Technology Orchestration For Enhanced Security

TABLE OF CONTENTS:

Executive Summary

One of the biggest issues facing cybersecurity teams today is obtaining an integrated and holistic view of their organization's entire technology portfolio. What the best teams are realizing, as well, is that once all the crucial IT asset management subsystems are integrated and turned into data feeds, then an orchestrated approach can manage technology assets like code. This enables broad improvements in coverage, scalability, and response times that enable step-function improvements in security postures. This white paper examines the new requirements for an orchestration-driven solution, the benefits of those systems, and what attributes they should have.

Introduction: a serious Chrome vulnerability highlights the need for technology orchestration

Google Project Zero is a superstar security team inside of the search giant tasked with finding the worst hidden vulnerabilities in the world of IT. Formed in 2014, Project Zero has consistently identified and suggested patches for the dozens serious zero-day vulnerabilities affecting popular operating systems and software such as browsers. Project Zero has over the course of 2020 discovered multiple bugs impacting Google's own Chrome Browser. Google has issued patches for all of the bugs but users aren't necessarily updating their browsers in a timely fashion. Research by Menlo Security published in November 2020 found that 83% of users were not running the latest version of Google Chrome.

For IT administrators and security teams, this presents a huge problem. Here's why. Many business users are loath to upgrade their browsers to the latest versions for fear of disruption or that the browser will no longer work with internal applications running on dated platforms. In fact, financial sector companies and others in regulated industries often run several versions behind the latest specifically to ensure continuity and, ironically, due to security concerns with upgraded browsers. While most of these organizations are running extended support versions, those versions may not be patchable against cutting edge exploits. Then there is the reality of work from home and employees increasingly accessing work assets from their home devices. Consumers

"Many business users are loath to upgrade their browsers to the latest versions for fear of disruption."

are far less likely to upgrade browser versions and if they are working from home they are more likely also to access SaaS, cloud, or other technologyassets from their personal devices.

In case of a breach, then, robust integration and orchestration capabilities across the entire technologyportfolio become crucial. The security team must be able to tie any asset to the user that owns it and map their location and history. This includes laptops, tablets, smartphone, SaaS, cloud infrastructure, and standard installed or local software. Consider the following scenarios:

- A sniffer installed on a personal laptops is used to sniff credentials for logging into a sensitive cloud server or business-critical SaaS platform
- An unpatched corporate browser is used to deliver ransomware
- The browser vulnerability allows installation of malware that exfiltrates sensitive data and passwords which are used in social engineering attacks

In all of these instances, a crucial means of preventing or identifying and remediating risk and cybersecurity threats is by enabling comprehensive integration and orchestration of your entire technology portfolio from a single system. In other words, a single pane of glass to acquire, validate and verify across the entire enterprise the status, ownership and location of all managed assets. The benefits of such integration and orchestration include empowering security and IT teams to

more quickly and easily:

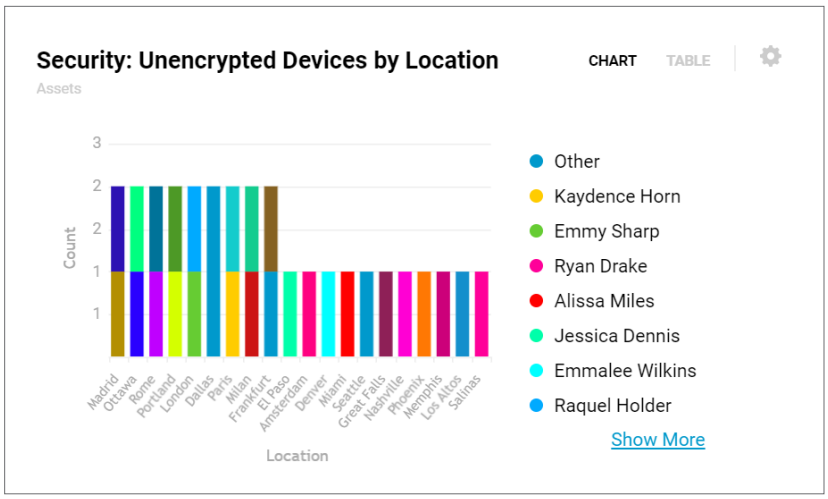
- **Identify and close gaps** in security enforcement
- **Determine who** is using which device, what they access, and where they are
- **Ensure that** all devices are encrypted, virus protected, and backed-up.
- **Map all assets** back to individual users
- **Identify devices** that have been lost or stolen in order to block their access and security
- **Manage, monitor and validate** that remote workforce protocols are followed
- **Ensure that all users** of cloud infrastructure assets adhere to security best practices

In this white paper, we will dive deep on this topic to explain in more detail how a modern technology orchestration solution might work. We will attempt to demonstrate the benefits of more robust orchestration and integration that seamlessly ties together systems for security, IT, finance and HR to create a unified security view and workflow engine for the entire enterprise.

Why siloed technology asset management is bad for security

From desktops to laptops to smartphones and tablets, the hardware landscape has evolved and grown more complex. Similarly, the software landscape has expanded from big system software to include first desktop and server software then on to Software-as-a-Service and cloud infrastructure. In our connected era, more and more devices - phones, video screens and conferencing systems, keyboards, and cameras - are attached to networks and communicate via IP and HTTP.

Unfortunately, this explosion of systems and devices has created a complicated spaghetti web of categories to manage each new layer of technology. The average IT department today must deploy multiple systems



to manage and secure its technology portfolio including IT asset management (ITAM), software asset management (SAM), configuration management databases (CMBDs), unified endpoint management (UEM), mobile device management (MDM), anti-virus and anti-malware software, virtual private network software, and cloud service brokerages. To control access and authorization for these systems, IT managers usually deploy both an employee directory (for some access) and a second SSO (for more robust control). Within categories, IT teams must manage two systems doing the same thing - one for Mac, one for Windows, one for iOS, and one for Android.

For the most part, all of these different components have different management consoles. An IT team looking at these systems is effectively peering at the world through soda straws, seeing a small picture that is useful but hardly comprehensive. Because most of these systems use different formatting schema for data or have different API structures, unifying the contents of these systems into a single pane of glass is challenging. More challenging still is eliminating redundant and incorrect data entered into these systems, which reveals the final big challenge. Most of these systems lack crucial automation components that require some manual work on the part of IT teams to collect, verify and deduplicate data.

All of these issues make it challenging to track assets in a holistic manner. More broadly, legacy ITAM becomes a liability rather than a strength: teams put more energy and resources into the discipline while receiving insufficient value from the practice. It is critical to think through the elements of why technology orchestration is so important.

Why technology orchestration matters so much for security

Cybersecurity today is increasingly about speed and coordination. Attacks are constant, faster, more varied, and harder to spot. Security teams require an integrated and holistic view of their entire asset portofolio. They also need the ability to integrate that view with other security tools and leverage that integration to orchestrate smarter, faster, and more effective policy enforcement. This orchestration must be easy to implement and must be cross-functional; while security ownership resides in the cyber team, the practice of proper security hygiene spans multiple stakeholders and roles. Here's a rundown of why robust technology orchestration is crucial to maintain a strong security posture.

SPEED

Hackers are moving faster than ever to exploit vulnerabilities and flaws. In April 2020, FireEye Mandiant Threat Intelligence analyzed 60 vulnerabilities that surfaced between Q1 2018 to Q3 2019. The majority were zero-days, exploited or announced before a patch was available. More than a quarter of those vulnerabilities were exploited within one month after the patch date. Smarter hackers, often led by state-sponsored Advanced Persistent Threat Groups (APTs are moving faster than ever to gain an advantage over white hat forces. By integrating your technology portfolio and creating a systematic way to poll and validate patching and coverage, you are upping your security metabolism to match that of the hackers.

ACCURACY

While zero-days are a major threat, the majority of attacks still result from simple misconfigurations of security controls or failure to apply existing patches - often for months or years after release. For this reason, building an accurate picture of security coverage and gaps is crucial in shoring up your security stance. While this has long been a goal, comprehensive technology orchestration improves accuracy by making control and status validation programmatic and automatic. In addition, by adding an intelligent data layer that acquires, normalizes and analyzes all technology portfolio assets, technology orchestration can reduce unnecessary work by removing duplicates and verifying the accuracy of asset data (owner, location, status, network, usage).

SCALABILITY

For fast growing companies, such as those approaching IPO, scalability of systems is critical. Linear scaling is expensive and requires unsustainable human capital additions. The grunt work of technology asset management for security is also unpleasant, tedious and slow. By introducing a programmatic and automated orchestration and integration layer, companies can improve their ability to scale out not only IT functions but also ensure that security coverage scales along with it.

FLEXIBILITY AND EXTENSIBILITY

Things change in technology. Your organization may acquire a competitor that uses a different CMBD or UEM or ITAM. You may also need to add coverage of new technologies as you move from one cloud to another or incorporate more SaaS. Or you may add a new vulnerability management or threat intelligence system that requires integration with technology portfolio status and management for incident response and threat analysis. By abstracting your orchestration layer and transforming it from manual labor into a machine-addressable data layer, security teams can gain the flexibility and extensibility required to adapt, evolve and future-proof security-focused technology orchestration.

BREAKS DOWN SILOS

To maintain a strong security stance at scale, security playbooks and workflows must span functions and break out of silos. While the security team may be responsible for threat intelligence and know that a certain APT is targeting U.S. healthcare companies with ransomware attacks, it is up to the IT team to ensure that systems are properly patched, and up to the HR and internal communications teams to ensure that org-wide communications about the threat are scheduled, distributed, and absorbed. Enterprise Technology Orchestration (ETO) solutions allow security to break down silos and automate or orchestrate tasks normally assigned to multiple functions or departments as part of a unified orchestration process.

Capabilities of a good technology orchestration solution for the enterprise

Now that you have a picture of why technology orchestration is crucial for security, let's consider what you need for such a platform to be maximally effective.

AGENTLESS

Adding another agent to the mix will inject complexity and increase the chances of problems. It is more desirable that an orchestration layer leverages the multiple data acquisition agents already installed in the various IT asset management sub-systems in your enterprise. Integration of agentless systems is simpler and faster. Agentless systems are also more in tune with the growing use of APIs for integration of all internal systems.

INTELLIGENT

Collecting data from all the asset management subsystems is a good start but the best orchestration solutions should also apply intelligence to data to dedupe and reconcile all records. This enhances the accuracy of technology asset data and also creates a trustworthy database of record to serve as a source for all workflows and all analysis of technology portfolio security issues.

EXTENSIBLE AND EASY TO INTEGRATE

This ensures that orchestration can be easily brought into security systems of record and incorporated into the existing workflows of the various security players. Red teams, blue teams, security ops teams, threat analysis and vulnerability

management all have different requirements and some differences in systems. To reach out to those systems, technology orchestration must have an easy-to-address system of connectors or well documented APIs. If integration requires special contractors or a big project, then this is a red flag. The best orchestration systems use common languages such as Python to ensure that anyone can quickly build extensions and connectors.

BI-DIRECTIONAL DATA SYNCING

The true power of orchestration lies in the ability to interact with other systems bi-directionally. Rather than simply broadcasting data to other systems and functions, orchestration can trigger workflows and playbooks based on either internal or external cues. This is a challenging ask; two-way syncing requires delicate data handling. But it is crucial for delivering on the full promise of the solution.

ROBUST BUT SIMPLE AUTOMATION AND WORKFLOW LAYER

A key attribute of orchestration is automation of workflows and playbooks. However, this is only as valuable as it is accessible and easy to use. A visual workflow tool with no code required empowers any stakeholder to automate a process. While security teams are likely code and script fluent, their lives are simpler if the workflow layer is simple. As well, if it is visual, then security teams can more easily collaborate with external teams to create and innovate on workflows.

HOLISTIC AND FLEXIBLE VISUALIZATION

As a security team, having the ability to quickly telescope from the ground level (individual) up to the business unit level or to focus on a geography is crucial to seeing the security picture. This also allows security teams to communicate and share what they are seeing with stakeholders on terms that those stakeholders can better relate to and comprehend. Above all, the broadest possible coverage and integration is crucial for ensuring that every aspect of security is not missing crucial details or assets.

Conclusion: Why accurate, comprehensive and integrated technology orchestration is the new foundation of IT security for the enterprise

We live in an era of DevOps and data. Anything that can be reduced to data and managed like code will be. Security teams that quickly embrace this worldview will reap great benefits. They will have a clearer view of the assets they must protect, and be able to manipulate that view to better analyze their security stance or respond to security threats. They will be able to communicate better with external stakeholders to ensure that the entire organization is pulling together to improve security. And they will be able to better scale their efforts by automating key securiting management tasks and reducing policy determination and enforcement to code and rules. To gain these benefits, a crucial intermediation and abstraction layer must be overlaid atop the existing disparate asset management systems. By making this layer fully integrated, bi-directional, extensible, flexible, and holistic, IT security teams can save money, do more with less, and reduce the risks faced by their organization - while making the lives of their team and external stakeholders better.

About Oomnitza

Oomnitza is an agentless enterprise technology orchestration solution for digital business. By consolidating technology assets data from siloed systems into a single pane of glass, our customers are able to optimize their technology spend, automate their governance processes to meet compliance and auditing requirements, protect from security risks and ensure great employee experience and productivity. Oomnitza is based in San Francisco. For more information, visit us at *www.oomnitza.com*