omnitza

Use Case

Enterprise Technology Management for Security Enforcement

CONTENTS

Introduction and Context

The average total cost of a data breach to an enterprise is estimated at nearly $4 million. Ransomware attacks are growing exponentially, with annual damages already in the tens of billions of dollars. IT security teams are under intense pressure to improve enforcement, respond to incidents more quickly and improve the security posture of their organizations. They are often working with imperfect information and tools; it is not unusual for security teams to have outdated or inaccurate information for 20% to 40% of assets under enterprise management.

Enterprise Technology Management (ETM) solutions can address these security requirements by closely tracking the location and status of assets under management across multiple siloed systems. ETM can close gaps in security enforcement by:

DETERMINING who is using **which** device, **what** they access, and **where** they are located

ENSURING all devices are **encrypted**, virus-protected, and backed-up

QUICKLY identifying lost or stolen **devices** and blocking their access and security

SPOTTING anomalies and kicking off automated **workflows** to verify either an incident or a false alarm

VALIDATING on-boarding and off-boarding security steps to ensure all systems have **proper measures in place**

How ETM Can Secure Your Technology Portfolio

Most security solutions like Sophos, Crowdstrike and Trendmicro have dashboards that identify a domain or asset ID when an incident occurs. It can take many companies anywhere from 24 to 72 hours to identify the individual breach and location.

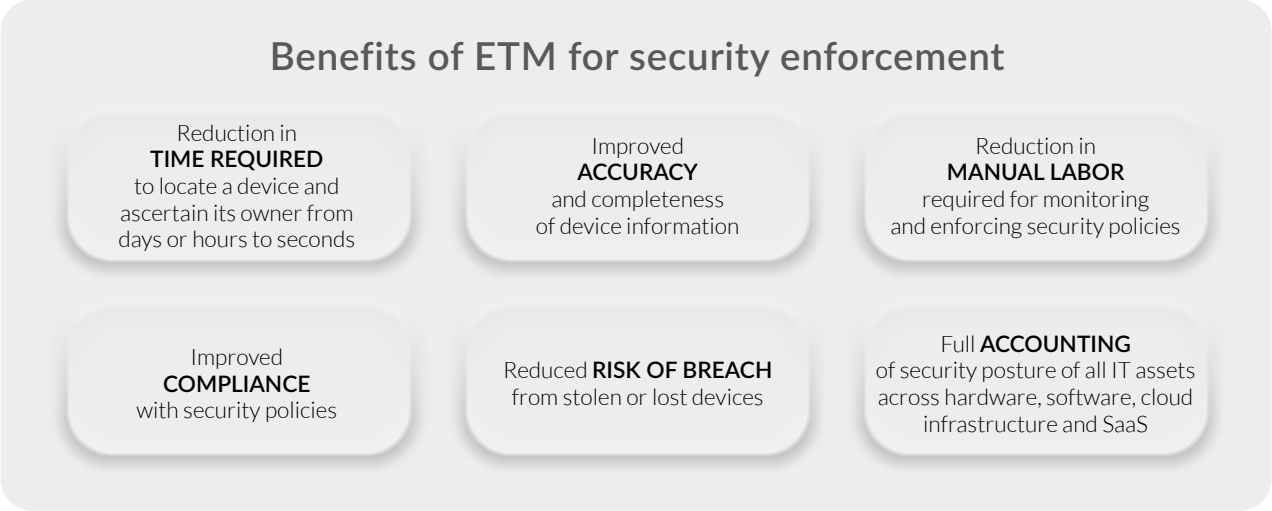
ETM is an "agentless" solution that aggregates and normalizes data from multiple siloed IT management systems, including security systems but also from IT Asset Management, Software Asset Management, Configuration Management Databases, Unified Endpoint Management systems and more. This provides a 10,000-foot view of security across all IT assets including hardware, traditional software, SaaS, cloud infrastructure, and connected devices or IoT assets. The view is also more accurate and trustworthy because the ETM can deduplicate assets and flag assets lacking key information required for security and compliance.

By constantly polling systems that have IP addresses or are operating on systems running on an enterprise network, IT security teams can create a holistic view of all the assets under management. This view can include asset status (patched, protected, version, etc.), ownership (group or individual), location (office, data center, or availability zone) and type.

A key part of this capability is ease of integration with identity management and HR systems; this creates a more accurate picture that goes beyond asset ID or domain ID. For example, if a salesperson based in San Francisco logs into a device from a new IP address in Brazil, the system can flag an anomaly alert. This can trigger an automated challenge to the salesperson or a phone call to request validation that they are in fact in Sao Paulo and not the Bay Area. IT security organizations can also set specific compliance rules and automated workflows for when a device shows up on network but unencrypted, kicking off emails to the employee and their manager, and blocking the device from accessing systems that contain PII or financial data.

Benefits of ETM for Security Enforcement

Deploying and using an ETM solution can help IT security teams achieve a more accurate and far more complete picture of assets under management. ETM can also help them respond more quickly, identify significant threats more readily, and enforce better security hygiene with less manual toil and greater automation. Specific key benefits of ETM for security enforcement include:



Conclusion: ETM Crucial for Security Enforcement

In today's risk environment, with the volume and severity of attacks rising sharply, IT security teams need a solid, accurate foundation of knowledge about the assets they must monitor and track. ETM provides this foundation and makes it easy to build complex workflows to react to changes or anomalies in asset status in an automated fashion without adding headcount or increasing manual labor requirements.

Oomnitza is the first Enterprise Technology Management solution that provides a single source of truth for endpoints, applications, cloud, networking, and accessories. Our customers can orchestrate lifecycle processes, from purchase to end-of-life, across all IT assets, ensuring their technology is secure, compliant, and optimized, enabling their employees. Oomnitza is headquartered in San Francisco, CA.
For more information, visit www.oomnitza.com.