Managing Security Vulnerabilities in the Cloud

Get security leadership training at SANS Institute!

MGT516: Managing Security Vulnerabilities: Enterprise & Cloud

featured at
Cloud & DevOps Security Summit & Training 2019
Denver
November 6th – 10th

featured at
SANS Security East 2020
New Orleans
February 3rd – 7th

featured at
SANS Philadelphia 2020
Philadelphia, PA
March 30th – April 3rd

Register at sans.org/mgt516
About

• David Hazar (@HazarDSec)
  • HazarDSec LLC
    • Vulnerability management, application security, cloud security, secure DevOps, and automation
    • 20 years hands-on technology & security experience with last 3 years at Deloitte helping clients improve vulnerability management
  • SANS Institute
    • Co-Author & Instructor – MGT516: Managing Security Vulnerabilities: Enterprise & Cloud (new course)
    • Instructor & Contributor – SEC540: Cloud Security and DevOps Automation
What Is Vulnerability Management (VM)?
What Is Vulnerability Management Really?

- P - Prepare
- I - Identify
- A - Analyze
- C - Communicate
- T - Treat
How does Cloud affect vulnerability management?

• Dependent on cloud strategy
  • Ad-hoc (no strategy or shadow IT)
  • Lift and shift
  • Future state
  • Lift and shift (temporary) to future state
  • PaaS, SaaS, and Serverless first
• Infrastructure as a Service (IaaS)
• Platform as a Service (PaaS)
  • Function(s) as a Service (FaaS)
• Software as a Service (SaaS)
The glass it half empty

This Photo by David Airey is licensed under CC BY-NC-ND
The Downside to Cloud VM – Visibility

• We no longer have complete visibility (shared responsibility)
  • May not be able to identify for PaaS, SaaS, and serverless
  • Certain compensating controls may no longer be as effective
    • Network layer monitoring and response less effective for any cloud services
    • Less OS visibility for PaaS and above
    • Primarily application logs for SaaS and serverless
The Downside to Cloud VM – Cloud-specific Identification

- Some vulnerabilities not identified with traditional VM toolset
  - Some vulnerabilities specific to Cloud or cloud vendor
    - Cloud misconfiguration or deviations from best practices
    - Infrastructure as Code issues (not unique to Cloud, but more common)
  - May require specialized tools
The Downside to Cloud VM – Teams and Processes

- Cloud teams and processes may be different
  - Most organizations leverage different resources to build or operate in the Cloud
  - Typically utilize different architecture, design patterns, technology, etc.
- Need to be able to adapt our policies, standards, and processes
  - Focus on goals and work with teams themselves to come up with processes
- Will most likely require many changes
The Downside to Cloud VM – Standards and Evolution

- Cloud capabilities and standards constantly changing
- Our own standards for cloud usage may not be well-defined or under development
- We may need to update our approach more frequently than we have historically
The Downside to Cloud VM (1) – Treatment Options

• May not have access to treat vulnerabilities, must rely on vendors
  • Hypervisor for IaaS
  • OS for PaaS, SaaS, Serverless
  • Core application for SaaS
• Subject to vendor treatment timelines
  • Should seek to understand their processes so we can inform our stakeholders when needed
  • Should document how we engage when concerned
The downside to cloud – Size and Scale

• Cloud usage can also evolve rapidly
  • Changes from one cloud service type to another (VMs to containers)
  • Increases in the number of resources due to the ease of setup
    • High Availability
    • Global distribution
The Downside to Cloud VM – Architecture & Design Changes

• VM architecture may require significant updates
  • Where are we allowed to store vulnerability data?
  • What does it cost to transfer that data?
  • Who is allowed to view reports for a specific region?
  • Where do we need additional scanners?
  • Should we leverage agents?
  • How do we handle overlapping IP addresses?
The Downside to Cloud VM – Resource Lifecycles / Longevity

• Cloud resources may not stick around as long, especially if we follow an immutable architecture
  • Virtual Machines / Instances – weeks or days
  • Containers – days or minutes
  • Functions – minutes or seconds

• How do we properly identify and report vulnerabilities when the underlying resources no longer exist?
• Certain metrics more difficult to capture or overall risk harder to quantify
  • Total number of vulnerabilities – how will this number ever be accurate for more than a few minutes or hours?
  • How do we calculate the risk associated with images in more dynamic environments and compare that risk to more static environments?
The Downside to Cloud VM – Operational Costs

• In the Cloud, all costs are operational
• We don’t always account for costs of scanners, data transfer, or data storage in on-premise environments due to excess capacity
• We will need to be more thorough in our analysis when expanding into the Cloud
• Pilots may be necessary to get a true picture of potential costs
The Downside to Cloud VM – Global / Regional Differences

• Easier to expand globally and introduce complexity due to regional or country-specific standards or capabilities
  • May introduce new security or privacy standards
  • Cloud capabilities not always available in all regions requiring different processes and procedures
  • Some vendor technology may not be supported in specific countries or regions as well
The glass is half full
The Upside to Cloud VM – Less Responsibility

• We no longer have complete responsibility (shared responsibility)
  • Can choose to give up responsibility for most VM processes for certain workloads
  • Allows organizations to focus on what is most important
  • Organizations will need to determine the right mix, but a heavy reliance on PaaS, SaaS, and FaaS may be appropriate since most companies are struggling to keep up
The upside to Cloud VM – Similar Technology

- The technology used is largely the same even though we may not be responsible for all of it
  - If we retain responsibility, we can leverage the same or similar technology to that we use on-premise
  - Cloud-specific, cloud-optimized, or even cloud-native solutions exist but not required and should be familiar (e.g. Amazon Inspector, AWS Config)
The Upside to Cloud VM – Similar Vulnerabilities

- The number or truly new or unique vulnerabilities is minimal
  - Infrastructure – Common Vulnerabilities & Exposures (CVEs)
  - Applications – Common Weakness Enumeration (CWEs) or OWASP Top 10 categories
The Upside to Cloud VM – Similar Metrics

• Metrics are largely the same
  • Complexity in gathering or updating may exist but formulas for calculation largely the same
  • Maybe a few different groupings or additional cloud-specific context
The Upside to Cloud VM – Cloud APIs

• Application Programming Interfaces (APIs) available
  • Most cloud vendors are either API-first or extremely API-friendly
  • Can be used for discovery to replace broad scans
  • Can aid in integration with other data sources
  • Tags can capture contextual data
  • Reporting and alerting capabilities may be more readily available
The Upside to Cloud VM – Easier to Treat / Mitigate

• Options to treat (remediate or mitigate) may be more plentiful
  • Immutable architecture allows for easier testing of changes, transition to new versions, and backout from failures
  • Compensating controls more readily available (e.g. WAF, IAM, Marketplace Solutions)
The Upside to Cloud VM - Automation

- Cloud was built on automation
- Vendors have shared many of their internal automation capabilities with customers as services
- Third-parties also providing solutions to remain relevant or solve hybrid cloud inefficiencies
The Upside to Cloud VM – Standardization

- Image usage is more common due to deployment process (possibly fewer snowflakes)
- PaaS, SaaS, and FaaS services will deprecate software versions over time forcing us to shed technical debt
- Historically, a huge reason why large numbers of vulnerabilities cannot be remediated
The Upside to Cloud VM – Economies of Scale

• More and more cloud solutions
• Cloud consumers are often struggling with same problems
• This incentivizes vendors to offer solutions
• On-premise our unique technology or unique requirements make outside help less likely without specific projects or funding
The Upside to Cloud VM – Private & Hybrid Cloud

• Will continue to become more familiar as private/hybrid cloud options become more common
  • Azure Stack, AWS Outposts, Google Anthos, VMWare Cloud, and OpenStack may replace the traditional data center
  • Over time, VM program may require less customization between on-premise and cloud workloads
Summary

• Think about vulnerability management holistically
• Don’t fear the Cloud, leverage the Cloud
• Seek to understand the Cloud in order to develop cloud-optimized strategy
• Know your organization’s cloud strategy and become integrated into that strategy
• Avoid only identifying problems by focusing on solutions
Questions?

Get security leadership training at SANS Institute!

**MGT516: Managing Security Vulnerabilities: Enterprise & Cloud**

*featured at*
- Cloud & DevOps Security Summit & Training 2019
  - Denver
  - November 6th – 10th

*featured at*
- SANS Security East 2020
  - New Orleans
  - February 3rd – 7th

*featured at*
- SANS Philadelphia 2020
  - Philadelphia, PA
  - March 30th – April 3rd

Register at sans.org/mgt516
Thank You!

David Hazar
david@hazardsec.com
https://linkedin.com/in/DavidHazar
@HazarDSec

Presentation based on:
MGT516: Managing Security Vulnerabilities: Enterprise & Cloud