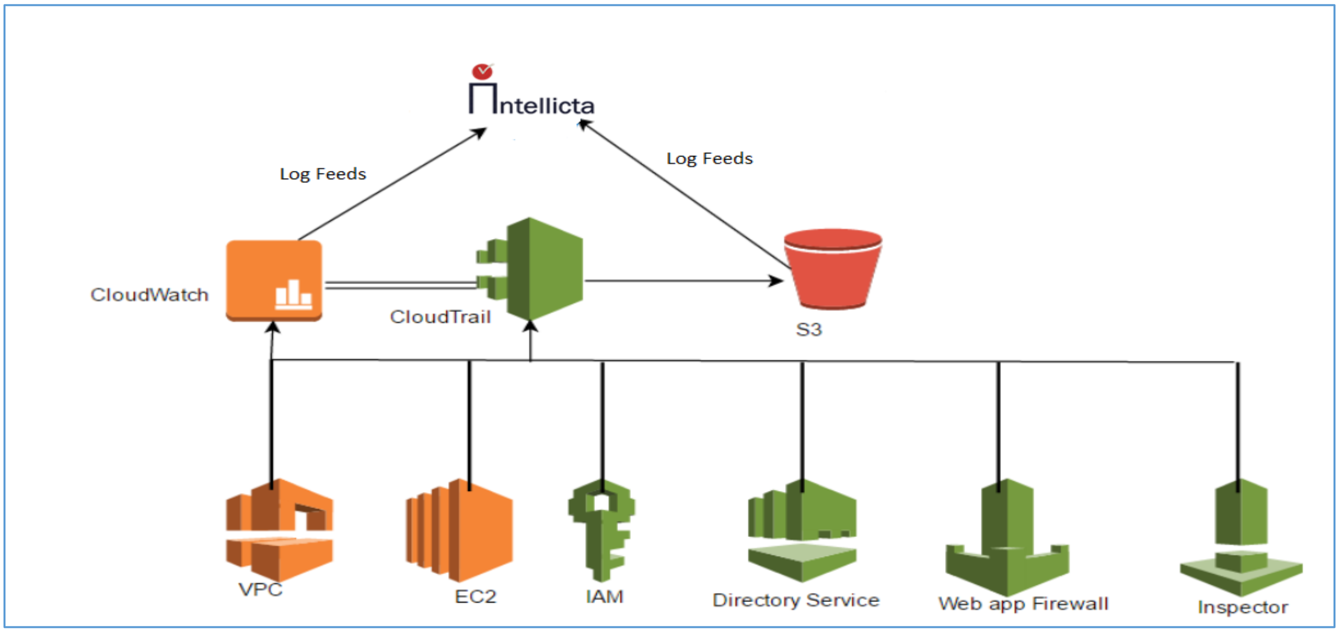
Amazon Web Services (AWS) Security – Intellicta

Under the AWS shared responsibility model, Intellicta risk assurance framework provides a 360 ^{0} visibility of multiple threat vectors that arises under the areas of Infrastructure Security, Access Control, Logging and Monitoring and Configuration and Vulnerability Analysis and Data Loss Prevention. Our unique **Digital Risk Management (DRM)** Assurance framework offers **Situational Awareness** capability to get proactive and comprehensive view for the overall cybersecurity resilience and all-inclusive dashboard across each services and application within AWS. Intellicta **Intelligent risk assurance** enables organizations to achieve a holistic view of the risk posture, detect misconfigurations, access control violation, protects from Insider threats due to privileged escalation. It bridges the gap between enterprise security silos and AWS by ensuring a peace of mind been safe and protected.

Get Protected with Intellicta for AWS Security Challenges

Intellicta powered by TechDemocracy provides 200+ unique situations and security controls as out of the box features which can be deployed day 1 for any enterprise to perform continuous monitoring the effectiveness of AWS security posture.

- **Detective Security Control**: Provide full visibility and transparency over AWS Infrastructure and Configuration, assist is adhering best practices for AWS services such as IAM, S3, EC2, ELB, VPC, RDS, and any operations on AWS etc.
- **Preventive Security Control:** Protect workloads and mitigate risks coming from Workloads with open Internet access via Security Groups, Open SSH ports, FTP Port, Telnet Port etc. Our framework also provides clear systematic alerts for Workloads deployed outside VPC, Unencrypted EBS, and Non-optimized EBS etc.

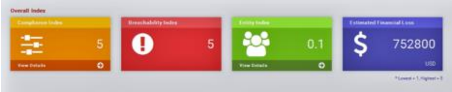


Categorization of Intellicta Driven AWS Security

TechDemocracy DRM framework reduce overall risk while accelerating growth of our customer business within AWS public infrastructure.

AWS configuration Data validation	✓ Configuration change detection with respective to Versioning, Replication, Encryption in Amazon S3, EC2, RDS, ELB etc. ✓ Detecting non MFA AWS account users ✓ Restricting the admin activities to AWS full access service users ✓ Validation of S3 public write access rule and S3 checking unrestricted public read access rule
Activity Monitoring and threat protection	✓ Creation and immediate deletion of user instantly, Change detection in cloud trail logging status(on/off), ✓ AWS user modification identification by non-root account

	✓ Detects suspicious action on S3 bucket, EC2 instance ✓ Restricts traffic to blacklist of IP Addresses and route 53 etc. ✓ Detecting suspicious AWS console login
Privilege Access Governance for AWS	✓ Privileged access management in AWS should be elastic. It is suggested to create IAM Policies only with necessary actions/permissions before assigning them to IAM users, groups and policy. ✓ Identify and manage disconnected residual access
Encrypt or Tokenize Stored Data(S3 and RDS)	✓ Detects S3 Objects with disabled Server side encryption ✓ Detects encryption on RDS DB instance connection ✓ Detects encryption on Rest data ✓ Detects RDS DB table and column encryption ✓ Detects encryption on data transition
Lateral Movement of Attack Protection	✓ Discouraging IAM users to use the Amazon STS API calls whose CLI/REST permission revoked recently ✓ Revoke STS API permission as soon as CLI/REST/SDK permission revoked ✓ Triggering an alarm when specific API calls are made such as ✓ Disabling log tracking services (Cloud Trail etc.) - Any Configuration level changes S3 / EC2 ✓ Identifying ELB configuration with insecure SSL protocols ✓ Identifying the ELB configured with week Cipher

Continuous Compliance Management	✓ Capable to load and update regulations (ISO 27001, SOX, DFS-500, NIST, HIPAA Security et..), standards or frameworks based controls
Step-up to Stronger Authentication	✓ AWS-IAM accounts creation/deletion detection by non-root account ✓ AWS user modification identification by non-root account ✓ Validate MFA in AWS account an extra layer of protection for privileged users
 Overall Index Compliance Index 5 View Details Breachability Index 5 Entity Index 0.1 View Details Estimated Financial Loss $ 752800 USD *Lowest = 1, Highest = 5 **Executive Board Level Reporting**	✓ Presentation of Gaps in Access Controls and Violation in best practices via a Dash Board ✓ Executive Reports ✓ Management Reports ✓ Quantitative Reporting