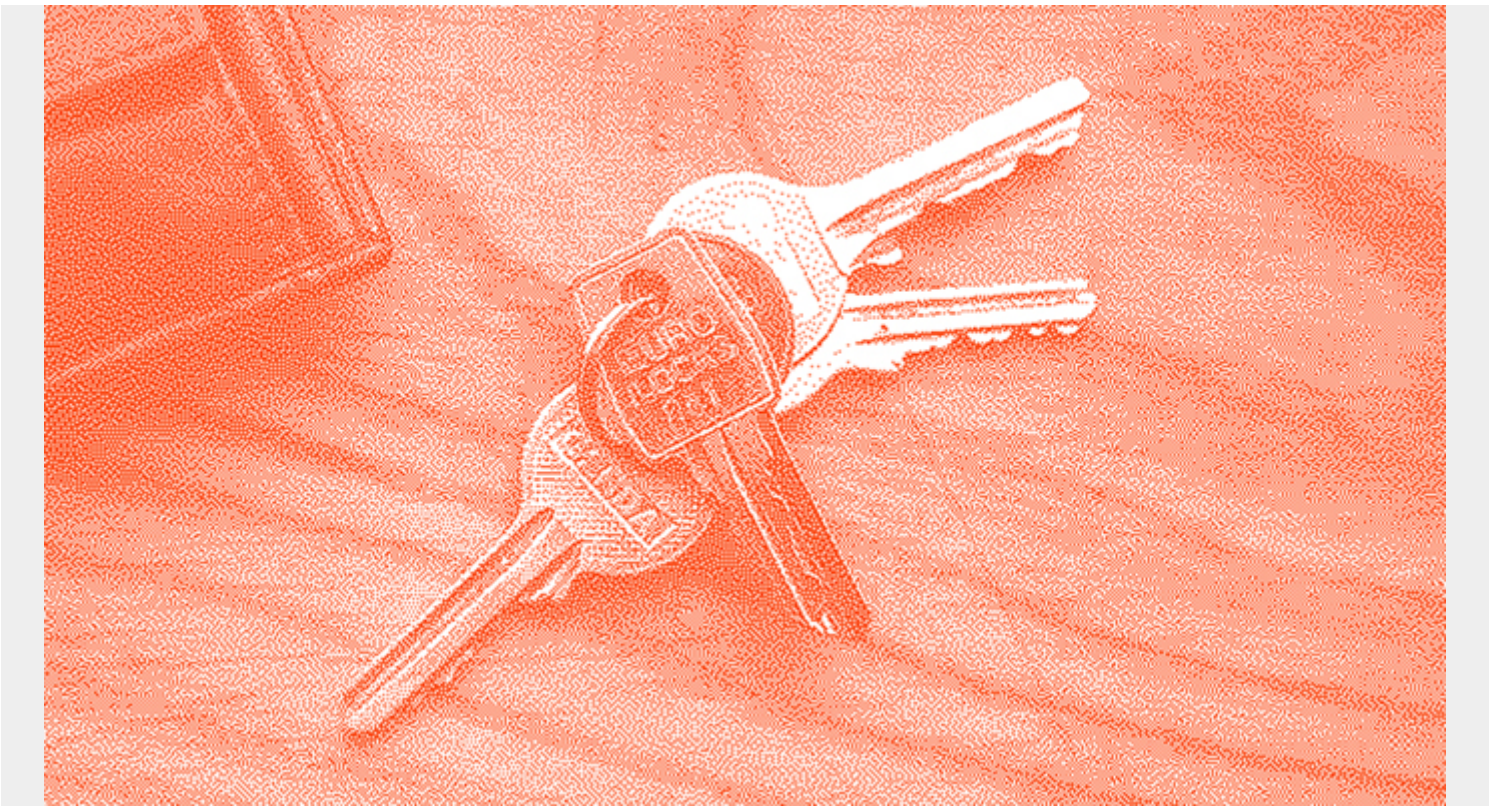
TOO MANY VULNERABILITIES AND TOO LITTLE TIME? WHY AUTOMATION IS AN IMPERATIVE



Too Many Vulnerabilities and Too Little Time? Why Automation is an Imperative

For today's security and operations teams there are too many threats and vulnerabilities, and too little time and resources to address them. As a result, the use of automation for remediating vulnerabilities, deploying patches, and correcting misconfigured IaaS and PaaS resources in hybrid clouds has become a requirement. In addition, software-as-a-service (SaaS) offerings present new choices to organizations that want to shift from a CAPEX to an OPEX model, and outsource IT infrastructure, maintenance, and deployment costs. This post examines why automation has become critical, the benefits of SaaS, and the key requirements that need to be met for security and operations teams to maximize its potential.

Introduction: Escalating Security Threats

For today's enterprises, security imperatives are clear. When organizations are victimized by security breaches and failed compliance audits, they can face steep penalties, including fines, lost revenues, brand damage, customer churn, and more. According to the Ponemon Institute's 2019 Cost of a Data Breach Report, the average cost of a data breach globally now exceeds $3.9 M.

For security teams, the need for security is constant: There's no reward for 364 days of security if a major breach happens on day 365. On the other hand, virtually everything else security and operations teams contend with changes and evolves. Now, these teams are confronting several

trends that make their jobs more difficult:

- **More sophisticated and persistent attacks.** For the security teams wearing white hats, the adversaries in black hats continue to grow more formidable. Cyber criminals continue to up their game, waging attacks that continue to grow more persistent, pervasive, and stealthy.
- **Proliferating vulnerabilities.** At the same time, the vulnerabilities that teams have to contend with continue to proliferate. According to statistics available on the CVE Details site, between 2017 and 2018, the number of security vulnerabilities grew by 13%, reaching an all-time high of 16,555.
- **Expanding attack surfaces.** The increasing complexity of today's IT ecosystems only exacerbates these issues. As they grow to contain more systems and services, these environments present a larger attack surface that needs to be protected. Plus, as an organization's footprint in the cloud grows, teams need to expand their tools and processes to address these additional environments.
- **Misconfigured resources in the public cloud.** According to the shared responsibility model for cloud security, the customer is responsible for the security of the data and content they have in the cloud. Many mistakenly believe that the public cloud provider is responsible for this, and misconfigured resources pose a very significant security exposure. In fact, a Gartner analyst has estimated that, "Through 2025, 99% of cloud security failures will be the customer's fault."

Challenges: Manual Efforts a Significant Barrier to Success

As if the escalation of threats and demands weren't tough enough, the reality is that many security teams are confronting a number of obstacles that make it more difficult to achieve their objectives.

Within most security organizations, there's an acute shortage of skilled staff. Expert security professionals are hard to find, hard to hire, and hard to keep. One ESG survey found that 74 percent of respondents say that their organizations have been affected by the cybersecurity skills shortage.

What's worse is that while staff time is precious, teams continue to be saddled with manual, labor-intensive vulnerability management methods and tools. Often, tasks throughout the entire process, from running vulnerability scans to mapping vulnerabilities to assets and patches, prioritizing remediation efforts, obtaining the required fix, and implementing the changes needed, are all done manually.

For short-staffed operations teams that have long been struggling to meet their objectives, these manual, labor-intensive vulnerability remediation efforts are an obstacle to success. They simply cannot keep up. This leaves teams operating in a largely reactive fashion, which means they constantly have to contend with the inefficiency, stress, and waste associated with fire-drill responses to critical security exposures.

A Ponemon Institute study commissioned by BMC found that 53 percent of respondents agreed or strongly agreed with the following statement: "Our organization's approach to dealing with threats is reactive, focusing on the immediate threat or hack du jour."

Implications: Vulnerabilities Left Unaddressed, Leaving

Organizations Exposed

Given the obstacles and challenges outlined above, security and operations teams are struggling, and too often failing, to keep pace. There are too many vulnerabilities and not enough time to address them all. As a result, organizations continue to be exposed to cyber security threats.

A Forrester report stated that 58% of enterprises suffered a breach at least once in the past year, and over 41% of those external breaches exploited some form of software vulnerability. Further, the earlier-referenced Ponemon survey found that, of those organizations who'd been hit by a breach, 57% of respondents said these breaches could have occurred because a patch for a known vulnerability was not applied.

Further, the manual efforts teams undertake every day can lead to errors, exposing the organization to inefficiency, rollbacks, and downtime. A handbook from the IT Process Institute states that 80 percent of unplanned outages are due to ill-planned changes made by staff. In addition, in the cloud, manual processes will result in organizations being exposed to a breach by issues like misconfigured cloud resources.

Automated Vulnerability Management: Key Requirements

Security and operations organizations have a lot to gain by automating their vulnerability management efforts. However, to date, many have failed to fully capitalize on this opportunity. To maximize the advantages of automation, teams need to employ solutions that address the following key requirements:

Choice of deployment model

Traditional methods of patching and remediating security vulnerabilities have largely been based on systems and software solutions deployed on-premises. Advantages of this approach include control, because the configuration, upgrading, and system changes are done on-location, and access since you do not have to rely on internet connectivity to reach your software.

Alternatively, SaaS offers a new choice for remediating vulnerabilities. Advantages of software-as-a-service include shifting from a CAPEX to an OPEX model, reduced infrastructure, deployment and maintenance costs, automatic installation of updates, greater flexibility and scalability, and choice of cloud.

Comprehensive automation capabilities

Teams also need solutions that use automation to find and fix security vulnerabilities in hybrid cloud environments. They need to discover missing patches and misconfigured resources and then take automated, corrective action. This should include identifying the assets and business services exposed, the severity and duration of the vulnerability, deployment of patches based on policies, and more.

In addition, it is also important to leverage solutions that can automatically identify misconfigured cloud services, including IaaS and PaaS resources, and remediate them. Solutions should automate compliance with security policies and regulatory mandates, such as the General Data Protection Regulation (GDPR) and Center for Internet Security (CIS).

Flexible integrations

To maximize value, solutions should offer flexible integration with other tools and capabilities. For example, they should support integration with incident and change management to increase speed and efficiency, and keep operations available and running smoothly. Solutions should also offer integration with robust discovery offerings – you can only secure it if you know you have it. By enabling integrated discovery and automated remediation, solutions can effectively eliminate blind spots that can lead to vulnerabilities being left unaddressed.

Unified support for hybrid environments

Security and operations teams need a unified approach to managing automation of security and compliance across their organization's entire hybrid cloud footprint, including on-premises servers, networks, and public cloud environments. Solutions should offer support for a range of environments and technologies, including AWS, Azure, Google Cloud Platform, Docker, and Kubernetes. In addition, to ensure effective alignment with today's hybrid realities, teams need solutions that offer cloud-based implementation, while enabling automated management of on-premises data centers and multi-clouds. Look for solutions that offer container-based deployment, which fosters easy installation, configuration, and upgrading.

Intelligence and analytics

To manage automation optimally, it's vital that teams have automation solutions that are backed by advanced analytics and intelligence. Analytics and intelligence are needed to map vulnerabilities to the resources exposed, the required corrective action (patch or configuration change), help set priorities, and track vulnerabilities within the context of SLAs. When analyzing vulnerabilities, teams should also be able to gain instantaneous visibility into which applications and services are at risk. Analytics also need to leverage discovery data to identify and support remediation of vulnerabilities missed by security scanners.

Benefits: Strengthening Security and Boosting Productivity

By leveraging advanced solutions that address the requirements above, teams can maximize the potential of automated vulnerability management using the deployment model of their choice – either via SaaS or on-premises. With these capabilities, teams can fortify their infrastructures more consistently and efficiently, and significantly boost security and compliance.

Further, this automation can be invaluable for stretched, under-staffed security teams. By offloading manual, repetitive tasks from security staff, teams can spend less time focused on maintenance, and more time focused on innovation. Further, through automation, teams can see improved productivity, efficiency, morale, and employee retention.

Conclusion

To maintain an effective security and compliance posture and keep pace with escalating security threats, automated vulnerability remediation has emerged as an urgent imperative. By leveraging solutions that address the key requirements outlined above, security teams can strengthen security, while boosting staff productivity.

To learn more about how BMC is helping customers fully capitalize on the potential of automated vulnerability remediation.