IDC TECHNOLOGY SPOTLIGHT

Leveraging the Cloud to Achieve Comprehensive Asset Visibility, Tracking, and Security

March 2017

Adapted from *Worldwide Cloud Hosted Enterprise Security Services (Security as a Service) Forecast, 2015–2019* by Christian A. Christiansen, Elizabeth Corr, et al., IDC #257959

Sponsored by Tenable

As more organizations embrace public cloud, mobile, and DevOps, the fundamental concept of an asset changes and significantly impacts how security teams interact with their colleagues and do their jobs. The traditional approach of scanning a network is no longer effective because the flux of assets prohibits security teams from gaining an accurate snapshot of their environment. By leveraging the cloud and new technologies that deliver greater visibility, organizations can gain an accurate picture of their assets and overall risk posture. This is a critical step toward addressing the current landscape where attackers are using a wide variety of vectors such as mobile, social, and cloud-based attacks to infiltrate organizations and steal data. This Technology Spotlight examines the evolution of vulnerability management and the need for organizations to achieve greater visibility into all of their assets and vulnerabilities, including new asset types such as containers. This paper also details the advantages provided by cloud-based vulnerability management as exemplified by Tenable.io, an approach that enables end users to leverage the elastic and scalable nature of the cloud to monitor changing corporate assets.

Introduction

Despite our best efforts as an industry, attackers are winning the battle. The latest Verizon *Data Breach Investigations Report* provided several sobering statistics:

- 89% of incidents have either a financial incentive or espionage as the motive.
- 30% of all phishing emails were clicked across all campaigns.
- 97% of breaches featuring stolen credentials leveraged legitimate partner access.

These statistics reflect the challenges facing chief information security officers (CISOs) on a daily basis. In a 2016 survey, IDC asked CISOs what things "kept them up at night." While the role of CISO is broad and varied, most responses tended to cluster around the following:

- Reputation damage through negative publicity and loss of trust, all tinted with the possible perception of incompetence or negligence
- Loss of the productivity that keeps an organization running on a day-to-day basis
- Loss of a competitive edge that might be driven by key intellectual property
- Regulatory violations associated with any of the aforementioned

On the surface, the answer seems trivial — add more security. However, as we continue to see, adding layer upon layer of security to existing systems is not the answer. CISOs struggle to address the challenges posed by increasingly sophisticated attackers while securing a changing business environment in which employees are working from anywhere, on any number of devices, across a variety of applications that may or may not be owned by their organizations.

To manage the ever-growing number of devices, applications, and data flowing through organizations every day, businesses must turn to platforms that provide actionable information around the threats facing them and the vulnerabilities present in their networks. Vulnerability management as a practice has been established for many years, but modern tools must address changes in devices, applications, and platforms. Today's approaches should provide a broad, holistic view of the risks facing organizations over time and provide the context needed to determine which risks need to be addressed first.

IDC research shows that the cloud-hosted security services market is growing rapidly.
With vulnerability management being the fastest-growing subsegment, it is important that organizations work with vendors that are actively addressing the challenges in this market. Specific drivers are generating this growth, and solutions must address these needs to succeed.

Benefits of Cloud-Based Security and Vulnerability Management

A properly designed cloud-hosted vulnerability management platform will provide comprehensive visibility into traditional and dynamic assets such as cloud, mobile, and containers (both during the build process and in production) as well as web applications. The key benefits provided by certain cloud-based platforms are:

- **Broad asset coverage delivers comprehensive visibility.** Unless an organization knows exactly what devices and resources are on the network, effective security is impossible. In many cases, organizations with generally strong security practices have fallen prey to having an unknown, unprotected asset become compromised and contribute to a data breach. Today, this is increasingly likely due to the proliferation of new and short-lived assets, such as cloud instances and containers. However, certain cloud-based platforms can now track the full range of assets and vulnerabilities, no matter where they reside.
- **Integrated user experience improves productivity.** Security professionals are often frustrated by the need to switch between multiple tools in order to get their jobs done. Besides causing inefficiency, tools that don't communicate or interoperate can lead to security risks being missed. An integrated cloud-based platform can provide a consistent user interface, enabling users to quickly address problems across multiple domains.
- **Simplified integrations improve visibility and efficiency.** Security and vulnerability management (SVM) is a broad category that encompasses many different functions. To manage an effective security program, organizations need their security, infrastructure, networking, and other systems to seamlessly share data. Using a cloud-based solution with prebuilt integrations and the ability to quickly build new integrations via a well-documented API allows security professionals to both improve overall visibility and increase their efficiency.
- **Capex can be reduced by leveraging cloud resources.** Using a subscription-based cloud solution allows organizations to lower their capex by leveraging a shared cloud infrastructure for storage and processing. This is particularly important for smaller organizations that simply may not have the resources to build and manage the datacenter capabilities necessary to perform all the functions related to SVM.

- **Elasticity helps organizations.** The ability to flex capacity higher or lower in real time gives businesses the coverage they need with the opportunity to scale easily as required. Organizations are always concerned about investing wisely while remaining responsive to the needs of the business. The elasticity of a cloud-based platform, particularly one with the ability to flex licensing capacity, allows organizations to achieve this agility. CISOs can have the confidence to move forward knowing they can easily add or reduce coverage based on changing requirements.

Moving Toward Cloud-Based Security

For many years, security professionals treated the cloud as a high-risk platform. Concerns about the control and the handling of information prompted organizations to move only small amounts of data and processing to the cloud. Over time, it has become clear that the cloud offers significant price and performance advantages and that cloud-specific data security concerns were often overstated. As a result, many are shifting their resources toward cloud-based security products, leading to a compound annual growth rate of 17.2% for the cloud-hosted SVM market from 2014 to 2019, according to IDC research. Key reasons for the shift include:

- **Smaller organizations desire the same level of security as large organizations but have fewer resources.** There is no doubt that a cybersecurity workforce shortage exists. Estimates put the shortage of professionals at 1 million in the United States alone and 6 million worldwide by 2020. This shortage has had a significant impact across the industry, but in particular, it has affected small and midsize organizations that have security requirements similar to those of large companies but simply cannot afford the workforce needed to maintain all security products on-premises.
- **There is a need for protection to extend across all form factors.** This includes physical, virtual, private and public cloud, and even containers. Access to enterprise resources used to be tightly controlled and more easily visible. Today, compute, application, and data resources reside on-premises or in the cloud, or sometimes both. These resources are accessed from workstations, laptops, smartphones, tablets, and other devices. Cybersecurity professionals have been tasked with protecting corporate resources and maintaining compliance with a host of standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) standards, and the ISO 27000 family of standards.

Considering Tenable.io

Tenable.io is designed to deliver visibility and insight through an open and elastic platform. It is also designed to provide maximum coverage for evolving assets, supporting cloud, containers, and web applications as easily as traditional assets. The product uses a multi-attribute asset identification algorithm to track the identities of resources within an organization's environment, regardless of where they roam and how long they last.

The solution has been designed to deliver value quickly through a streamlined and intuitive user interface. Predefined templates and configuration audit checks follow industry best practices such as CIS, DISA STIG, and others. The Tenable research team provides frequent updates to ensure that the latest vulnerability checks and configuration benchmarks are immediately available to customers.

Tenable.io also includes prebuilt integrations with complementary systems such as password vault, patch management, network access control, and mobile device management (MDM) solutions to help organizations streamline their vulnerability management practices and improve asset and vulnerability insight. Users can access a well-documented API and software development kit (SDK) to support data import and export and integrate vulnerability management into other business processes.

Tenable has also changed its licensing model with Tenable.io to better reflect the modern computing environment. Tenable.io is licensed by assets instead of IP addresses — the first vulnerability management solution to do so. This elastic asset licensing helps identify, track, and license all of the assets in an organization's environment, without double counting. It handles the tracking and licensing of mobile devices, public cloud instances, and short-lived VMs. Supporting the elastic nature of many environments, Tenable.io automatically reclaims licenses from assets not seen for 90 days, without deleting the historical data.

Challenges

While adoption of cloud-based solutions continues, many organizations have already made significant investments in their on-premises solutions. Although these are lessening over time, some questions remain in the security community about the security of data managed in cloud-based solutions. As these concerns fade, this inhibitor to adoption of cloud-based solutions such as Tenable.io will likewise dissipate.

Another challenge for Tenable is the inclusion of container protection as part of the platform. Today, containers are just starting to gain acceptance in development and operations. While this acceptance is predicted to grow and security will become a necessary component of container-based development, many organizations do not yet have a need for container security.

Conclusion

SVM is a broad market that has traditionally seen numerous competitors introduce products designed to address a specific function. Today, organizations must manage vulnerabilities in assets ranging from the smallest and shortest-lived containers to the largest and most complex web applications — with laptops, servers, virtual machines, cloud instances, and more thrown in for good measure. This broad attack surface makes vulnerability management more complex than ever.

Organizations are looking for a platform, not a point solution. They want to be able to view the risks associated with any asset, no matter what form that asset takes. They need the ability to prioritize responses based on the most significant exposures, and they need to manage security across the life cycle from development to deployment.

Tenable, with its new cloud-based Tenable.io solution, provides a comprehensive, asset-centric solution to accurately track resources while accommodating dynamic assets such as cloud and containers. By providing effective asset and vulnerability tracking across all form factors, designed for a streamlined user experience and elastic licensing, Tenable.io is addressing the most critical needs with a single platform. To the extent that Tenable can address the challenges described in this paper, IDC believes that the company's solution is well positioned for success.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com