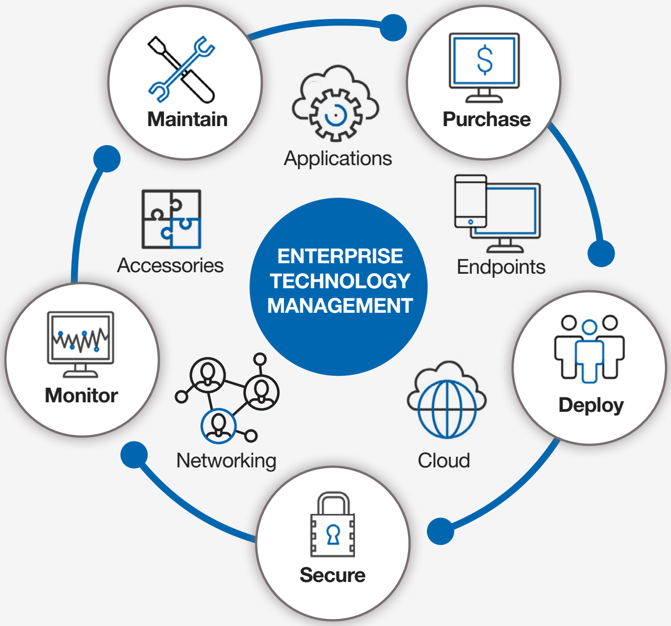
The task isn't becoming easier. Increasingly distributed workforces make it difficult to rely on IP addresses to understand what devices are in use, how and where people are logging in, and whether their behavior fits typical (and desirable) patterns. It's also difficult to ensure that systems, software, and antivirus subscriptions are up to date.

How Enterprise Technology Management Improves Security

An automated, orchestrated asset management solution can reduce risk and complexity. It makes it possible for an organization to automatically discover devices, software, and systems—including IoT devices that may have been installed and connected to the network without IT's knowledge. The right solution automates highly manual tasks that can cause configuration errors and provides the ability to spot problems before they occur.

Enterprise Technology Management delivers a single source of truth to eliminate siloed information and visibility gaps. It removes the need to manage devices and IT resources independently and manually through a variety of programs and tools. The right ETM solution reduces staff time and delivers a level of discovery, control, and technology management through automation.

Figure 1. Technology Management for the Digital Enterprise



A single pane of glass delivers deep visibility and control by pooling data from all IT assets. This improves risk and threat detection, while also reducing the overwhelming number of alerts that security teams must handle. It also extends visibility and protection to existing security tools and solutions, and to the metadata they generate. This allows staff to work more strategically.

In addition, ETM can reduce the costs associated with requiring multiple point solutions and manually managing all that information. Workflows can automate tasks and allow an organization to establish a framework that addresses its specific challenges and risks. At the same time, IT can automatically enforce rules and ensure that controls match roles within the organization to retain governance and minimize risks.

ETM: A Framework for Improved Security

ETM aggregates stovepipes and consolidates metadata and system information across numerous channels, platforms, people, and endpoints. The right solution provides five critical advantages:

1 Visibility

Using a web browser or a mobile app, security teams can drill down through IP addresses, network scanners, Mac IDs, and device identifiers to find everything that touches an enterprise. This includes legacy computing systems, storage devices, and IoT devices that use cryptic identifiers. ETM flags potential problems and identifies security risks that can span cloud instances and edge devices.

2 Integrated management and automation

Security teams benefit when there's a single system that sees across security information and event management solutions, endpoints, and Clouds to streamline alerts and notifications for incident detection and fast remediation. ETM layers on top of and integrates with existing asset management systems. It acquires, normalizes, and validates data, and establishes a single source of truth for all devices, software, and virtual Cloud services. For example, if a developer spins up an instance of a Cloud using default settings, ETM can instantly detect it and isolate or stop the instance until the settings are correct.

3 Critical information

Once it has collected and enhanced asset data, the ETM solution can then present IT and security managers with a single-pane view over their entire technology estate. It also allows them to implement best-practice workflows to simplify management of assets. What's more, the right solution reacts to changes in data. For example, if ETM grabs data from a security endpoint system and it sees that virus signatures on a particular machine haven't been updated for the last month, it can reach out to the appropriate system, such as a VPN, and block the user until the machine is secure. This makes it possible to turn integrated asset management into a strategic tool for security.

4 Customization

ETM makes it possible to turn information into action through preset workflows and the ability to set thresholds that trigger alerts or shut down a system or device. For example, if someone logs in from an unusual or authorized IP address, ETM can issue an alert or automatically block access. If an individual uses a laptop that was supposed to be retired or logs in from a device after a 30-day gap, the security team is notified. These alerts can be easily customized.

5 Strong audit and compliance tracking

Deep and broad visibility offers yet another advantage: strong audit and compliance tracking. This aids in adhering to various regulations and industry standards, but it also boosts security by ensuring that assets are classified correctly, the right controls are in place, and that shadow IT and unreconciled assets are temporarily blocked or permanently shut down. As regulatory compliance grows in scope and complexity, the need for a more sophisticated framework becomes an imperative.

Oomnitza ETM Improves Organizational Security Posture

Oomnitza is pioneering the ETM discipline. 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 security benefits from its deployment.

As part of its ETM service, Oomnitza offers a broad range of 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.

Organizations also gain the ability to adhere to key industry security standards and certifications. These include:

- SOC 2 Type 1 certification
- ISO 27001 certification
- CyberGRX Tier 2 certification
- Jira Security Self-A certification

ETM can transform the way an organization approaches security. It tears down silos, automates governance and delivers insights that take security to the next level.

Oomnitza ETM Capabilities

- Visibility into almost every type of asset residing within an enterprise and out to partners and supply chains
- Real-time information about devices and users
- The ability to establish, update and change workflows and rules quickly and easily
- The ability to build security into workflows by classes of assets, department, geographic location and more. Any attribute in a product can serve as a trigger.
- Use schedules, events and other criteria to define actions in the underlying technology asset
- The ability to set thresholds, notifications, alerts and automatic actions based on highly specific rules—and deliver them over numerous channels
- An API block allows organizations to reach out to third-party systems and initiate actions.
- Presets in Oomnitza allow security teams, with one or two clicks, to stop a Cloud instance, remove a user from SaaS software, or restart an instance.
- The ability to generate service desk incidents
- Auto-enrollment of new assets
- Robust reporting

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