Vulnerability and Access Risk Management

The first look into understanding how Vulnerability and Access Risk Management are better together

By Felicia Thomas

March 2016
# Table of Contents

 Introduction ................................................................................................................................................. 3  
 What is Vulnerability and Access Risk Management? ................................................................. 4  
 How does Vulnerability and Access Risk Management really work? ........................................ 5  
 Governance and Remediation Systems: The Holistic Approach ........................................ 6  
 Can This Be Done on Your Own? ........................................................................................................ 7  
 Tools: The Ability to Remediate from Visibility ........................................................................ 8  
 Prioritize How You Solve Risk ....................................................................................................... 9  
 The VARM Checklist .................................................................................................................. 10  
 References ............................................................................................................................................ 11
Introduction

Threat intelligence is a company’s worst nightmare which pushes cyber security and risk management to the top of the list for standard operating procedures (SOP). Traditional risk management is a thing of the past, and corporations have begun investing in top-notch security solutions for their various databases. Although no solution will ever be 100% capable of preventing attacks, there are solutions that can help provide roadblocks to deter these occurrences. With proper detection solutions, a company becomes proactive—rather than reactive—to fight against vulnerabilities that exist in their systems.

Large organizations are riddled with increasing threats to their system infrastructures and customer data. The vast majority have moved into protecting these assets with Identity and Access Risk Management (IAM). An emphasis on compliant provisioning of users, identifying management of roles, the maintenance of compliant roles, and processes to manage segregation of duties (SoD) are the focuses of this type of management tool. However, in some cases, the traditional IAM solution is not enough protection against threats.

Many large corporations want an automated, rules-driven solution that can provide quick remediation around network access controls. However, before an attack occurs and remediation can begin, there is the challenge of anomalous activity detection from the infrastructure level. To help with this detection, many companies have instituted consistent monitoring by scanning the system for potential threats to safeguard their infrastructures.

Dynamic provisioning capabilities through IAM, and the proper protection to deter attacks from the infrastructure level with vulnerability management, can position a corporation to achieve the best level of protection possible. This introduces the concept of the acronym VARM – Vulnerability and Access Risk Management. It’s not just the first line of defense; it’s a complete, end-to-end solution that will break the “kill chain” from system threats within the enterprise.
**What is Vulnerability and Access Risk Management?**

With an abundance of human error and inadequate monitoring, automation is the best way to begin defending a system’s infrastructure. At the same time, if there are precautions in place to detect when an account is compromised, a security team can build a risk assessment for the company that will be a key part of their security analytics. By introducing Vulnerability and Access Risk Management (VARM), the internal process for a corporation can be streamlined from infrastructure through account provisioning and compliance to continuously and comprehensively monitor both systems.

VARM can provide an efficient structure in many multifaceted IT environments. Because attacks tend to have lateral movement, a vulnerability solution can illustrate a probable attack path using threat intelligence from the front end of an infrastructure. By using continuous monitoring, remediation of potential threats and an IAM program, if an attacker breaches the infrastructure, there is another line of defense on the account level to defend against the attack path.

With these two forms of deterrent solutions, a company will have proper visibility to take necessary actions for accurate remediation.
How does Vulnerability and Access Risk Management really work?

When a company wants to prevent breaches that come through vulnerabilities, it can detect them with a vulnerability scanner. These scanners will show all vulnerabilities in the infrastructure, from tens to thousands, based on the size of the network. In addition, many vulnerability management solutions offer antivirus software capable of fact-finding analysis to discover undocumented malware. If it finds software behaving suspiciously—such as attempting to overwrite a system file—it will provide an alert.

Fast-acting correction to these vulnerabilities, such as adding security solutions, or educating users about social engineering, will be the difference between exposing a system to potential threats and protecting the system from those threats.

Access risk management (ARM) is the part of an IAM solution that identifies, assesses, and prioritizes risks from an access provisioning and compliance perspective. Because there are various sources from where risk comes from, utilizing access risk management helps to continuously monitor a system while providing preventative measures to manage user access and account entitlements.

Having VARM as a threat solution helps when identifying the sources of potential risk. Risk sources are more often identified and located not only in technological assets but within infrastructure and other tangible elements. It is extremely difficult for IT security personnel to be able to apply an objective and systematic observation of the state of their network without a solution in place. Utilizing VARM helps to identify not only that something is wrong, but it can support the clear understanding of how, when and where to act on a potential threat.
Governance and Remediation Systems: The Holistic Approach

Remediation is more than simple deletion; it is an information governance method concentrated on bringing order to information. It is focused on the overall management of information including cleaning, organizing, and transferring information. The overarching goals of a full remediation project are to retain information valuable or necessary to meet an organization’s business, legal, and/or regulatory objectives and obligations to make sure that it is organized and accessible. It is also in place to ensure that information no longer useful to the organization is deleted in a defensible manner.*

Having a holistic governance and remediation system allows a corporation to implement strategies to manage uncertainties from infrastructure to dynamic provisioning. Typical corporations will benefit from having a holistic approach because it provides new and innovative ideas to old and new problems. VARM can foster settings that encourage innovation within an organization as well.

Having a vulnerability and access risk management solution benefits an IT network is because it helps to detect, deter, and remediate potential threats and system attacks. This is another example of gaining a holistic view of your system.

Imagine being able to deter a threat just from penetration testing (pen-testing), or detect an attack as soon as it passes through the infrastructure. With continuous monitoring, you have the ability to detect and/or remediate attacks to your database. This regular monitoring with a stable governance and remediation solution can allow a corporation to maintain compliance and conduct forecasts by analyzing the environment against the current security position. By using a Vulnerability and Access Risk Management solution, you can remain vigilant by continuously and comprehensively monitoring the entire environment.

Can This Be Done on Your Own?

It is much more difficult to manually monitor a company’s complete IT system for potential threats than many would think, especially on a continuous basis. Companies utilize pen-testing through malware as a small way to monitor vulnerability while some try manual pen-testing.

“Manual penetration testing adds the benefit of specialized human expertise to our automated binary static and dynamic analysis—and it uses the same methodology cyber-criminals use to exploit application weaknesses such as business logic vulnerabilities.” *

The harsh reality about manual pen-testing is that when it is NOT properly executed, testers can crash servers, corrupt or expose data, or cause other opposing effects associated with mimicking hackers. The goal of pen-testing has many pros and cons, but to avoid potential problems, it is best to have a system automated by a responsive software tool. A manual solution can produce inaccurate results which can leave many companies with a false sense of security within their databases.

Utilizing a VARM solution will not only provide continuous and comprehensive monitoring, but the amount of human error is nonexistent when providing both areas of security.

Aside from pen-testing, the other aspects of a Vulnerability and Access Risk Management solution are constantly dealing with hundreds of thousands of data points on an average server. For example, let’s assume your company has just 50 employees. Each of these employees has access to between 15-20 applications on your network. They also have access outside of your network to social media, personal email, and more. You also have contractors who need access to applications on a time-sensitive basis. When multiplying these factors, you can see how your access risk grows exponentially with every new hire or new application. Keeping up with the access risk factors across an organization is simply too much for one person or—more often—one team. If you have any more than 5-10 employees or more than 10 applications, an automated solution is the easiest and most accurate way to continuously and comprehensively monitor your vulnerability and access risk.

*2016 VERACODE
Tools: The Ability to Remediate from Visibility

The method of organizing access for many corporations can be ineffective and have discrepancies due to complexity within the security strategies. In the last chapter, we explained how access data grows exponentially with each new hire. Without tangible, adaptable visibility, security executives are challenged to be able to manage the abundance of user behavior and network behavior. From user rights, policies, and proper system compliance, a corporation will have not only a problem with visibility of potential threats but also the best form of action to take to prevent them.

In order for complete security protection, a company has to provide the proper tools to manage governance and make sure there is a process for executing controls. With VARM, both the infrastructure and the controls around access can be addressed.

With an access risk management solution, companies can see into their networks to gain visibility into who has access to what, how they are using it, and what they are doing with the data. With a Vulnerability Management tool, companies can test for vulnerabilities in their infrastructures, see their biggest risks are, and even visualize the most probable attack path into their networks. However, with a Vulnerability and Access Risk Management solution, they can see how the attackers are going to get in, and companies can set up controls to alert them if hackers succeed.

This visibility is important in all industries from healthcare and financial institutions, to retail and government platforms. VARM solutions not only defend against the governance, provisioning, and compliance area of security risk; it will do so on a constant all-inclusive basis.
When enterprises think of how to prioritize solving risk within their security systems, they look at the advantages of how to save both time and money. Threat Intelligence is a force multiplier. It has become a necessary part of any security solution. Threat Intelligence can serve as a stand-alone solution or can be incorporated into a variety of security infrastructures to add to or become the full value of that solution.

With Vulnerability and Access Risk Management added to a company, it benefits by VARM acting as its own force multiplier. For example, think of the firewall in a complex IT system; a firewall allows and prevents certain IT circulation with a set of rules. Engaging the circulation that could be covertly blocked before it gets to the firewall makes it a stand-alone force multiplier. VARM has the potential to act on the infrastructure and access level to provide this force multiplier.

Now what can that mean for your company? VARM acting as a force multiplier is visible in more ways than one. It has the ability to deter known threats by instituting multi-factor authentication to increase user credential security, and it can show you the most vulnerable parts of your network so that you can remediate these issues before they are exploited. This type of intelligence solution can allow an enterprise the ability stop the validation of these target attacks to be responsive and proactive from an orchestration perspective.

You won’t be able to solve all risk at the same time, but with the help of a VARM solution, you can gain more insight into your company’s database to not only see your vulnerabilities, but to know which ones are the biggest threats to your system. A VARM solution can not only show what vulnerabilities are in the system but can prioritize them by highest risk to the organization. By taking care of the highest risks, you can reduce your threat surface and save both time and money.
The top 10 things you need in a vulnerability and access management solution to reduce your threat surface, drive down IT costs, and increase efficiencies in your organization include the ability to:

1. Recognize a problem in the infrastructure of your organization
2. Consistently monitor user access information, compliance, and provisioning risks
3. Have a complete synergy between infrastructure and access risk
4. Maintain a continuous and comprehensive view of the attack chain: Be able to go beyond pen-testing and basic IAM to gain a continuous and comprehensive view of your entire network
5. Deter, Detect, Remediate: Deter an attack through pen-testing, multi-factor authentication, and attack path modeling, detect breaches as soon as they happen, and remediate them more quickly
6. Become proactive instead of reactive: Plan for attacks by knowing your most probable attack path, be alerted more quickly when a breach happens, and act faster to eliminate lost data
7. Safeguard your system throughout the entire lateral movement of an attack: The mission should be to break the “kill chain”
8. Maintain and manage visibility: The faster you can prevent or act on a potential threat the more benefits your organization will have to protect its assets
9. Save TIME and MONEY: The faster you can prevent a threat the less data you lose saving both your bottom line and your business reputation
10. Utilize VARM as your total security foundation

A Vulnerability and Access Risk Management solution is a better way to look at safeguarding your IT system with end-to-end security. Having both solutions together will allow you to have, in a single solution, the business intelligence your enterprise needs to deter a potential threat from the infrastructure level, detect any possible access risk that may occur, and remediate risks before any disruption can affect your business. VARM is not just a solution; it is the solution for total risk management.
References

http://sapinsider.wispubs.com/Assets/Articles/2012/January/Are-You-Doing-Enough-To-Prevent-Access-Risk-And-Fraud

http://www.adviceonmanagement.com/advice_uncertainty.html


http://csqa.info/risk_management_training

http://www.veracode.com/services/penetration-testing
