

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:

Benefits of ETM for security enforcement

Reduction in
TIME REQUIRED
to locate a device and
ascertain its owner from
days or hours to seconds

Improved
ACCURACY
and completeness
of device information

Reduction in
MANUAL LABOR
required for monitoring
and enforcing security policies

Improved
COMPLIANCE
with security policies

Reduced **RISK OF BREACH**
from stolen or lost devices

Full **ACCOUNTING**
of security posture of all IT assets
across hardware, software, cloud
infrastructure and SaaS

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.