Solution Brief

Managing Security Requirements in a Hybrid IT Environment

CONTENTS

Introduction

Over the past two years, enterprises have rapidly shifted to a hybrid IT environment that blurs the lines of how technology is used and deployed. A hybrid environment overturns the traditional model of a hardened perimeter inside which all activities can be trusted. Cloud applications and infrastructure, work from anywhere, and the huge explosion of connected devices make this older security model obsolete and unworkable. By extension, the shift to hybrid IT dramatically expands and complicates the enterprise attack surface. Newer approaches are needed to harden enterprises and enhance their security. A modern, agile and flexible Enterprise Technology Management (ETM) solution that discovers, aggregates and orchestrates management of the entire hybrid IT environment is the foundation for this new approach to security. Agentless ETM pulls in data broadcast and collected by numerous sub-systems for device and service management to create a single, accurate database and orchestration layer that simplifies, streamlines, and improves the secure deployment, management and maintenance of hybrid IT architectures.

The 5 Drivers of Hybrid IT Security Risk

The Global IT environment of the average enterprise today is far more dynamic and risky than at any point in history. As the workforce continues to adjust to a "work from anywhere" model, devices and users are in constant motion. This means they are likely accessing cloud-based applications and company infrastructure through a wider variety of networking devices, including WiFi at public hotspots and their under-secured home routers. Rarely are these networking devices hardened, let alone managed by competent enterprise IT security teams. What's more, the average number of devices per employee has never been greater. Those devices might include laptops, tablets, phones and smart watches. Often, these devices may not be controlled or maintained by the company; workers access cloud-based services on unsecured browsers or from their personal smartphones. Making things more risky, employees increasingly connect to these devices using bluetooth accessories, including headsets or earbuds, keyboards, and more.

1. Migration to the Cloud

In the cloud, hybrid IT takes on a different meaning. Employees have rapidly shifted software consumption from programs running on their devices to Software-as-a-Service delivered via browsers or thin-client applications using HTTP as a transport layer. From Microsoft Word to Adobe's Creative Cloud to Salesforce CRM, software from the cloud is becoming the dominant delivery mode. In the not so distant future, over 90% of all applications will be delivered via the cloud; for many younger companies, this is already the case. A similar shift is ongoing in infrastructure; companies have moved from physical servers and networks to cloud-based infrastructure for virtualization technologies that multiply the number of systems running on any given piece of hardware. These virtual and cloud servers are ephemeral, spinning up and down as needed, and moving workloads around the globe to be closer to the customer or to be located in the right geography to comply with data and privacy laws. This creates a constantly morphing and moving attack surface that requires a new level of monitoring and management to handle.

2. APIs for Everything

Accompanying and accelerating the growth of hybrid IT is the rise of APIs that connect applications to one another, internally and externally. Enterprises access a growing array of APIs to talk to partners, software or hardware, or to add new capabilities like Kubernetes and microservices. The typical web application today access dozens of internal and external APIs. Each API provides a potential security hole that might allow attackers to take over infrastructure or user devices and co-opt them for malicious ends.

3. Explosive Growth of IoT

Inexpensive sensors and ubiquitous high-speed network connectivity have led to the growth of the Internet of Things. Today many billions of connected devices are located inside of or are connecting to corporate networks of factories, hospitals, transportation companies and more. This new monitoring and management layer for the world of industry, healthcare and government presents an even greater expansion of the attack surface; IoT nodes can be co opted for malicious purposes. Ensuring that all these IoT systems are properly secured and hardened is exceptionally challenging.

4. 5G Network Expansion

The coming age of 5G Connectivity will mean significant improvements in wireless data connection speeds from the global cellular networks. This will accelerate the expansion of hybrid IT for several reasons. 5G is nearly 100 times faster than the networks that preceded it, which will not be that noticeable to humans, but will be very noticeable to IoT devices (for example, autonomous vehicles, which absolutely require a hyper-fast connection). Because 5G provides faster connectivity, more users will run more of their work on the network and disconnect from corporate WiFi. As well, 5G will also deliver greater capacity, enabling a rapid expansion in IoT and connected devices. Lastly, 5G will power a new and more interactive generation of cloud-native applications, pushing more computing to the edge and creating more distributed architectures that require more robust orchestration and tracking capabilities.

5. Work from Anywhere

COVID pushed enterprises to equip employees to work from home. This spurred many of them to work from anywhere, including vacation destinations and global cities far from their home base. Even as offices are (sort of) reopening, employees have made it clear that they are unwilling to give up hybrid work situations and demand to work from anywhere at least several days per week. In other words, IT security teams now must design security processes and solutions to function effectively even as the geolocation of employees could be almost anywhere.

How Hybrid IT Increases Specific Security Risks

The broad trends discussed in the previous section filter down to increases in specific security risks including, but not limited to, the following.

Unsecured devices (AV and encryption)
Because more devices are connected to enterprise applications and often on networks that are not under the control of the IT team, enforcing encryption and AV is more challenging.

Under-secured networks (VPN)
Similar to above, employees are accessing critical applications and infrastructure from home broadband networks, usually over routers that often are running default admin and password combos straight from the factory. These under-secured routers mean VPN use is even more important, as is anomaly detection based on user, device and asset behaviors.

More complex employee and asset behavior patterns
Users may be accessing networks or using devices in remote locations that may appear to be anomalous. Usual patterns of usage may be scrambled or transformed by changes in time zone or work behaviors—parents working from home who pause in the afternoon then work late into the night for example.

More broadly distributed infrastructure
More advanced enterprises deploying distributed applications in different availability zones or across multiple clouds can present opportunities for attackers to exploit the geographic diversity of infrastructure assets by timing attacks to off-hours for security teams or compliance checks (at financial institutions, for example).

What is ETM and How it Addresses Hybrid IT Security

Enterprise Technology Management is a new category of solutions that provides a comprehensive foundation for building out a hybrid IT security program. ETM functions as a meta-layer atop numerous other IT management and orchestration systems; it is agentless and aggregates data from sub-systems such as ITAM, SAM, MDM, UEM, CRM, SSO, employee directories, HRIS, cloud brokerage, DevOps, ticketing and CMDB tools. ETM cleans, reconciles, and validates data from all these systems with continuous discovery pulls, creating an up-to-date, accurate single-source-of-truth for all hybrid IT data across devices, connected peripherals, IoT, SaaS, PaaS, and IaaS.

Unlike any of those systems, ETMs create two-way data channels between other systems, enabling IT security teams to build multi-step workflows that automate complex processes across multiple departments. These workflows can be conditional and can trigger actions in integrated systems such SIEMs or threat intelligence alerting. ETM is particularly useful for securing hybrid IT because it provides a flexible, extensible and holistic solution to continuously discover, aggregate and validate device information to provide the most accurate and up-to-date view of your security stance. ETMs can then become mission control for orchestrating security policies and responding proactively to anomalies, or accelerating incident response by quickly tying any affected or breached asset to its owner, location, business unit and exposure to networks and other assets. Specifically, for hybrid IT security, ETMs can:

AUTOMATE
anomaly reporting and provide role-based dashboards sliced by asset type, employee role, location, business unit, or asset status

MANAGE
the entire IT environment as a holistic entity for anomaly detection and incident response

ESTABLISH
user-specific policies (or permissions) across all devices, software and cloud services accessed or controlled by a user

PUT IN PLACE
granular management and controls across the entire lifecycle of the asset to ensure it is properly secured, patched, assigned, deployed and then decommissioned

With ETM, IT security teams can quickly react to changes while flexibly and reliably orchestrating security processes and workflows to minimize security drift and maximize coverage of assets with existing security solutions.

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.