oomnitza

Joint Solution Brief

Integrating End-Point and Enterprise Technology Management to Secure Your Potential Attack Surface

CONTENTS

Introduction

The question for CIOs is quickly becoming "What can we not move to the Cloud?" According to Synergy Research, cloud infrastructure spending for Q2 2021 grew by 39% year-over-year, to $42 billion. Consultancy Gartner estimated in April 2021 that the total market for Cloud computing, including infrastructure, SaaS, BPaaS, cloud security and more - would hit $397 billion in 2022, marketing a decade of explosive growth. Every single part of the IT asset landscape is rapidly moving to the Cloud — even hard to move, legacy systems such as PBX and databases. Part of what has driven this shift is the increased imperative for employees shifting to a work-from-anywhere model and its sub-components; the necessity of supporting remote and hybrid work environments, demand for multi-channel delivery of and access to both internal and external services, and the insistence on superior customer and employee experiences by increasingly sophisticated workers and consumers.

The shift to Cloud has also increased the attack surface of most enterprises. Users have more devices, more online log-ins for services, and are more frequently accessing sensitive assets from insecure networks. This has made the old "hardened perimeter" defense paradigm less useful. This has forced enterprise IT and cybersecurity teams to place more emphasis on internal security and making sure that all systems are properly patched, versioned, updated and in compliance with security policies and regulatory frameworks. In addition, Cloud infrastructure is increasingly ephemeral and containerized, resulting in a constantly changing attack

surface. The shift to Cloud has clarified that IT asset management and endpoint management must also shift to Cloud-centric paradigms. IT asset management and security must be flexible and agile enough to handle the new era of "dynamic mobility" of the asset and use base, as well as the desire by IT and security teams to manage endpoints and assets using Cloudbased tooling. Making the need for agility and speed more compelling, the window between release of zero-day attacks, unknown vulnerabilities and the appearance of exploits in the wild has shrunk. The upshot? IT and security teams must know where all their assets and endpoints are located, who is on them, and what their security and patching status is at all times. Those teams must then be prepared to mitigate risks to those assets within a matter of minutes, not hours, not weeks or months.

How Automox Addresses Cloud Challenges

Automox is designed to provide agile and adaptive endpoint security for the era of dynamic mobility and rapid IT paradigm shifts by simplifying, streamlining and automating system management tasks and processes. Automox supports all three major compute platforms including Windows, Linux and macOS, as well as virtual servers running those operating systems. Built for the Cloud, Automox provides a single console for IT and security teams to manage and monitor endpoint security across all three platforms, from anywhere.

How Oomnitza Addresses Dynamic IT Challenges

Oomnitza is an Enterprise Technology Management solution that provides a holistic view of all IT assets in a single system, and empowers IT and security teams to manage the full lifecycle of assets and devices across all classes from a single unified view. Oomnitza enables two-way data flows between siloed solutions, creating an integrated view of the entire IT portfolio in a single, accurate database. An agentless solution with a REST API and extensible Python-based connector architecture, Oomnitza is pre-configured to connect directly with the Automox API. Oomnitza acquires, cleans and reconciles data, and empowers IT and security teams to create detailed, multi-step automated workflows and playbooks to execute in conjunction with Automox endpoint management and security processes. This also allows IT and security admins to gain a holistic view of users, business units, geographic locations and functions across all asset types (mobile, Cloud, physical) and across SaaS, IaaS, DaaS and other modalities.

Automox + Oomnitza: Benefits of the Joint Solution

Working together, Automox and Oomnitza can provide granular management for every stage of asset lifecycle from purchase to commissioning and imaging, to assignment and deployment, to updates and refresh, to retirement or reassignment. Oomnitza provides higher-level dashboards and enables integration of Automox with

Potential uses cases for the Automox – Oomnitza integration include:

- Unified patching and system maintenance across all three major operating systems
- Real-time patching and system updating on demand from the Cloud
- Automated endpoint hardening processes
- Continuous compliance verification and auditing
- Automated software recovery and repatriation at system, desktop and SaaS layers
- Closed-loop complete lifecycle management of software and endpoints

Demonstrated benefits of the Automox – Oomnitza integration include:

- Faster mean-time-to-remediate vulnerabilities and zero-day threat
- Reduced time spent by IT and security teams on patch management and endpoint hardening
- Reduced complexity of managing software updates and patching
- Improved software utilization rates and reduced time to reassignment / reuse of repatriated licenses and endpoints
- Reduced infrastructure costs due to consolidation of multiple endpoint management tools into a unified, cloud-based platform
- More reliable and trustworthy maintenance and verification of third-party certifications including HIPAA, NIST, PCI, ISO, SOX and SOC1+2 standards

Detailed benefits of the Automox – Oomnitza integration include:

- Out-of-the-box integration that can be set up in minutes
- Easy creation of additional connectors with Python-based API Automated field mapping for data as well as enablement of rapid custom field creation
- Integrated reporting of endpoint data into organization-wide report templates
- Easy creation of workflows spanning multiple systems and organizational silos for alerting, anomaly detection and remediation
- Integration between Automox and Oomnitza supporting two-way data pipelines between HRIS, finance, compliance and auditing, cybersecurity, and IT platforms

other normally siloed but crucial systems related to endpoint management including HR, SIEM, SSO, ticketing, and support.

Industry Use Case: Healthcare

Healthcare organizations often manage a wide variety of endpoint types. This often includes many devices that may be running older versions of embedded Windows or Linux software as well as consumer-grade devices running macOS or the latest Windows OS and cloud-based EMR solutions. These organizations have faced a dramatic increase in risks due to the recent success of ransomware campaigns and sophisticated attacks targeting COVID-19 resources. Healthcare organizations using Automox and Oomnitza together enjoy an improved security stance, faster security response, and more accurate records of endpoint status and history.

For enterprises and organizations in the healthcare field, the Automox + Oomnitza integration delivers the following specific benefits:

- Improved compliance with and enforcement of HIPAA and privacy regulations.
- Simplified endpoint hardening across multiple OS versions and OS platforms.
- Reduced staffing time managing endpoint hardening and easier spin-up of new IT and security staffs on endpoint management.
- Unified visualization and reporting of endpoint status and history.

Industry Use Case: Technology

Technology companies tend to have highly diverse IT asset footprints that can create greater complexity for patching and endpoint hardening. Due to partner and compliance demands, technology enterprises increasingly face the need to maintain strict compliance with privacy and industry certification standards like SOC2 and ISO 27001. Technology companies also face strong regulations on customer privacy and disclosure of breaches; for this reason, securing endpoints to prevent breaches or insider attacks is paramount. Many fast-growing technology companies also have IT teams that are dealing with multiple roles, including IT service management and cybersecurity. In this context, unified solutions that provide holistic views and easy integrations are highly valuable.

For techology firms, the Automox + Oomnitza integration has been proven to deliver these specific benefits:

- Improved security stance and accelerated patching capabilities.
- Higher IT staff efficiency in managing servers, laptops, and other endpoints from a single cloud-based console.
- Simplified integration with additional security management solutions such as Crowdstrike.

Industry Use Case: Financial Services

Financial services companies have come under increasing pressure by attackers seeking to take over accounts of customers, install ransomware or malware, and execute business email compromise campaigns. In addition, international banking standards under the Basel Committee now mandate that financial institutions undertake more comprehensive cybersecurity and technology risk management programs. Because financial services firms are often targeted by the most sophisticated attackers, maintaining a robust security stance and having real-time

For financial services firms, the Automox + Oomnitza integration provides the following benefits:

- Multi-platform endpoint hardening and management with a single lightweight agent.
- Real-time updating and patch installation capabilities.
- Status updates and real-time information on every endpoint under management including location, ownership, business unit, and recent access or activity.
- Recall of desktop and system software to block or control endpoints corrupted by malware, spear phishing or other sophisticated attacks.
- Direct integration with employee directories and SSO systems to enable security workflows triggered by changes to endpoint status.

update and endpoint ownership identification and remediation capabilities are critical.

Conclusion: Integration Delivers Time Savings, Cost Savings, Better Security Stance

With the Automox + Oomnitza integration, IT and security teams of all sizes enjoy simplified and easier management of endpoints across Windows, Linux and macOS, saving significant time for busy IT and security teams. In addition, the integration provides cost savings by replacing multiple installed solutions requiring a custom integration for holistic data aggregation and cleaning. The systems are both Cloud-based, eliminating costs for dedicated hardware or VMs. Because Oomnitza and Automox are both Cloud-based and are continuously updated and connected, IT and security teams enjoy faster remediation times, more frequent verification and more proactive patching of systems, leading to an improved security stance. The two systems can also easily tie into dozens of other systems integrated by Oomnitza, affording IT and security teams an accurate and easy to search or report on record of the status of all IT assets and endpoints across the entire enterprise technology portfolio.

About Oomnitza

Oomnitza offers the industry's most versatile Enterprise Technology Management platform that delivers key business process automation for IT. Our SaaS solution, featuring agentless integrations, best practices and low-code workflows, enables enterprises to quickly achieve operational, security and financial efficiency leveraging their existing endpoint, application, network infrastructure and cloud infrastructure systems. We help some of the most well-known and innovative companies to optimize resources, mitigate cyber risk, expedite audits and fortify digital experience.

Learn more at Oomnitza.com.