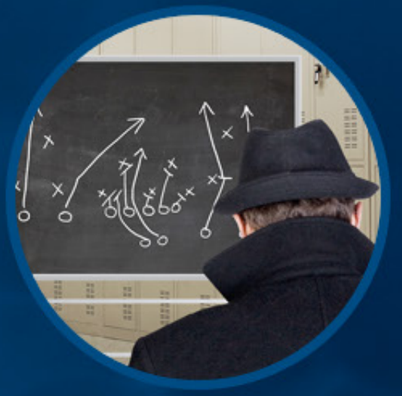


brought to you by
evident.io

TOP TEN AWS CLOUD SECURITY RISKS

and How to Resolve Them

From the company that analyzes 10 billion events every month, we present the top ten security risks found in AWS deployments.

Amazon Web Services (AWS) is so easy to get running. In an afternoon, you can build a whole new world of servers and services, ready for your workload. But when you flip the switch and make it public, what doors are you leaving open?

Proper configuration can get tricky if you don't know what you don't know. Even experts can miss avoidable, high-risk vulnerabilities in their cloud deployments. Through the Evident Security Platform (ESP), we see (and help to remediate) these issues every day.

SECURITY BEGINS WITH DISCOVERY

ESP captures over 10 billion AWS cloud events each month. These events come from companies both large and small with a broad range of experience – from cloud veterans to first timers. Every event is analyzed, prioritized, and categorized using our risk engine.

Undetected, these errors probably don't affect day-to-day operations. However, they leave the door open for potentially serious problems.

Remediation begins with discovery. Read on to learn more about establishing reliable, continuous security for your AWS assets.

Cloud technology infrastructure can quickly grow in complexity, making it difficult to be sure all of your AWS assets are properly secured.

1 CONFIGURATION PERMITS TOO MUCH NETWORK ACCESS

An insecure or invalid Network Access Control List (NACL) is in use and present in the default configuration.

WHY IS THIS A SECURITY RISK?

An insecure NACL is allowing too much network access to your AWS Virtual Private Cloud (VPC).

The default NACL is too lazy to offer much protection, and a poorly constructed NACL won't be of much use, either. This is the most common high-level risk, and should be one of the first things you fix to lock down access to your VPC and AWS services.

WHY IS THIS ALERT IMPORTANT?

Virtual Private Clouds are supposed to be private. With an insecure NACL, you have no idea who's gaining access, and your VPC's data could be at risk. Keep access locked down and only allow access to those devices and locations that need it.

AN UNSECURED VPC PUTS YOUR DATA IN DANGER.

Unsecured networks can expose customer data, personal data, and lead to legal and financial risks. New network-accessible vulnerabilities are discovered all the time, but even old vulnerabilities can lead to data breaches and open gates for bad actors. The best, most comprehensive defense is to secure your network with a strong NACL.

HOW IS IT REMEDIATED?

You can mitigate this risk by configuring a non-default NACL and applying it to your VPC. Your NACL should be restrictive, only permitting the valid internet traffic required to operate your applications and services while delivering a high quality of service to your customers.

2 ADMINISTRATIVE SSH LOGIN IS ACCESSIBLE FROM ANYWHERE

This means the entire internet has access to connect to Transmission Control Protocol (TCP) port 22.

When a security group has global permission, everyone and anyone on the internet can sink their hooks into your cloud systems.

WHY IS THIS A SECURITY RISK?

AWS defaults to this level of access. Since many users, especially those new to AWS, simply aren't aware of this out-of-the-box configuration and its potential security risks, this alert is quite common.

In fact, ESP triggers AWS:EC2-002 alerts almost as often as the signature at the top of the charts. With occurrence frequency three times that of the #3 signature in the top ten, AWS:EC2-002 represents an avoidable, **high-risk** instance that requires immediate remediation by AWS users.

WHY IS THIS ALERT IMPORTANT?

If everyone can access and connect to TCP port 22, anyone can potentially be an attacker. Too much access increases the level of risk, especially when it comes to admin accounts. A breach of this nature opens the door to denial of service (DoS) attacks and even irretrievable loss of data critical for sustaining operations.

Such attacks can – and do – cause significant revenue loss, expensive legal challenges, and even the complete shuttering of companies.

THE RISKS ARE REAL.

In 2014, CodeSpaces.com was forced to shut down after its account on AWS Elastic Compute Cloud (EC2) was compromised and hackers deleted almost all of the company's digital assets. In a more recent and higher profile incident, developers at Ashley Madison simply forgot to mitigate their AWS cloud security risk—exacerbating an already devastating breach.

HOW ARE THEY REMEDIATED?

It's pretty simple. Reduce the access to TCP port 22. You can do this by:

- Limiting permitted IP addresses allowed to communicate to destination hosts on TCP port 22
- Using the static office or home IP addresses of your employees as the permitted hosts
- Deploying a bastion host with 2-factor authentication
- Making that host the only permitted IP to communicate with any other nodes inside your account

Mitigation begins with discovery, so paying attention to and dealing with these alerts is critical to establishment of reliable, continuous security for your assets deployed on AWS.

3 USE MULTI-FACTOR AUTHENTICATION INSTEAD OF JUST PASSWORDS

Multi-factor authentication (MFA) is not enabled for your AWS user accounts.

WHY IS THIS A SECURITY RISK?

You haven't configured your AWS user accounts to use MFA. This leaves your AWS accounts open to the most embarrassing of hacks: bad passwords.

WHY IS THIS ALERT IMPORTANT?

MFA is one of the best ways to secure user accounts. It ensures that gaining access to the AWS control panel requires not only something the user knows (a password), but also something the user possesses (such as a hardware token). This additional layer of protection means you are not one stolen password away from disaster.

If someone gains unauthorized access to your AWS user accounts, they might have access to sensitive parts of your AWS configuration, private data, and important services.

If someone gets a hold of a username and password, they are already invading your network!

SINGLE-FACTOR AUTHENTICATION INCREASES YOUR VULNERABILITY.

Passwords are easy to crack. Sometimes they don't even need to be cracked, such as when French TV network TV5Monde accidentally exposed important passwords on the air in 2015. If your user accounts only need a password to be accessed, it's possible for anybody with the password or the ability to brute-force the password to gain access.

HOW IS IT REMEDIATED?

Mitigation requires enabling MFA in your AWS account. You'll get to decide between a number of different hardware and software options for authentication token generation. AWS will walk you through the selection.

4 UNUSED ACCESS KEYS AVAILABLE

Old and unused AWS access keys remain enabled in the system.

WHY IS THIS A SECURITY RISK?

Sarah left the company two years ago. Part of her job involved AWS management, so her access keys open a lot of doors. Did anybody delete or deactivate her account when she left?

It's easy to have unused, old access keys laying around. People leave the company, applications and servers go into disuse, and old devices are replaced and forgotten.

WHY IS THIS ALERT IMPORTANT?

Old, unused credentials might still be stored in retired hardware, forgotten software, or retained by ex-employees. It's important to keep access to your AWS resources locked down to just known actors. Disabling or removing unnecessary credentials will reduce the window of opportunity for malicious use of compromised credentials.

STALE AND UNUSED ACCESS CREDENTIALS CAN THREATEN YOUR INFORMATION SECURITY.

Passwords and security credentials end up in unexpected places. This happens more often than you might think. In 2014, secondhand mobile phones were used to access AT&T customer data. Keeping strict control of access keys means that they won't fall into the hands of attackers.

HOW IS IT REMEDIATED?

Evident notifies you of each account with old security credentials. It's then a simple matter to use the AWS Identity and Access Management console to delete or deactivate the unnecessary keys.

Old, unused credentials can turn up in unexpected places.

5 AUDIT LOGGING NOT TRACKING AWS ACTIVITY

No CloudTrail audit logs are being kept for AWS services in a region.

WHY IS THIS A SECURITY RISK?

Great audit tools are available in AWS, but you don't have them enabled. This means that all kinds of activity could be going on right under your nose, but you have no way to tell.

WHY IS THIS ALERT IMPORTANT?

Without audit logging, you may as well be flying blindfolded. If you don't know what's going on, how will you know if you're practicing good IT security? AWS offers a superior audit logging service called CloudTrail which provides information you'll need to know who's accessing your systems.

Without good audit logging, you're flying blind.

IGNORANCE IS BLISS, EXCEPT IN INFORMATION SECURITY.

There's nothing more embarrassing than being unaware of a security breach. In the massive 2014 eBay data breach, the lag time before discovery gave hackers a huge head start. Audit logs can give you a leg up on noticing unusual AWS activity. Insufficient or absent audit logs endanger both your company's data and your customers' information.

HOW IS IT REMEDIATED?

To be as secure and auditable as possible, always enable AWS CloudTrail. CloudTrail offers audit-logging capabilities to AWS users. To maintain consistent best practices, enable it for every account and region.

6 ANYBODY CAN ACCESS WINDOWS REMOTE DESKTOP

Permission to access the Windows Remote Desktop Protocol has been granted to everybody.

WHY IS THIS A SECURITY RISK?

Don't pile bricks in front of your Windows. Your AWS network configuration is too permissive, and any device, anywhere, can access RDP on your systems.

This can happen with a default configuration, or by a later misconfiguration. Luckily, it's easy to mitigate.

WHY IS THIS ALERT IMPORTANT?

If everyone can access and connect to your RDP ports, anyone can potentially be an attacker. Too much access increases the level of risk, especially when it comes to management protocols like this one. A breach of this nature opens the door to password hacks, complete takeovers of your Windows servers, and even irretrievable loss of critical data and customer information.

Such attacks can cause significant revenue loss, expensive legal challenges, and even the complete shuttering of companies.

PROTECTING YOUR WINDOWS SERVERS IS VITAL!

Microsoft Windows has more reported security vulnerabilities than its competitors. The Windows RDP protocol has had its share of crippling vulnerabilities in the past, and it's safe to say that it will have more in the future. Lock this protocol down and only allow access from trusted devices and locations!

HOW IS IT REMEDIATED?

Restrict access to management protocols solely to specific devices and locations within your control. Unless there's a specific reason for somebody to gain access to Windows RDP on a server, keep it locked down.

The best way to protect your Windows servers is to keep them hidden from potential attackers.

evident.io

7 ANYBODY CAN LOOK THROUGH YOUR PLAYBOOK

Internet Control Message Protocol is accessible by everybody, giving too much information to potential attackers.

WHY IS THIS A SECURITY RISK?

The network configuration for your AWS infrastructure is allowing anybody to access Internet Control Message Protocol (ICMP) information.

WHY IS THIS ALERT IMPORTANT?

ICMP is a family of network protocols used by your IT team to make sure your network is working properly. When it's open to everybody, important information could be leaked. Bad actors might discover things about your AWS infrastructure that they shouldn't know.

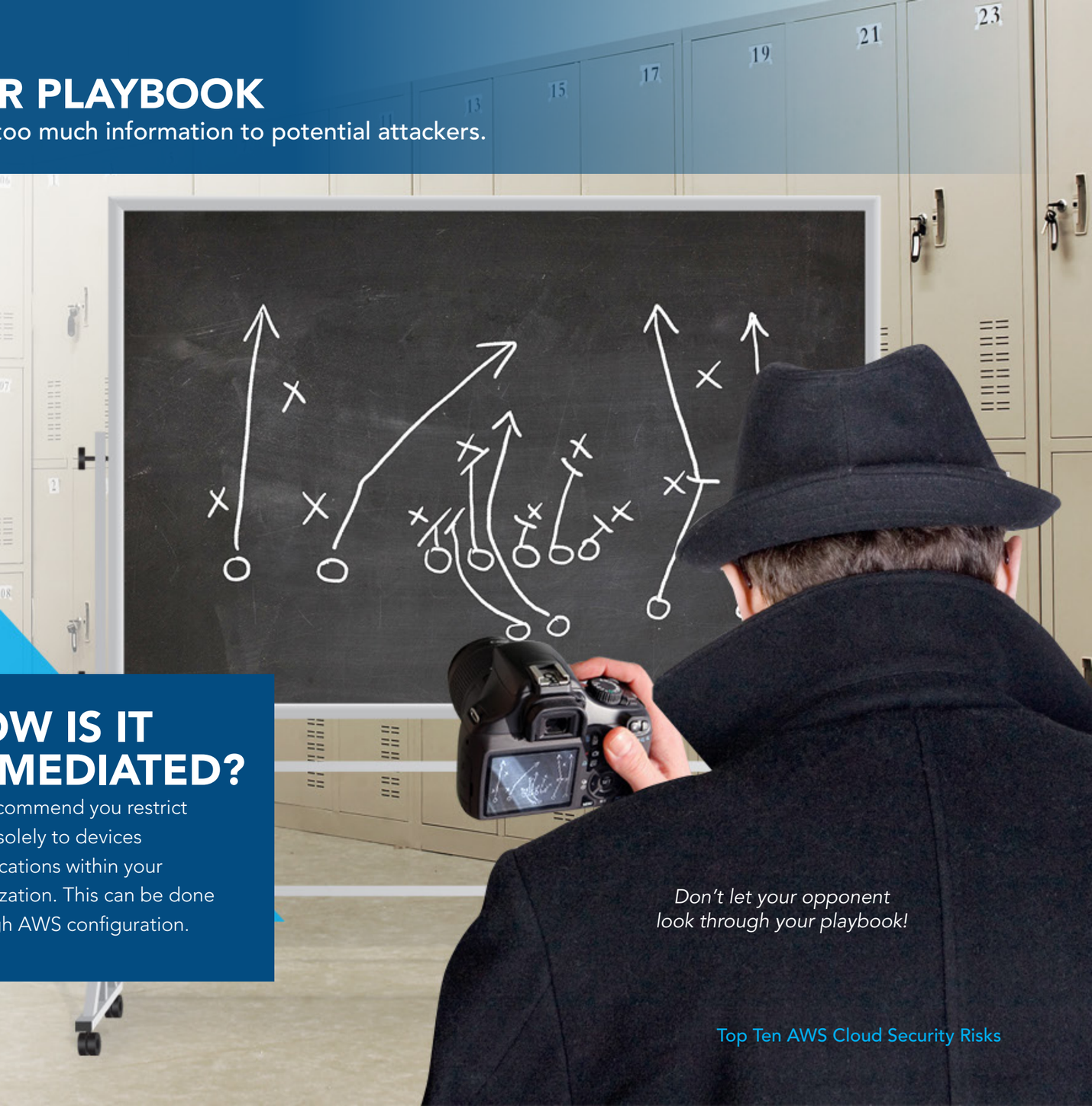
While this information might not constitute a direct threat, it makes an attacker's job a lot easier. It's like opening up your playbook and letting the opposing team learn all of your tricks!

YOUR AWS INFRASTRUCTURE IS NOT FOR PRYING EYES.

Hackers can use ICMP to probe for all kinds of information, from port scanning to network topology and even OS fingerprinting. It gets worse! The teardrop attack could use ICMP to remotely reboot certain machines. Keep ICMP usage limited to those who really need it: your DevOps team.

HOW IS IT REMEDIATED?

We recommend you restrict ICMP solely to devices and locations within your organization. This can be done through AWS configuration.



Don't let your opponent look through your playbook!

8 ANYBODY CAN CONNECT TO YOUR MYSQL DATABASE

Your MySQL database is wide open, and anybody, anywhere can try to access it.

WHY IS THIS A SECURITY RISK?

As bad ideas go, this one is way up on the list.

Your AWS configuration allows global access to MySQL. This means that anybody, anywhere can connect to your database and potentially access it.

WHY IS THIS ALERT IMPORTANT?

Maybe you really want to let the entire world have access to your MySQL database, but probably not. This is the sort of signature that should make you very uncomfortable. Never, ever leave your database open to everybody! MySQL has a robust security system built into it, but that doesn't mean that a zero day vulnerability won't give unprecedented access to a bad actor.

A compromised database can be one of the most crippling attacks. Every piece of information stored in the database can be accessed, leading to a complete data breach.

DON'T LAY OUT THE WELCOME MAT FOR BAD ACTORS.

Allowing global access to your MySQL server is a really, really bad idea. There are literally tutorials available with methods for hacking MySQL. Lock this network access down tight, to only trusted devices and locations. Better yet, make sure they are all local to the MySQL database and using encrypted connections!

HOW IS IT REMEDIATED?

Restrict network access to MySQL solely to trusted devices. Do not let the entire galaxy connect to your database!

Don't lay out the welcome mat for bad actors.

9 WIDE-OPEN EMAIL SERVERS DETECTED

You have email servers that are globally accessible, which may be a problem.

WHY IS THIS A SECURITY RISK?

Globally accessible email servers have been detected and this may or may not be a problem, depending on your use case. Your EC2 instance has a wide-open network port which allows anybody to connect to email services, and they could be sending email or clogging your disk space with garbage.

WHY IS THIS ALERT IMPORTANT?

Simple Mail Transport Protocol (SMTP) is the venerable granddad of network protocols. Everything on the internet relies on SMTP to deliver email. However, because of its age, much of the software used to handle SMTP needs extra configuration to secure it against a modern internet full of threats and bad actors.

This signature is more about awareness than an outright dangerous security hole. An open SMTP server can lead to your services being hijacked by spammers and phishers, and can also lead to an incoming flood of unexpected emails that fill up server storage and bring other vital services to a grinding halt.

KEEP YOUR EMAIL SERVERS UNDER CONTROL.

Only properly configured email servers should allow inbound connections. In most configurations, this will probably be just one or two dedicated EC2 instances built to handle SMTP. Email services on all other EC2 instances should not be reachable globally, or even externally at all. They should be configured to use an SMTP smarthost, a central mail hub designed to handle an entire organization's email.

HOW IS IT REMEDIATED?

Remove global access to email services for all EC2 instances except for those explicitly configured to manage email.

Globally accessible mail servers may be a problem – a big one!

10

GLOBALLY ACCESSIBLE FTP SERVICES HAVE BEEN DETECTED

People may be reaching your data through an old, insecure protocol.

WHY IS THIS A SECURITY RISK?

If the history of the internet were the history of rock and roll, FTP would be Beethoven. It's unencrypted, deaf to modern security threats, but still around.

File Transfer Protocol (FTP) is a very old method used to transfer files from one device to another. This signature is triggered when FTP is globally accessible for one or more of your EC2 instances.

WHY IS THIS ALERT IMPORTANT?

FTP is one of the oldest and most venerable internet protocols, dating back to 1971. It is not used for much anymore, but many systems still have legacy FTP services enabled by default. FTP has a number of problems, the biggest being that it is completely unencrypted. This means that all FTP traffic, from usernames and passwords to file contents, has the potential to be captured and read by bad actors.

USE SECURE PROTOCOLS TO TRANSFER FILES.

There is one big advantage to FTP: it's really fast over modern network connections. Unfortunately, FTP was never designed to be a secure protocol, and has numerous known weaknesses. There are many robust and secure alternatives. For file downloads, most people use web servers. For secure file transfers, you can use Secure Copy Protocol (SCP). This doesn't mean that FTP should never be used, but its limitations and weaknesses need to be well understood.

HOW IS IT REMEDIATED?

Restrict FTP access only to specific devices and for very specific reasons. If in doubt, disable it entirely and switch to SCP or another secure alternative.

FTP is one of the oldest internet protocols and has many known weaknesses.

FACING SECURITY RISKS WITH OPEN EYES

AWS CLOUD SECURITY SIMPLIFIED

AWS has lots of advantages, but can be a bit difficult to secure properly. The Evident Security Platform removes the guesswork, eliminates cumbersome manual processes, and guides you through the steps for remediation.

Take it for a spin today to see if you have any of these risks in your AWS environment. **Sign up for the free trial**.

BETTER SECURITY, HEALTHIER CLOUD

Discovering and remediating the risks associated with these top ten security alerts will make your cloud assets more secure -- saving you time and money in the process.

To learn more about how Evident.io can deliver continuous security and compliance for your assets in AWS, contact us today.

Reliable, continuous, automated security and compliance for all your AWS assets equates to reduced costs and a smoother technology operation.

*Reliable, continuous, **automated** security for all of your AWS assets equates to reduced costs and a smoother technology operation.*

evident.io

Top Ten AWS Cloud Security Risks

evident.io

Security & Compliance Automation for Public Clouds

7901 Stoneridge Dr., Suite 207, Pleasanton, CA 94588 | (855) 933-1337 | sales@evident.io | support@evident.io