5 WAYS MULTI-CLOUD DISCOVERY CAN ENHANCE IT SECURITY

While several huge security breaches have been in the news this year, the threat level continues to grow, with cybercrime getting more organized, and derailing the power of new technology.

If your organization is still struggling with ways to improve security, here are 5 ways to more efficiently bridge the gap between IT security teams and operations teams by leveraging the insight provided by data center discovery and dependency mapping.

#1 Build a common configuration repository

Establishing a configuration management process across the enterprise allows you to break silos when decisions are made that involve enterprise architecture, systems management, and IT security. Using a common repository for configuration data enables you to reduce the effort required to gather and maintain quality data from multiple sources, agree on data formats, and speak common languages.

Leveraging a comprehensive heterogenous cloud discovery and dependency mapping solution also helps reduce implementation complexity. This drives requirements for such solutions to address hybrid and multi-cloud deployments, be scalable, secured through industry certifications (e.g. FIPS140-2, Common Criteria), and able to integrate with security tools (e.g. PAM such as CyberArk, portals such as BMC Threat Director, SIEM, etc).

I have seen many implementations come to faster success via a close partnership between the configuration management team and the IT security group who provide access authorizations. This

is made possible by prioritizing the benefits of relying on trusted and up-to-date data over the risks of giving such access rights.

#2 Leverage automated inventory scans for compliance

Internal or regulatory compliance (e.g. PCI, SOX, HIPAA) require regular assessment of asset inventory, and their business function.

However, a mature organization should consider inventory audits as non-events, and rather target continuous checks and improvements. It is much more cost-effective to implement automated discovery that guarantees always available and high quality reports.

Also, at the pace of change required by digital transformation, inventory data is difficult to gather and maintain. A benefit to a multi-cloud approach is to avoid vendor lock-in, so you can expect even more change going forward. There are many benefits to establishing good discovery practices, including identifying integrations with virtualization or cloud APIs as well as identifying unknown use of applications and servers, commonly referred to as Shadow IT. Now might be a good time to review how you keep track of your compute, software, network and storage inventory and seek optimizations.

#3 Consistently identify misconfigurations

Many security breaches are a direct result of misconfigurations. Another benefit of multi-cloud discovery is achieved through leveraging its data to participate in the vulnerability management process.

Through the richness of both the raw data that is gathered, as well as additional intelligence to interpret this data, derive relationships etc, it is possible to proactively identify misconfigurations:

- This can be basic technical data such as ports that should not be open, unsupported hardware, unauthorized or vulnerable software or operating systems
- It can also be components that are not attached to a business function or that do not have the baseline security tools installed
- And dependency mapping can participate in more complex assessments such as disaster recovery or when merging infrastructure post-acquisition

Having a well-established process relying on trusted data to address configuration issues can lead you to quick wins in protecting your organization.

#4 Pragmatically prioritize remediation

Because eradicating all vulnerabilities is impossible, organizations need to prioritize vulnerabilities to isolate those that have the greatest impact, and deploy resources in the most effective manner possible.

Vulnerability knowledge bases and scanning tools allow you to sort security issue criticality, but a second angle to prioritization is to look at application maps and impact models to determine the exposure to the business.

Data center discovery and dependency mapping augments the vulnerability management process

by:

- Providing insight into how applications are deployed and protected (e.g. it might not matter as much that a web server is vulnerable to certain attacks if it is protected by a firewall)
- Providing the business context to infrastructure components (e.g. adjust the priorities based on the business impact that would result from loss of data or disruption)

#5 Strengthen change management

A challenge that is commonly faced is the friction between security teams that make system configuration recommendations (e.g. patches to deploy) and operations teams who are focused on reliability and availability.

This friction frequently results in lengthy decision cycles with an unacceptable window of exposure, and potential re-work of unplanned downtime.

Multi-cloud discovery and dependency mapping delivers an accurate and comprehensive understanding of change impacts to ensure that security implementation and remediation plans are appropriate and will result in a smooth transition. It also allows to properly track changes over time.

This results in faster decisions, safer rollouts, and improved collaboration.

Now is a good time to review your change management process and ensure it relies on robust data. The benefits will extend beyond IT security.

This post updated 10/17/2017