CLOUDY WITH A CHANCE OF AUTOMATION

Securing the cloud requires a different mindset than securing your on-prem infrastructure

ebook
An SC Media publication

Sponsored by
RAPID7

Cloud automation

Adventures in securing the cloud

As cloud operations become increasingly popular, enterprises are recognizing that they require automated cloud security services to mitigate risk. But the road to automation is not always a smooth journey, or one with a distinct destination. Security experts discuss the promise and the perils of embracing automated cloud security services. Karen Epper Hoffman reports.

Enterprise cloud operations are expanding and maturing. But like during any natural maturation, inevitable growing pains must be endured and overcome.

As organizations increasingly migrate operations to the cloud providers, security experts rapidly are realizing that automated cloud security services are essential to mitigate risk in these environments. But *automated*, they are also learning, does not mean easy or unchallenging. And further, even once the applications are firmly ensconced in the cloud automated security operations do not end.

OUR EXPERTS: Cloud

Steven Aiello, security and compliance principal, AHEAD

Doug Barbin, principal and cybersecurity practice leader, Schellman & Co

Bruce Beam, director of infrastructure and security, (ISC)²

Patrick Criss, CISO, Surety Bank

Jacob Lehmann, managing director, Friedman CyZen LLC

William Rials, associate director and professor, Tulane University

Linda Rhodes, partner and attorney, Mayer Brown LLP

Nathan Wenzler, senior director of cybersecurity, Moss Adams

Matt Wilson, chief information security advisor, BTB Security

"With the accelerating use of cloud solutions and connected devices, evolving cyber threats and changing regulatory landscapes, data privacy and cybersecurity are top priorities for businesses," says Linda Rhodes, attorney and partner in Mayer Brown LLP's technology transactions legal practice in Washington, D.C. "At the same time, big data, combined with mass computing power, is fueling the advancement and sophistication of automation and artificial intelligence, which opens up the potential for tackling difficult data privacy and cybersecurity issues."

Indeed, since the financial, operational and even security benefits of cloud environments are becoming sharply clear for a growing number of enterprises, they recognize that they must learn how to best make it all work. Forrester Research, Inc. predicted that the public cloud services market will blossom to more than $236 billion by 2020 on the strength of the business case for offloading operations to the cloud.

William Rials, associate director and professor of practice and applied computing at Tulane University's School of Professional Advancement (SoPA), teaches courses on business and technology. He points out that according to researcher Gartner Inc., by 2020 a "no-cloud policy will be as rare as a no internet policy and the global cloud market. This creates challenges for compliance and security governance using traditional, slower-moving IT methods."

But, with ever-growing cyber concerns and a continued dearth of experienced security personnel to field these issues, automated security operations must be in place as companies migrate their applications and these applications must be seen to remain secure. This is especially true even when the servers themselves are no longer under the control of the internal IT team.

21%

Percentage of files in the cloud that contain sensitive data

– McAfee

Irvine, Calif.-based Nathan Wenzler, senior director of cybersecurity at Seattle's Moss Adams accounting, consulting and wealth management firm, points out that as more companies are moving their operations into the cloud, security becomes even more critical on two fronts: security within the underlying infrastructure of the cloud service itself and additional layers of security that are hosted in their own cloud platforms to protect hosted assets.

Steven Aiello, security and compliance principal, AHEAD

"In both cases, the scalability cloud platforms provide is one of the key benefits that organizations are looking to take advantage of, but it's that same scalability that can make security measures incredibly difficult to implement and manage," Wenzler says. "For organizations [that] are not fully comfortable operating in a cloud environment, or are just making that transition, this can be a jarring problem, as the tools and techniques they once relied on for protecting their own data centers where they controlled every variable may not necessarily work any longer." Hence, the necessity of automated security tools and functions, he adds.

Security is still your responsibility

Most organizations want to move to the cloud not only to replace their data centers, but to reap business benefits such as agility, time to value, and cost control for "bursty applications," says Steven Aiello, security and compliance solutions principal for Chicago-based AHEAD, a technology consulting firm. "The cloud changes the way that security teams operate in a very similar fashion," he notes. "Security engineers no longer need to worry if hypervisors are being patched, or if their router and switching firmware is up to date."

And, as more small-and-mid-sized enterprises move to cloud environments, the requisite automated security services are moving downstream as well, according to Matt Wilson, chief information security advisor at Southampton, Pa.-based BTB Security, a cybersecurity consulting firm.

"Automation and orchestration have become the go-to methodology for risk mitigation in many organizations, but typically this practice has been reserved for larger enterprises and those with more mature information security programs," he says. "However, we've seen an increased interest from smaller organizations, although we're far from critical mass."

One of the key missteps organizations can make is in assuming that because their data or processing centers are no longer in their internal network that they can become more complacent in their own security management. This sort of out-of-sight, out-of-mind thinking can be costly.

> "Security engineers no longer need to worry if hypervisors are being patched, or if their router and switching firmware is up to date."
>
> *– Steven Aiello, security and compliance principal, AHEAD*

Patrick Criss, CISO for Deland, Fla.'s fast-growing Surety Bank, points out that by employing cloud and properly implementing automated security tools, enterprises can gain "an additional level of control and, in some cases, cover security gaps that exist in the organization itself."

>3.2B

Number of "events" generated per month in the cloud for the average organization, of which 31.3 are actual threats

– McAfee

A cloudy outlook for security?

Ensuring consistency in an enterprise's security posture is difficult enough, but in a cloud environment, this imperative becomes decidedly more complicated.

Our cybersecurity experts provide insights for how organizations might better orchestrate their security services to fit within this new cloud environment.

It's not just the technology, stupid. It is important to remember that security is not just a "technology problem" but rather is meant to address risk at all levels, including from a legal liability standpoint, says Nathan Wenzler, senior director of cybersecurity at Moss Adams consulting. "It's imperative that organizations must understand the terms of use and where liability rests for any issues that may come up from using a cloud provider's services," he says.

"The tools and automation are all there that can empower your organization to develop robust security measures around all of your cloud-based assets, but the responsibility to make good use of them is on you, not the providers," Wenzler notes Taking complete ownership of the enterprise's cloud security efforts, both with the platform and the security tools it leverages, is the key way to avoid most all of the problems that come up when running your operations from the cloud.

Leverage APIs wherever possible. One of the most important ways to help make security in the new cloud environments work is to leverage APIs wherever possible, according to Wenzler. "This is true for both your hosting platforms as well as any security tools you plan to use to protect your assets," he says. "Thankfully, most all of the major players in the cloud infrastructure services market make fairly robust APIs available so that customers can create automated integrations with their own services, applications and assets."

However, it is important to ensure that one's cloud security vendors offer products that also take full advantage of these services. It can make the difference between a security tool that claims to have some means to protect your cloud-hosted assets and one that has a more native integration with the platform itself and can scale and flex as the environment needs.

Keep the basics in mind. Countless examples exist where organizations fail spectacularly at the basics of patching, as well as hardening, configuration and access control, according to Matt Wilson, chief information security advisor at BTB Security, a cybersecurity consulting firm.

"Before we can automate, we must execute the basics well," Wilson says. "There must be qualities, parameters, and metrics measured continuously in a structured process formally assigned to someone within the organization." Another example of sticking to the basics, Wilson points out, is the ability to monitor cloud-native log events effectively. Major providers such as Amazon, Microsoft, and Google make available tremendous capabilities for audit and visibility through a variety of tools that come as part of their services.

Get it all in writing. Enterprises must ensure that their service provider gives them proper documentation and holds the certifications they require, according to Bruce Beam, (ISC)^2 director of infrastructure and security. "Once this has been established," he adds, "you can implement the automated roadmap to keep security consistent and make sure it remotes to a common location or dashboard."

Plan for changing load-balancing. Organizations should plan on cloud workloads having a very different infrastructure, according to William Rials, professor for Tulane University's School of Professional Advancement (SoPA). "We are not going to have a single cloud world or a single hypervisor world," he says. "Organization's automated cloud security should not be dependent on any single cloud service provider." The automated cloud security plan should focus on open standards as much as possible to achieve maximum compatibility, he says. — KEH

65%

Percentage of respondents who said they deploy tools that automatically enforce and redeploy configuration settings in the cloud

– Tripwire

"While this provides value, it remains paramount that the organization maintained a strong security program with the technical expertise to review and validate the controls," Criss continues. "It becomes even more important and challenging to review and validate the services that are outside of the organization's control."

Jacob Lehmann, managing director, Friedman CyZen LLC

Jacob Lehmann, managing director of Friedman CyZen LLC, the cybersecurity advisory practice of Friedman LLP, agrees. "Don't assume because it's on the cloud that security of your data and your clients' data are not your responsibility," Lehmann cautions. "Rest assured if there is a breach, your terms and services agreement will not make your cloud provider responsible for any of your lost or stolen data."

With the move to automated cloud security, enterprises still must test on a regular basis for weak credentials, lack of two-factor authentication, insecure APIs, operating system image vulnerabilities, malicious insiders, unintended information disclosures and denial of service attacks, he adds.

> "Don't assume because it's on the cloud that security of your data and your clients' data are not your responsibility"
>
> – *Jacob Lehmann, managing director, Friedman CyZen LLC*

With automation, enterprises security teams also have to be more mindful than ever before about how they keep the practices and processes regimented across the board. One of the critical security benefits of automation is that it can greatly help standardize secure configurations by removing — or at least reducing — human intervention, which can lead to inconsistencies and misconfigurations of users, Lehmann points out. But with this change comes a new, more imperative obligation for consistency.

"There needs to be a standard process for utilizing cloud resources in a secure manor, which is easily automated," Lehmann explains, citing examples of processes related to using private keys and how they are managed to access resources. "This needs to be standard operating procedure."

Adventures (and misadventures) in automating cloud security

In the military, the saying goes that a failure to plan is a plan for failure. So too it is with moving to automated cloud security services, our experts point out. "The most common mistake is starting without a plan," says Bruce Beam, (ISC)^2 director of infrastructure and security. "Without a clear plan and strategy many security vulnerabilities can be created and they often multiply as the environment expands."

Criss says that ensuring a smooth move to automated cloud services begins with the process of selecting a cloud service provider itself. "It is imperative to ensure that the service provider has applied the same security controls across all of the hosting platforms," Criss advises, noting that enterprises demand that their service provider should be contractually obligated to produce reporting, evidence of testing, and notifications of security changes or events that affect any of the existing environments where the application is currently hosted

95%

Percentage of cloud security failures predicted to be the customers' fault between now and 2022.

– Gartner

along with an environment where the application could be moved.

"As the client," Criss adds, "you should include your specific security requirements along with the regular reporting requirements, intervals and the right to audit the security controls that are agreed to."

Doug Barbin, principal and cybersecurity practice leader, Schellman & Co

As basic as it might seem, another critical misstep is in ignoring the value of embracing more automated security services in the first place. Rials says it is still commonplace for many organizations to continue using traditional — and arguably outdated — IT tools and techniques to manage cloud security and compliance. Well-meaning but misaligned enterprise cybersecurity professionals might install a firewall and intrusion prevention system/ intrusion detection system (IPS/IDS) at the network edge and control ingress and egress to the protected assets inside the network, without thought for how cloud environments demands defense in depth, he says.

"Often times it is assumed that if you simply host your firewall in the cloud, you can properly secure your cloud resources in the same way that you manage them on-premises. This type of security architecture is fundamentally at odds with today's cloud architecture," Rials says. "Applying 'tried and true' traditional cyber defense methods will not be successful in an automated cloud security environment." Instead, enterprise security teams should utilize software defined networking (SDN) security features, micro-segmentation and other cloud based security options, Rials suggests.

Even when an enterprise recognizes the vaunted need for automated security services as they venture into the cloud, they might not be doing their correct due diligence beforehand, according to Doug Barbin, principal and cybersecurity practice leader of Schellman & Company, Inc., an independent security and privacy compliance assessor, who is based in Sacramento, Calif. "The largest mistake we see is not doing a proper risk assessment," Barbin says. "Everyone says they do a risk assessment, but understanding the specific use cases and threats is most important, even when heavily leveraging cloud services."

Security concerns that might have been an issue in traditional, on-premise environments can often be more serious in the faster-paced, more rote, and often less-forgiving automated cloud scenario, according to Aiello. "When you automate a process, not only is the process executed faster, but it's executed the same way, every time, [with] servers and applications built in that same consistent manner," Aiello points out. "Dangerous cyber-attackers live in the cracks of human error in misconfiguration, and even the most advanced security analysts find deviations from the norm in their environment."

> "As the client, you should include your specific security requirements along with the regular reporting requirements, intervals and the right to audit the security controls that are agreed to."
>
> – Patrick Criss, CISO, Surety Bank

With automation completely changing the security paradigm, new security threats can emerge. For example, Aiello suggests

51%

Percentage of companies that exposed at least one cloud storage service

– RedLock

an attacker might change Windows registry keys without the IT security team knowing, or drop a web shell backdoor onto a server farm and gain remote access, if companies are not tracking their event logs.

Lehmann concurs, noting that cybersecurity professionals failing to keep tabs on these automated processes, as well as regularly monitoring and validating that all systems are working correctly, are frequent and crucial mistakes he has seen.

> “The most common mistake is starting without a plan.”
>
> – *Bruce Beam, director of infrastructure and security, (ISC)²*

“This gives a false sense of confidence that all is well,” he adds. “Companies have to be diligent in establishing secure baselines of where and how data is used on the cloud.” With automation, Lehmann says, comes a greater focus on “baking security into [development operations], not just bolting it on afterwards, [which becomes] especially critical on any platforms hosted on the cloud.”

He continues: “We see a ton of applications that are rushed into the cloud with security as an afterthought and not part of the development lifecycle.” When enterprises more frequently and thoughtfully ingrain security into their development operations (DevOps), he says, it mitigates common risk issues such as hard-coded credentials in plain text, unnecessary API functions, and a lack of business continuity regarding data privacy issues.

While automated cloud security offers undeniable advantages, Rhodes cautions that enterprises should refrain from thinking that it is a panacea for all their security ills. Since the artificial intelligence and machine learning utilized by these systems works, in large part, on probabilities — analyzing large volumes of data — these systems can more effectively and efficiently analyze certain patterns of behavior as “threats” or “non-threats.” However, as cyber threats evolve, Rhodes says, even automated security systems might “mischaracterize a behavior as a threat, when it is really not, or vice versa.”

Also, she points out, there are types of threats that “may not be subject to detection by an automated system, at least not yet or not in all cases,” such as for an unauthorized user of otherwise valid credentials or human error in uploading regulated data into a non-compliant cloud offering. For these reasons alone, Rhodes underscores the importance of continuing to actively manage, monitor and update these newer systems.

“Automated security should be viewed as a means for enhancing a company’s existing cybersecurity and data privacy program,” she concludes, “not a replacement of it.” ■

For more information about eBooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

80%

Percentage of security breaches in the cloud that involve privileged credentials

– Forrester

Sponsor

RAPID7

Rapid7 (NASDAQ:RPD) powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response, and log management for more than 7,000 organizations across more than 120 countries, including 52% of the Fortune 100.

More information is available at www.rapid7.com

Masthead

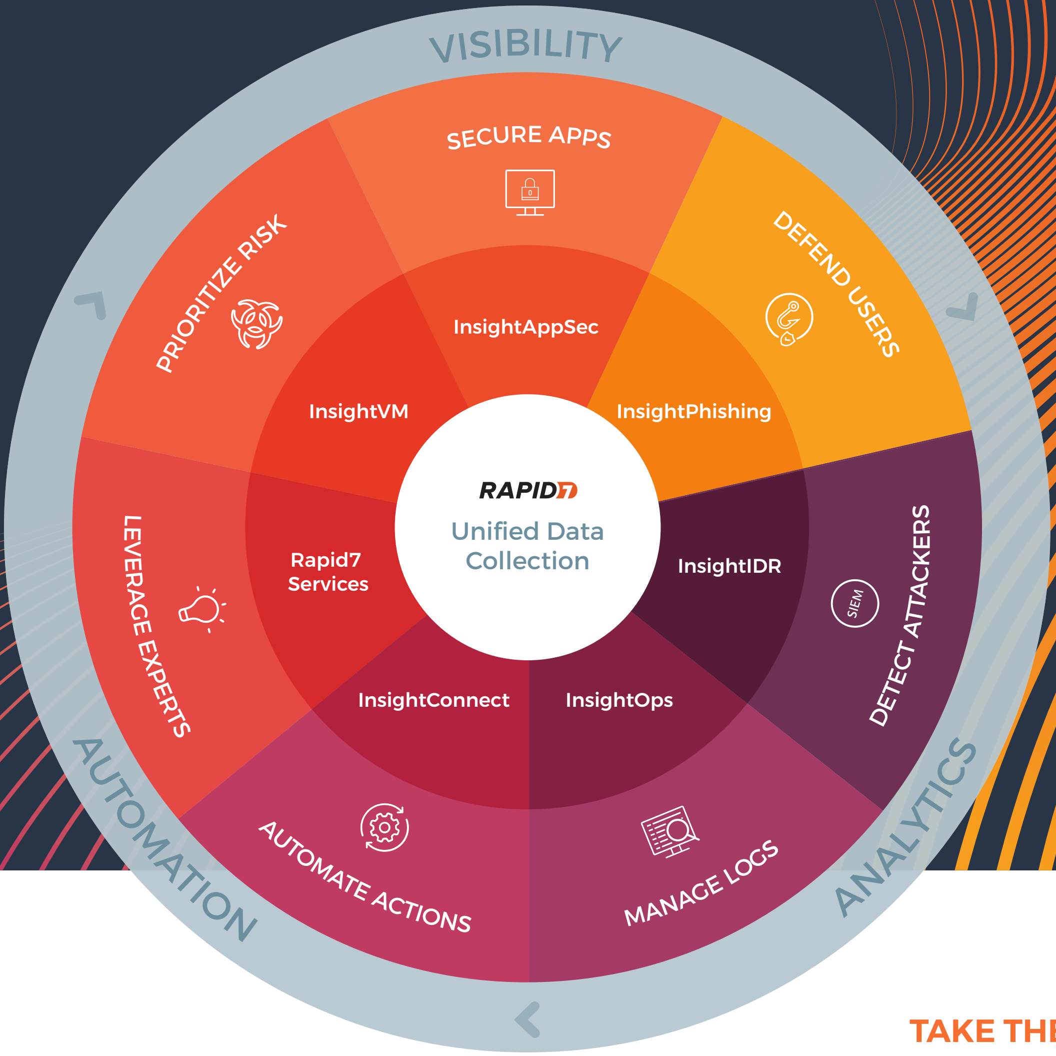
EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
SPECIAL PROJECTS EDITORIAL DIRECTOR
Stephen Lawton
stephen.lawton@haymarketmedia.com
SPECIAL PROJECTS MANAGER
Samantha Lubey
samantha.lubey@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@haymarketmedia.com*

Powering the Practice of SecOps

Security and IT solutions to reduce risk, accelerate innovation, and advance your business



TAKE THE NEXT STEP:
Visit us at www.rapid7.com