Realizing the Benefits of Vulnerability Management in the Cloud

April 2011
Gordon MacKay
CTO, Digital Defense, Inc.

Digital Defense Whitepaper
9000 Tesoro Drive, Suite 100 | San Antonio, Texas 78217 | www.ddifrontline.com

Introduction

I would like to start out this whitepaper with a short story.

One day earlier this year, I was taking my dog for our daily walk. In passing a bend, this lively Pomeranian took notice of a few birds nearby. She became alert and excited! In the next moments, we experienced the beauty of a large flock of birds, as they took flight from the ground and nearby trees in their escape. They were brisk and noisy as they made their way up into the sky. It was an impressive sight for our small neighborhood. For the remainder of our walk, I pondered this.

The few birds' reaction to the threat caused the entire flock to become aware of the danger. This "safety in numbers"[1] behavior prompted the following thought: *Often in nature, an organism is more secure in a community than alone*. I thought about the DDI vulnerability management solution and I realized that this same "safety in numbers" concept is also applicable to vulnerability management.

In this paper, I discuss two types of vulnerability management deliveries, cloud-based and premised-based. I highlight several challenges with vulnerability management and I argue that a cloud-based vulnerability management delivery keeps organizations more secure as compared to a premise-based solution.

Vulnerability Management Delivery Options

Before describing some of the challenges with vulnerability management, it is worthwhile to provide a brief description of what vulnerability management includes and then describe the differences between the two types of deployments, Software as a Service or SaaS-based (also known as cloud-based), and the second type, premise-based. Realizing that SaaS forms part of the cloud computing stack, many solution providers refer to SaaS-based approaches as "In the cloud", cloud application services or cloud-based[2]. For the remainder of this paper, I will refer to this deployment as cloud-based.

Vulnerability management involves a lifecycle process that includes discovering assets and vulnerabilities, prioritizing assets, prioritizing the remediation activities for vulnerabilities associated with the assets, performing the remediation activities, and finally, measuring the process[3]. Security vulnerabilities are a fact of life. The problem will never go away. The goal of this lifecycle process is to assess and manage the risk associated with security vulnerabilities. Part of managing the risk is remediation and understanding what to remediate based on pre-determined priorities.

Several solution providers have introduced products and services that automate parts of the vulnerability management process. In a premise-based deployment, the solution includes hardware and/or software vulnerability scanners and associated components, which are entirely installed on the client premises. Client users typically

login to a web portal accessible via the vulnerability management system within the organization's network. The scanners are located within the client premises and will typically assess vulnerabilities from outside or inside the organization's external firewall for the purpose of performing external and internal vulnerability assessments. All vulnerability findings are stored within the vulnerability management solution on the client premises. Figure 1 illustrates a premise-based vulnerability management approach.

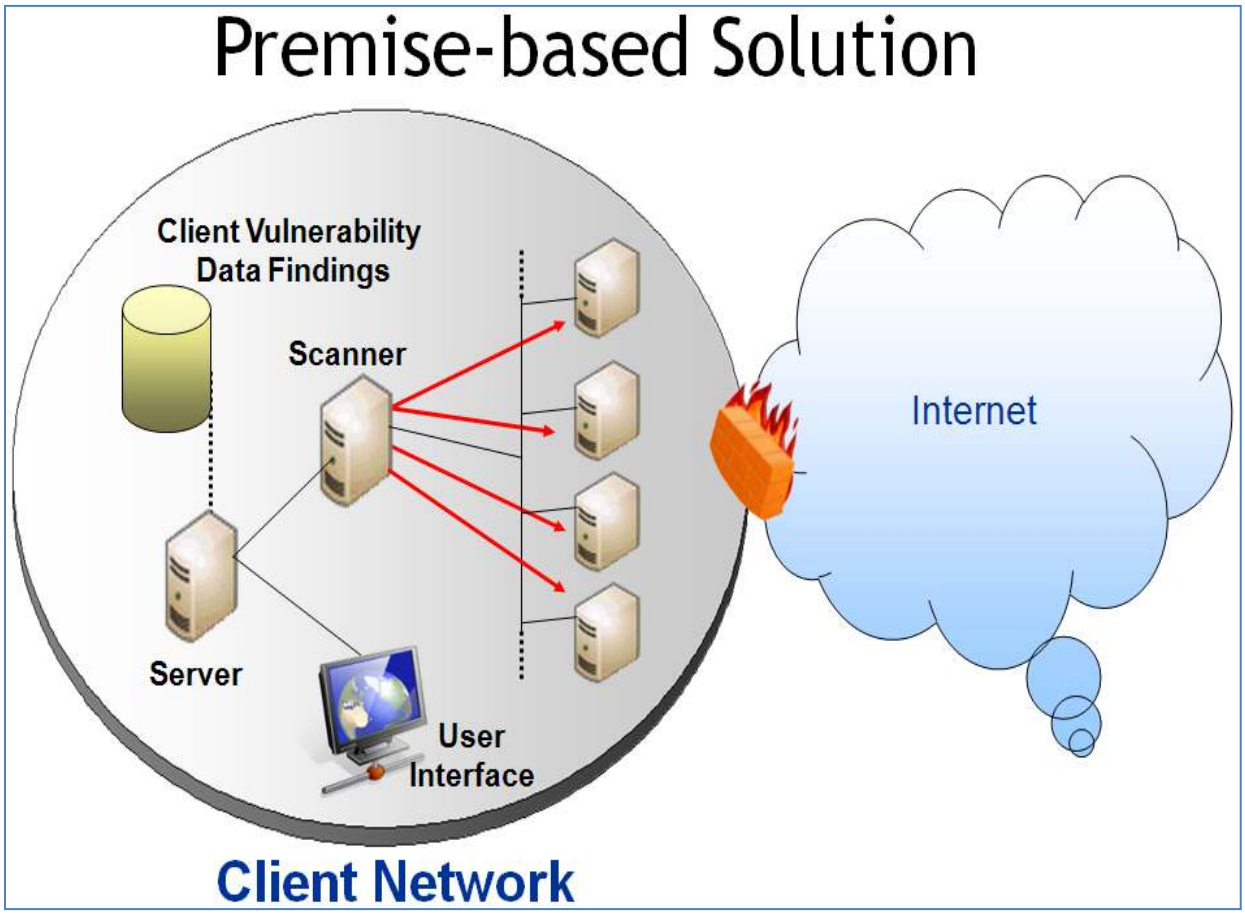

Figure 1 Premise-based Vulnerability Management Offering

In a cloud-based deployment, vendors house a vulnerability management platform "in the cloud", typically in their own data center. Organizations login to a common web portal over the Internet. They are able to view and manage their vulnerability assessment data within the portal. Vulnerability scanners for external vulnerability assessments are located at the solution provider's site. The solution typically includes one or more scanners that are deployed on the organization's premises for the purpose of performing internal vulnerability assessments. Vulnerability information for the assessments is stored at the solution provider's site (not at the client site) for both internal and external vulnerability assessments.

Figure 2 illustrates a cloud-based vulnerability management approach.

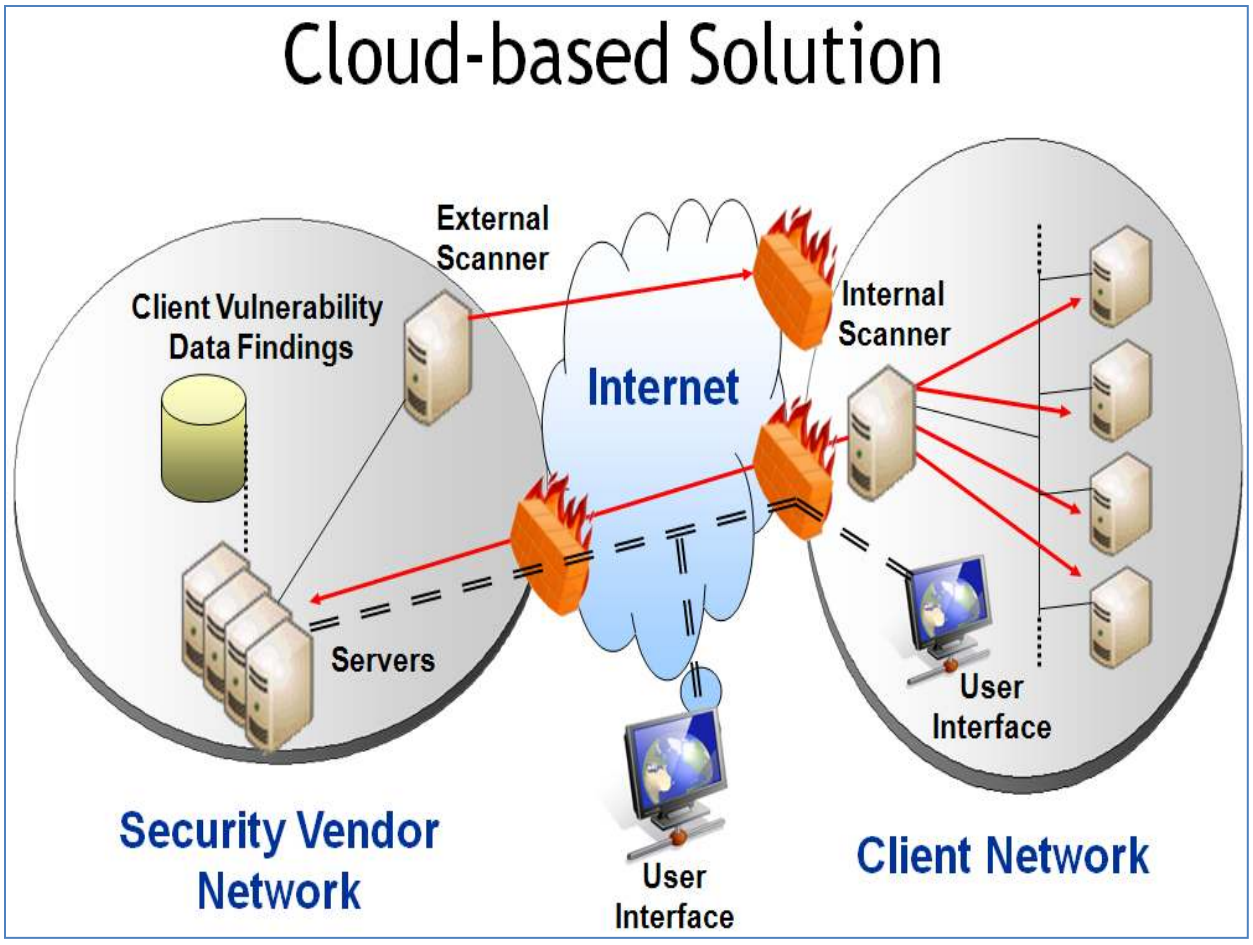

Figure 2 Cloud-based Vulnerability Management Offering

There are many references available, which compare the pros and cons of cloud-based versus premise-based deployments for all types of products and services. In general, these include:

- Cloud-based deployments involve lower installation costs since there is no installation and configuration for the client to complete.
- Cloud-based deployments involve lower maintenance costs as there is only one centralized component to maintain and it is maintained by the vendor (not the end client).

- Hardware/Software upgrades to the solution are included in a subscription to a cloud-based deployment whereas upgrades typically require additional service agreements for premised-based deployments.
- Cloud-based deployment costs are distributed among all organizations and therefore are typically lower as compared to premise-based.
- Cloud-based deployments do not require the client to provide onsite equipment such as scanners, storage management, or software resources, as the vendor provides all these.
- One argument for premised-based deployments is that the data findings are stored at the organization's site, whereas in a cloud-based deployment, the data is resident with the solution provider. As a result, cloud-based solution providers must assure the security of the vulnerability data, whereas with a premise-based solution the responsibility falls to the end client.

Many organizations have traditionally resisted cloud-based deployments due to the perceived risk mentioned in the last bullet. However, this is changing as organizations are becoming more educated on the security solutions cloud-based vendors utilize. In fact, a recent Forrester study indicates that cloud-based security will shift from being an inhibitor to an enabler of cloud service adoption and that the cloud security market will grow to 1.5B by 2015[4].

Vulnerability Management Challenges and Solutions

There are numerous challenges faced by organizations utilizing automated vulnerability management solutions, regardless of their implementation method. In this section, I expand on three of the most common and expose how they can directly influence effectiveness of a vulnerability management solution. Finally, I elaborate on how cloud-based offerings negate each of them, and as a result, help keep organizations more secure.

1- New Vulnerability Identification Lag

Organizations typically schedule their vulnerability assessments to recur over time as part of their ongoing vulnerability management program. Often they will scan devices in their network at a frequency that aligns with their network size, IT budget, risk level, and variety of other factors. Unfortunately, many organizations do not conduct vulnerability scans as frequently as these factors would indicate they should, in most cases because of the time and expense involved.

As a result of the ad hoc nature of their vulnerability scanning programs, these same organizations may not have assessed their devices for an extended period of time and may not be aware that they are affected by a new critical vulnerability that has recently been discovered and for which their solution provider released a new detection.

A cloud-based vulnerability management offering provides a solution.

Within a cloud-based offering where multiple organizations are part of the ecosystem, at any given point in time a set of organizations would have already launched recent vulnerability assessments that provide information on whether or not the new vulnerability in question is present under various conditions. A cloud-based solution has the capability of aggregating this information and feeding it back as information to an entire client base. To follow the "security in numbers" analogy given in the introduction of this paper, this ability would provide awareness to all "birds" in the group even though only a few "birds" have seen the danger.

A premised-based offering cannot offer a comparable solution to this problem, as the vulnerability data is not visible to the vulnerability management solution provider and therefore no data aggregation and feedback to other organizations is possible.

2- Vulnerability Detection Accuracy - False Positive/False Negative Identification

All vulnerability management solution providers are subject to vulnerability detections that result in false positives as well as false negatives. It is common knowledge, though very few solution providers in the industry like to discuss the matter.

As an example of how these types of issues are realized, I'd like to elaborate on both scenarios.

- If a newly developed vulnerability detection is introduced into an organization's ecosystem by a solution provider and has 0 (zero) positive detections across many scans within its first week, there is a high likelihood that the detection is experiencing false negative conditions.
- On the other end of the spectrum, if a new vulnerability detection indicates positive at close to100% of the time, there is a strong possibility of a false positive condition.

To address these issues, some solution providers err on the conservative side and identify many vulnerabilities, most of which they are not truly able to detect with certainty, as possible or potential vulnerabilities. These solution providers would claim that they have a low false negative detection rate since they include all of the potential vulnerability identifications as true identifications. Yet, these same vendors also claim a low false positive rate because they only include those detections that they categorize as "certain" detections (not potentials).

Arguably, cloud-based vulnerability management solution providers are more accurate in detecting these vulnerabilities as compared to premised-based solution providers. Before moving on, I want to be clear, I am only considering the

vulnerabilities that network vulnerability scanners are able to identify with certainty when I make that statement.

But on what basis can I make that statement? Simply put, cloud-based solution providers can "see" what premise based solutions are "blind" to when conducting vulnerability scans.

A cloud-based vulnerability management solution provider has visibility to the aggregate vulnerability detection results across its entire client base. They have visibility to the number of times each detection shows as positive or as negative. They can use this aggregate information as indicators of possible false positive/false negative occurrences. Additionally, strong conclusions on false positive and false negative instances may be drawn regardless of percentage of indicators to detection launches when one considers other variables such as applications, ports, the presence of other vulnerabilities, and more.

Premise-based solution providers would argue they determine these same issues in their test farm labs. However, I would argue that there is no test farm lab as large as a cloud-based solution provider's client base. Premise-based solution providers do not see their client detection information and cannot glean information from what is going on in the field in this regard. On the contrary, cloud-based solution providers do have this visibility and therefore have an advantage in this regard. As a result, they have the capability to identify issues, react, and rapidly correct normally occurring software bugs. Given this, it stands to reason that cloud-based offerings are more accurate with detections as compared to premise-based offerings for detectable vulnerabilities as I defined earlier.

Once again, I am not including possible or potential vulnerabilities in this paper. But even with possible and potential vulnerabilities included, one could make a strong case that cloud-based offerings will make more accurate "guesses" on potential vulnerabilities as compared to premise-based offerings. Again, the reason is that cloud-based solution providers can mine a much larger and diverse data set than any premise-based solution could ever hope to have for their use.

3- Remediation Challenges

I think that anyone reading this document will agree that the success of any vulnerability management program is largely dependent upon the success of the ability of an organization to remediate discovered issues. Although vulnerability management solution providers include detailed remediation steps for vulnerabilities, and their solution often integrates with automated remediation solutions, vulnerability remediation remains challenging. This is because, as many an IT manager will tell you, vulnerability remediation is never fully automated.

But with all of the automation and API access between platforms available today, why not?

In some cases, the challenge exists because patches for software flaws are not always available, in which case remediation involves some level of mitigation. For this reason, the detailed remediation steps found within vulnerability management providers' databases is never truly complete. As a result, the end client requires a certain level of remediation expertise and must always perform remediation research in conducting their remediation activities. The greatest challenge to vulnerability remediation is knowledge, or the lack thereof. Organizations frequently do not have the remediation expertise in-house and even those that do often lack the time and money to research and effectively remediate issues to elevate them above their risk tolerance level.

As with the two prior challenges, cloud-based vulnerability management providers offer help in this area.

Most vulnerability management systems allow organizations to document the remediation steps taken to remediate the vulnerabilities. This is especially useful in the case where no specific solution exists for a given vulnerability and where mitigation is required. Many enterprises track their remediation activities, including custom mitigation steps, in a database, often within the vulnerability management system. This allows a system user to refer back to their solutions in the case where a similar vulnerability is found in a different part of the network.

For example, in a given fictitious company *Gordo Technologies*, suppose Tom from the Development department needs to remediate a vulnerability for which a patch does not exist. Tom then solves the problem with a creative mitigation solution and documents the steps in the vulnerability management system. Then suppose Bob, who also works for *Gordo Technologies* but in the Corporate IT department, has a similar vulnerability that he must also remediate. Bob has the ability to consult the remediation database and learn what Tom did to mitigate the issue. This saves Bob a lot of research time, and in the process, makes the entire company's vulnerability remediation program more efficient and effective.

While this ability to share information can exist within cloud-based and premised-based vulnerability management solutions, cloud-based solutions take the ability to the next level by allowing sharing not only within the same organization, but within the client ecosystem as well (as long as there are no sensitive data sets involved). In fact, if *Gordo Technologies* were part of a cloud-based vulnerability management system, Tom would have the ability to consult the remediation database for the entire vulnerability management cloud and he could quickly find the needed mitigation information and saved himself a great deal of research time! Once again, members who participate in the cloud learn from the knowledge of others in the same cloud.

Conclusion

It is an undeniable and unavoidable truth that almost all organizations bear some level of network security risk. This risk is the unfortunate consequence of businesses operating in an ever more connected world and it will only continue to grow as more and more business operations are automated by IP-connected systems.

Given this, it is a fair assumption that those organizations that chose to adopt an ongoing vulnerability management program within their enterprise will prove to be much more resilient and much less likely to realize these risks than those organizations that opt for an easier path. With that being said, all organizations, regardless of the path they choose, would naturally select a vulnerability management solution that allows them to minimize their risk and remain within their budget. As outlined and discussed in earlier sections of this document, a cloud-based offering provides organizations with that option.

But why do I maintain that a cloud-based solution is a better option than one that is premised-based?

In summary...

- A cloud-based vulnerability management solution can effectively tell you how prevalent vulnerabilities are across an entire ecosystem of organizations. Organizations in essence get a "heads up" on risks identified by recently implemented detections even before their scans run.
- A cloud-based vulnerability management solution should theoretically be more accurate at vulnerability detection as compared to a premised-based solution given the vast number of IP-enabled systems it assesses vs. a premise-based solution that can only utilize a sampling of systems in a developer's lab.
- With cloud-based vulnerability management, user tenant knowledge can be shared with users across the entire cloud. More security knowledge more quickly leads to a lower network security risk level with a smaller time and cost investment.

Given these factors, cloud-based vulnerability management wins out over premise-based solutions in keeping organizations more secure.

In closing, I leave you with one additional thought: My Pomeranian did not catch any birds that day during our inspirational walk. Like the birds of the flock, do you want to go it alone and possibly get caught, or do you want to be part of a greater secure group who subscribes to a Cloud-based vulnerability management solution?

References

1. Safety in Numbers - http://en.wikipedia.org/wiki/Safety_in_numbers#Description
2. SaaS as In the Cloud - http://en.wikipedia.org/wiki/Cloud_computing
3. NIST Vulnerability Management - http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
4. Cloud-based security a cloud service enabler - http://www.darkreading.com/security-services/167801101/security/application-security/227900512/index.html