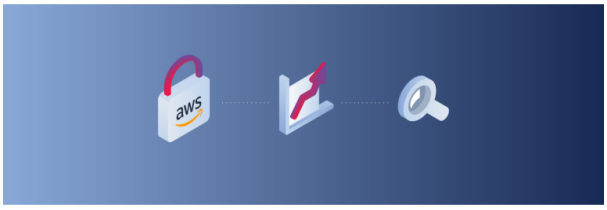
22 Most Under-Used AWS Security Metrics

by Hank Schless on September 21, 2018



22 AWS Security Pros Reveal the Most Underused/Under-Appreciated AWS Security Metrics

AWS offers a variety of built-in security features that users can take advantage of, but it's easy for users of all experience levels to get lost in the sea of options and metrics. In fact, in a November 2017 survey, we found that 73% of companies have critical AWS cloud security

misconfigurations, and more than one-fourth (27%) were not taking advantage of AWS-native security services like CloudTrail. (Misconfigurations are considered critical if they reduce or eliminate visibility for security or compliance, if they can be leveraged in a direct or complex attack, or if they enable trivial attacks on an AWS console.)

As an AWS Advanced Security Competency Partner, Threat Stack integrates deeply into AWS to provide its customers with unprecedented visibility, more advanced security capabilities, and a cloud-native user experience. Threat Stack's CloudTrail integration, for instance, bridges the visibility gap between your AWS services and the core systems running in your cloud, giving you automatic alerts about changes to your instances, security groups, S3 buckets, and access keys.

Visibility is essential for sound AWS security, and continuously monitoring your security metrics is a must. Still, while many users understand the importance of ongoing monitoring, many AWS security metrics go underutilized (or ignored). To gain more insight into these important, yet often overlooked security metrics, we reached out to a panel of AWS security experts and asked them to answer this question:

"What's the most under-used / under-appreciated metric when it comes to AWS security?"

Meet Our Panel of AWS Security Experts:

- Paul Ivanivsky
- Cris Daniluk
- Sherry Wei
- Davy Hua
- Brian Zambrano
- Lenny Liebmann
- Andrei Anisimov

- Kumar Sambhav Singh
- Ryan Kroonenburg
- Mike Baker
- Marty Burolla
- Peter Ayedun
- Uwe Weinkauf
- Vivek Chugh

- Marcus Turner
- Fraser Gough
- Marcus Bastian
- Paul McGough
- Lindsey Havens
- Jamie Shields
- Gregory Morawietz
- Stacy Caprio

Read on to find out what our panel had to say about the important AWS security metrics you might be overlooking.

Paul Ivanivsky

@ivanivsky

Paul Ivanivsky is a Security Engineer at Threat Stack. Paul has extensive experience in pentesting, blue teaming, and DevSecOps. Prior to his days in security, he held a variety of engineering positions in website and network operations, and in aerospace as a satellite operations engineer.

"AWS CloudTrail can be used for much more than mere auditing and logging purposes to conduct forensic investigations and operationalize cloud security."

Many cloud companies use AWS leverage CloudTrail in some capacity, but it's rare they're taking advantage of its full capabilities. Popular use cases for using CloudTrail include using it as a compliance aid and performing general auditing of the AWS Management Console and API calls. But it can also be leveraged as a powerful security tool. From a security perspective, it can be used to perform security analysis and automation, and highlight operational security issues. The events logs are very comprehensive, and the visibility CloudTrail provides can even help organizations investigate signs of malicious activity, such as data exfiltration and insider threats.

Cris Daniluk

@RhythmicTech
@crisdaniluk
Cris Daniluk leads Rhythmic Technologies, an innovative, compliance-oriented managed cloud and security services firm based in the Washington, D.C. area. Before founding Rhythmic, Cris was responsible for project management and business development at Claraview, where his work in securing projects worth over $100 million helped key the company's acquisition by Teradata.

"The most underused metrics are CloudWatch metrics for tracking changes reported through CloudTrail…"

CloudWatch metrics on infrequently changing security-related configurations are simple to set up. Unlike most security events that are

more often than not false positives, these are high-quality events that are always worth investigating.

We recommend everyone set up metric filters to alert on changes to account and IAM configuration at a minimum. It can also be helpful to set up metrics for changes to VPC configs, security groups, and ACLs when they're made outside of your team's business hours.

Sherry Wei

@PMEssentials_US

Sherry Wei started Aviatrix in 2013 and has raised $25 million. Aviatrix's goal is to make cloud networking as dynamic and easy as cloud computing and cloud storage. Prior to starting Aviatrix, she was senior architect at Huawei. She spent 13 years at Cisco as engineering manager. Sherry holds a Ph.D. from Purdue.

"The most under-used and under-appreciated metric in AWS security is…"

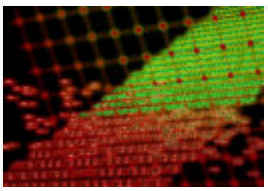
The amount of egress traffic leaving AWS VPCs that's headed for unauthorized internet sites. The reason this metric is under used is that

Illusive Networks

Tips to Secure IoT and Connected Systems w/ DigiCert

Industry Spotlight »


Overcoming the Shadow IT Catch-22


Know Your Firewall: Layer 3 vs. Layer 7

How to Safeguard Against APT Attacks

Top Stories »


Google Cracks Down on Malicious Chrome Extensions


100K Routers Hijacked for Phishing in GhostDNS Campaign

internet-bound VPC egress traffic has been a blind spot for organizations with more than a few VPCs, typically due to restrictions on how that egress traffic could be managed. Filtering traffic based on specified IP addresses provided limited visibility or involved potentially costly deployment of a separate firewall for each VPC. However, networking solutions such as software-defined cloud routers that are purpose-built for AWS can help organizations gain visibility over this traffic, effectively eliminating the blind spot — and allowing organizations to actually control their VPC egress traffic for the first time.

Davy Hua

@RealDavyHua

Davy Hua, Head of DevOps for ShiftLeft, has spent the past 17 years designing, building, and managing complex infrastructures and distributed systems architectures for both Fortune 500 enterprises and venture-backed startups. As an early adopter of the DevOps movement, his specialty is at the forefront and intersection of CI/CD and security.

“Proper attention given to the network I/O metric will add another effective tool in your AWS security practices…”

Monitoring the network I/O over a period of time will allow you to establish a baseline in order to gain a better understanding of the normal behavior of your application. This will help to isolate any anomalous spikes in network I/O traffic as an active and/or attempted attack when it cannot be correlated with a spike in normal visitor traffic.

Brian Zambrano

@brianzambrano
@very_possible
As a Senior Engineer & Cloud Architecture Practice Lead at Very, Brian Zambrano works with clients to build products that leverage serverless architecture and blockchain technologies. Brian holds two patents for his work in social event recommendations systems and authored the book *Serverless Design Patterns and Best Practices*, which was published by Packt Publications.

"The most under-appreciated metric in AWS security is…"

The number of stale IAM credentials/users with admin access. That's the most concerning thing I've noticed outside of security groups — the number of IAM users/credentials that are just floating out there unused,

potentially there for bad actors to find and exploit. Once a person has admin access, they can do a lot of damage.

Lenny Liebmann

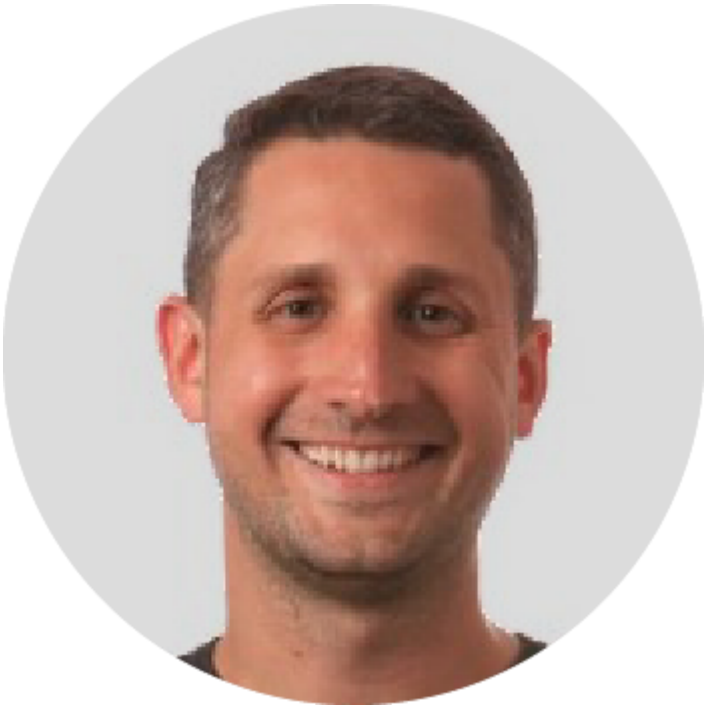
@lennyliebmann

Lenny Liebmann has been living at the intersection of business and technology for more than 30 years. After graduating Yale in 1979, he worked for AT&T Bell Laboratories during its heyday as a hotbed of innovation. He then began an independent practice that sucked him into the vortex of every successive revolution in IT — from distributed computing, the internet and convergence to mobile, social, Big Data, and cloud. Nowadays, he stays busy writing, moderating, speaking, consulting, and doing research for a diverse clientele.

"SecOps leaders generally don't pay enough attention to…"

The risk associated with the morale of their staff. We tend to think of metric as narrowly referring to numbers we can easily capture from our existing instrumentation. But of course that just means you're managing to what's easy to measure — not to what most affects your desired outcome. However, if your people are unhappy, it's not going to matter

much what kinds of tools and processes you have in place. They won't be used correctly or with the necessary passion.



Andrei Anisimov

@8baseinc

Andrei Anisimov is the Vice President of Technology at 8base, an application development platform and ecosystem that leverages blockchain technology to allow software teams to collaborate all over the world. Andrei is an experienced tech leader with a background in development for several industries and international markets. He wrote his first code at the age of 9 and won the Regional Programming Olympics in Russia at 15.

"Surprisingly, from our experience, many attack vectors don't come from sophisticated zero-day vulnerabilities…"

Rather, they have to do with basic mismanagement of logins and API keys. For example, it is not uncommon for developers to accidentally commit secret API keys into an open source GitHub repository. Hackers run automated scripts, routinely scraping AWS keys from GitHub repos in order to execute malicious activities inside captive AWS accounts. It

became so common that AWS had to implement a mechanism to notify users when their keys were exposed in a public GitHub repository. When it comes to logins, admins often fail to enable multi-factor authentication and password expiration/complexity requirements. These are well-known security practices. As such, API keys lifecycle management, password complexity, and mandatory multi-factor authentication are all important metrics to consider when evaluating AWS security.

Kumar Sambhav Singh

@Mantra_Labs
Kumar, CTO at Mantra Labs, is an expert on latest technologies like cloud computing (using AWS and Azure), blockchain, and artificial intelligence.

"Protection of data at rest is one of the most ignored aspects of security…"

AWS ensures the security of data centers, but data encryption safeguards any risk of data theft. AWS always said that it is responsible for security *of* the cloud, but that security *in* the cloud is the user's responsibility. Data in motion is already protected by AWS, but protecting data at rest — RDS, EBS, S3, Amazon Glacier, Amazon DynamoDB, Amazon EMR — with data

encryption is one of the most under-used capabilities. One of the main reasons for this ignorance is because a different mechanism or methodology has to be followed for data security.

Ryan Kroonenburg

@KroonenburgRyan

Ryan Kroonenburg is the Founder and Chairman of the Board at A Cloud Guru, the place to go and learn AWS. They have over 50,000 students and tons of courses including all 5 certification courses.

"The most under-observed security metric is…"

Your number of publicly accessible S3 buckets: That number should be zero. S3 buckets are private by default, and you have to take explicit steps to allow public, unauthenticated access. If you have questions about the security of your S3 buckets, you should run AWS Trusted Advisor's free S3 Bucket Permissions Check, which identifies S3 buckets that are publicly accessible due to Access Control Lists or policies that allow read/write access for any user.

Mike Baker

@Mosaic451

Mike Baker is the Founder and Managing Partner at Mosaic451, a managed cyber security service provider (MSSP) with expertise in building, operating, and defending some of the most secure networks in North America. Baker has decades of security monitoring and operations experience within the US government, utilities, and critical infrastructure.

"Keeping your AWS environment safe from hackers is entirely manageable…"

Barely a day goes by without news of yet another breach of an AWS S3 bucket, but these breaches are preventable. AWS is a powerful and highly secure cloud environment, but it must be configured and maintained properly. The most careless of mistakes that many companies make is not knowing what they are doing with default settings and not knowing what data they are actually making available.

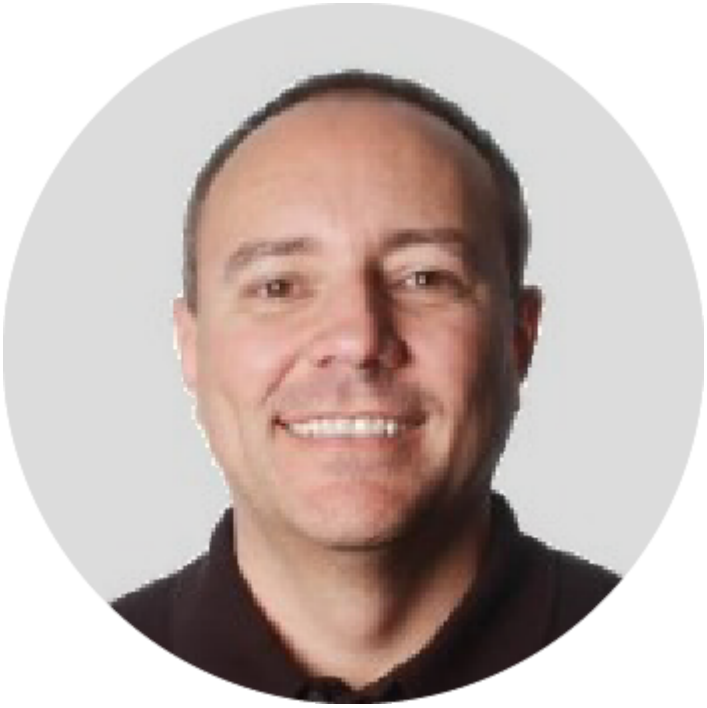
The default privacy setting for AWS S3 buckets is **owner-only**. Most AWS breaches involve organizations choosing the "all authorized users" setting when expanding access to their buckets, not realizing that this setting includes all authorized users of Amazon Web Services, not just their account. This means that anyone with an AWS account can access that bucket with whatever permissions are granted to that level of access: It's a free-for-all.

Organizations must understand what level of access they're granting to their data and who they are granting it to. A good rule of thumb is, if

you're not sure, don't do it! Get help before you end up exposing your data to the world.

The other half of this critical, but preventable, mistake is not knowing what data you actually have. Data governance is one of the pillars of cloud security. You cannot secure your data if you don't know what you have. Is your data important? Is it unique? Does it have value?

Many organizations fall prey to the "camel's nose under the tent" problem. They find that cloud computing is easy, so easy that they start migrating all manner of data into the cloud without evaluating it and considering whether it even belongs there. Eventually, really sensitive data ends up being stored in the cloud. Even worse, the IT people may not know this data exists, and it becomes a shadow IT problem. Always identify your data and run an assessment before putting it into the cloud. If you only have two levels of classification, Private or Public, treat everything as Private until you are sure it's public. Assume it's private until proven otherwise.



Marty Burolla

@EnolaLabs

Marty Burolla is a certified AWS solution architect at Enola Labs Software, an AWS consulting and service provider firm located in Austin, Texas.

“Unfortunately it’s often a tough task to assign a number to something like security…”

Security is a chain, and a chain is only as strong as the weakest link. There is not one magic dial that you can turn to make your cloud more secure. Instead, there are multiple tools/settings that have to be used correctly. Amazon has a security advisor in their AWS console that provides some tools; however, it’s quite basic and tells people to do the simple tasks that help with security. What the tool doesn’t tell you are that specific actions, such as auth tokens, should be cached in a private subnet instead of a public subnet. These tasks take an experienced engineer who understands how to build secure systems.

Peter Ayedun

@TruGridApp

Mr. Peter Ayedun has over 20 years’ of expertise in Microsoft, Cisco, and Citrix technologies. He has consulted for government and enterprise, implementing network and security solutions based on leading best practices. Microsoft regularly invites Peter to speak with, and educate business owners, on Microsoft cloud solutions, such as Azure and Office 365. Mr. Peter Ayedun is the CEO and co-founder of TruGrid, a company that specializes in Simple & Secure Workspaces for businesses.

“One of the things IT people could look at is…”

Security Event Logs to see login failure metrics to identify whether there are risks in the environment that are letting people try to hack the environment either externally or internally. Parsing through this data is often not done because the data is so large. This is why AI is so important in cybersecurity, to identity anomalies.

Uwe Weinkauf

Uwe Weinkauf is the CEO of MW2 Consulting, experts in Enterprise Application Development, Ecommerce, IT Outsourcing, and IT Operations that deliver valuable solutions for global business needs.

“AWS security can be achieved by following a variety of practices…”

There are simple ways to keep better control over data security. One way is to rotate your credentials regularly. You can create and maintain security measures over your credentials by choosing new passwords and access keys, and by making sure that all other IAM users change their passwords as well. This cuts down on the negative effects on the account if a password or access key is compromised without your knowledge.

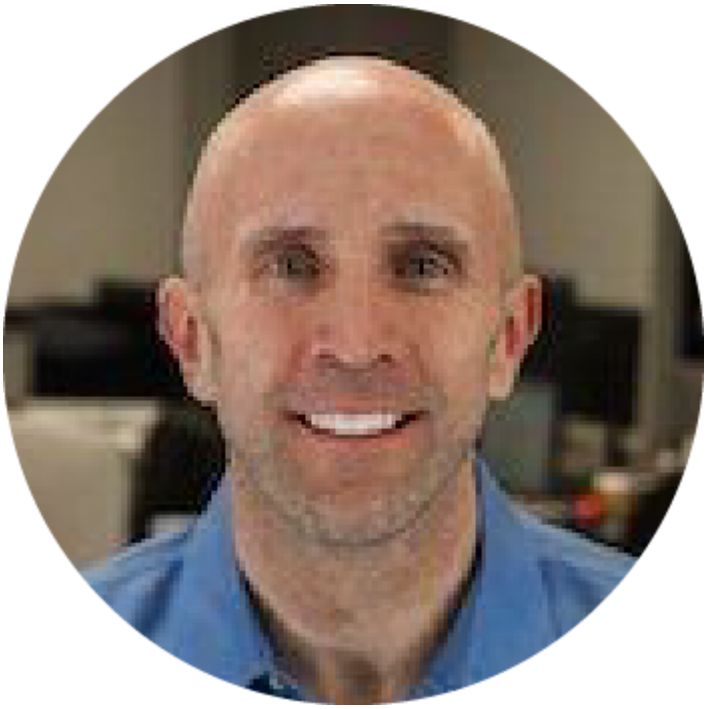
Vivek Chugh

@mylistables

Vivek Chugh is the Founder and CEO of Listables (available for Android and iOS). He's an accomplished technology leader with domestic and international experience in all business cycles, a recognized authority on the strategic application of technology to drive revenue, engineer, and manage world-class development teams, enhance service quality, improve production, and control costs.

"The most under-used and under-appreciated AWS security metric is…"

CloudTrail and CloudWatch events. They really help you to monitor the use or your app or website. For example, CloudTrail can help you define workflows that execute when events that can result in security attacks or harm are detected. It also helps with visibility into your user and resource activity by recording AWS API calls. CloudWatch can help you gain system-wide visibility into resource utilization, application performance, and operational health, in addition to many other use cases.



Marcus Turner

@EnolaLabs

Marcus Turner is the Chief Architect and CTO at Enola Labs Software, an Austin, Texas based software development and AWS consulting company. Marcus is a certified AWS architect, specializing in AWS security and legacy migration to AWS.

"The most under-used metric when it comes to AWS security is…"

Configuration Accuracy (AWS Config). AWS, when properly configured, is one of the most secure computing environments in the world. However, most data breaches are not the result of hackers leveraging complex programs to get access to critical data, but rather they come from simple unsecure points, the low hanging fruit. Even with the best security, human error is often to blame for the most critical gaps or breaches in security. Having routines to validate continuous configuration accuracy is really the most underused and under-appreciated metric.

Fraser Gough

@DigitalXRAID

Fraser Gough is the Senior Security Consultant (Security Tester) at DigitalXRAID. They provide industry-leading cyber security offerings to their customers, enabling them to reduce risk, protect digital assets, and gain knowledge using the most cost-effective approach.

“Users rarely utilize the built-in encryption for EBS (Elastic Block Storage) and S3 Storage, which is disabled by default…”

Many AWS users misconfigure S3 storage buckets. Within the AWS S3 Dashboard, ensure that no buckets have the Public tag attribute. When an S3 storage bucket is set to Public, all the information contained within is accessible by anyone over the internet without authentication. Ensure that management protocols (such as SSH) within AWS Inbound Security Group Rules are restricted to your company’s static IP address. Usually these are set to 0.0.0.0/0, which will allow anyone to have visibility to the management services over the internet.

Marcus Bastian

@clouductivity
Marcus Bastian heads Clouductivity, LLC. He is an AWS-Certified DevOps Engineer.

“Simply rotating your AWS access keys on a regular interval is a great start…”

In the IAM section of the AWS console, users can quickly see which users have stale access keys. There are also built-in facilities that allow you to determine risky security group configurations that allow remote management connectivity via ports that are opened to the entire world.

Minimizing one’s attack surface is important because usually, once an attacker is inside the walls, it’s easier to penetrate into resources. Most folks don’t realize that security isn’t intended to be a single layer system. Security is supposed to be built like an onion; that is, in layers.

Another metric that just came to mind is in the context of web application security. One can use the load balancer or HTTP access logs to alert operations teams of 401 errors. When an attacker attempts brute-force authentication or to tries to break in via other ways, you will likely see unauthorized errors in the logs. At that point, one would want to determine how they can mitigate the attack. This might be done by blocking a particular user agent that’s unexpected, or a specific IP address if the attack isn’t distributed.

Paul McGough

Paul McGough, Founder and CTO of Qwyit, LLC, a leading cryptosecurity technology firm, is a telecommunications expert with over 35 years' of progressively greater responsible experience managing IT technology teams for the development, integration, implementation, and support of financial, project management, database applications, and security systems.

"The focal point of AWS attack prevention (not recovery) is the host…"

And while HIDS (Host-based Intrusion Detection Services) will help you with a complete before, during, and after attack picture, prevention is all about taking action on those clues available prior to any attack. Access time, just like measuring the effectiveness of an athlete's actual participation time, is an extremely underutilized metric. Attacks take planning, and planning can be measured in access time — how long, when, where, and by whom. After implementing logging services at the host level, along with multi-factor authentication and login monitoring, an active, supervisory-level analysis — not just parameter-based auto reports — should be performed routinely. Access time trends, in either a positive or negative direction, when paired with systems selected, can produce surprising anomalies. The AI isn't there yet to handle this

sophisticated top-down trend view, revealing instant recognition of things “not quite right.” The best AWS security is a blend of the right tools, the right personnel, and training to look in all the right places: Attacks take planning, and planning takes access. Watch it!

Lindsey Havens

@PhishLabs

Lindsey Havens is the Senior Marketing Manager at PhishLabs with over 10 years’ of experience in Marketing, Communications, Public Relations, Lead Nurturing/Generation, and Analytics. With a unique blend of marketing and communications experience coupled with a background in behavioral and situational analysis, she brings metrics-driven results and the ability to focus sales and marketing efforts in a direction that offers the highest potential for long-term, sustainable growth.

“A common mistake that can be avoided is…”

Allowing incoming access by opening up ports for 0.0.0.0/0 in security groups. When users do this, they open their cloud networks, which can lead to their cloud resources and data being exposed to threats. One way

to avoid this unnecessary threat is to cut back on the number of open ports to reduce your attack surface.

Jamie Shields

@FlauntDigital

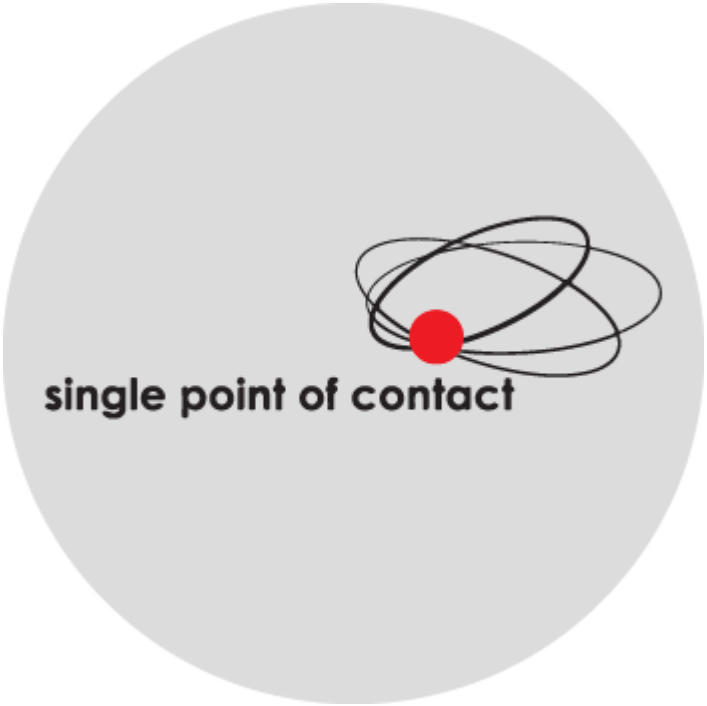
Jamie Shields is the CTO at Flaunt Digital. He's a full stack web developer, Zend and Oracle certified with over 7 years' experience working within technology startups and award-winning digital marketing agencies.

"The most under-appreciated metric for AWS security is definitely use of AWS CloudTrail…"

CloudTrail is an AWS service enabled by default on all AWS accounts. By simply logging in to the dashboard, you can find a log of every single action taken on your AWS account over the last 90 days. This type of audit trail is essential for IT security professionals and is totally free of charge.

On top of that, you can also create "trails." You can create one for free, which is a great way to test the functionality on offer. (After the first one, there is a small charge.) Trails allow you to write events to S3 buckets,

and, more recently, execute Lambda functions. This is extremely powerful. For example, you could trigger a Lambda function each time someone from outside of your corporate IP address range accesses your AWS console. The Lambda function could then alert the IT security team, or even automate some account protection functionality, or display a visual alert on the IT team dashboard.



Gregory Morawietz

@SinglePointOC

Gregory Morawietz is an IT Security Specialist at Single Point of Contact with over 20 years' of network and security experience. He has worked with hundreds of firms on improving IT environments, consulting, and integrating technology for the enterprise network.

"The most under-utilized and under-appreciated metrics are the simplest ones…"

Clearing up your basic alerts and answering your most basic security notifications is what needs to be fixed. These are actually the most important metrics. Identity and access management panels tell you what is wrong and what needs to be fixed. Pay close attention to those alarms

and alerts as they come up. Don't let an overload to occur and lose your way.

Stacy Caprio

@Stacy4Startups
Stacy Caprio is the Founder of Accelerated Growth Marketing, using proven methodologies as well as creative, customized solutions to profitably grow your business.

"Assigning different IAM roles to different IAM users is one of the most under-used and under-appreciated AWS security features…"

Many small companies have a single login with access to every role used by multiple people — which compromises security.

Recent Articles By Author

- 50 Useful Docker Tutorials for IT Professionals (from Beginner to Advanced)

- Threat Stack Announces General Availability of Its Docker Containerized Agent
- 45 Useful and Informative GDPR Presentations & Resources


More from Hank Schless

*** This is a Security Bloggers Network syndicated blog from Blog – Threat Stack authored by Hank Schless. Read the original post at: https://www.threatstack.com/blog/22-most-under-used-aws-security-metrics

AWS security, AWS Security Best Practices, AWS Security Metrics, Security Research & Strategy

← GovPayNow Breach Demonstrates Long & Short Term Impacts of Security Slips

DIS Computers benefits from switch to Managed Workplace | Avast Business →

Security Boulevard Comment Policy

Comments are moderated

ALSO ON **SECURITY BOULEVARD**

Data Breach Notification Laws: Is it Time for a Uniform

1 comment • 25 days ago

Ataur Rahman — I want cash money in my hand bangladesh any branch of the Dhaka

Pegasus Spyware Used in 45 Countries

1 comment • 15 days ago

Sy Burr — Remember "Checkpoint" security IDS systems from 20 years ago?

How and When Do You Trust a Security Vendor?

1 comment • a month ago

John Haden — Another great article David... and am interested in learning some of these

Unsuccessfully Defaced Websites

1 comment • 21 days ago

Owais Ali — Get the Fastest VPN for 2018 that allows you to access blocked and restricted content

Network
Write for Security Boulevard
Bloggers Meetup and Awards
Ask a Question
Email: info@securityboulevard.com

Sponsors Info
Copyright
TOS
Privacy Policy

DevOps.com
DevOps Connect
DevOps Institute