Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT

# Cloud Security Guardian

Fleming Shi and Tim Jefferson

**Cloud** is the new normal,

cloud **security** is anything but...

# Seattle, we have a problem…

500+

Native services across Azure, AWS, and GCP

K's

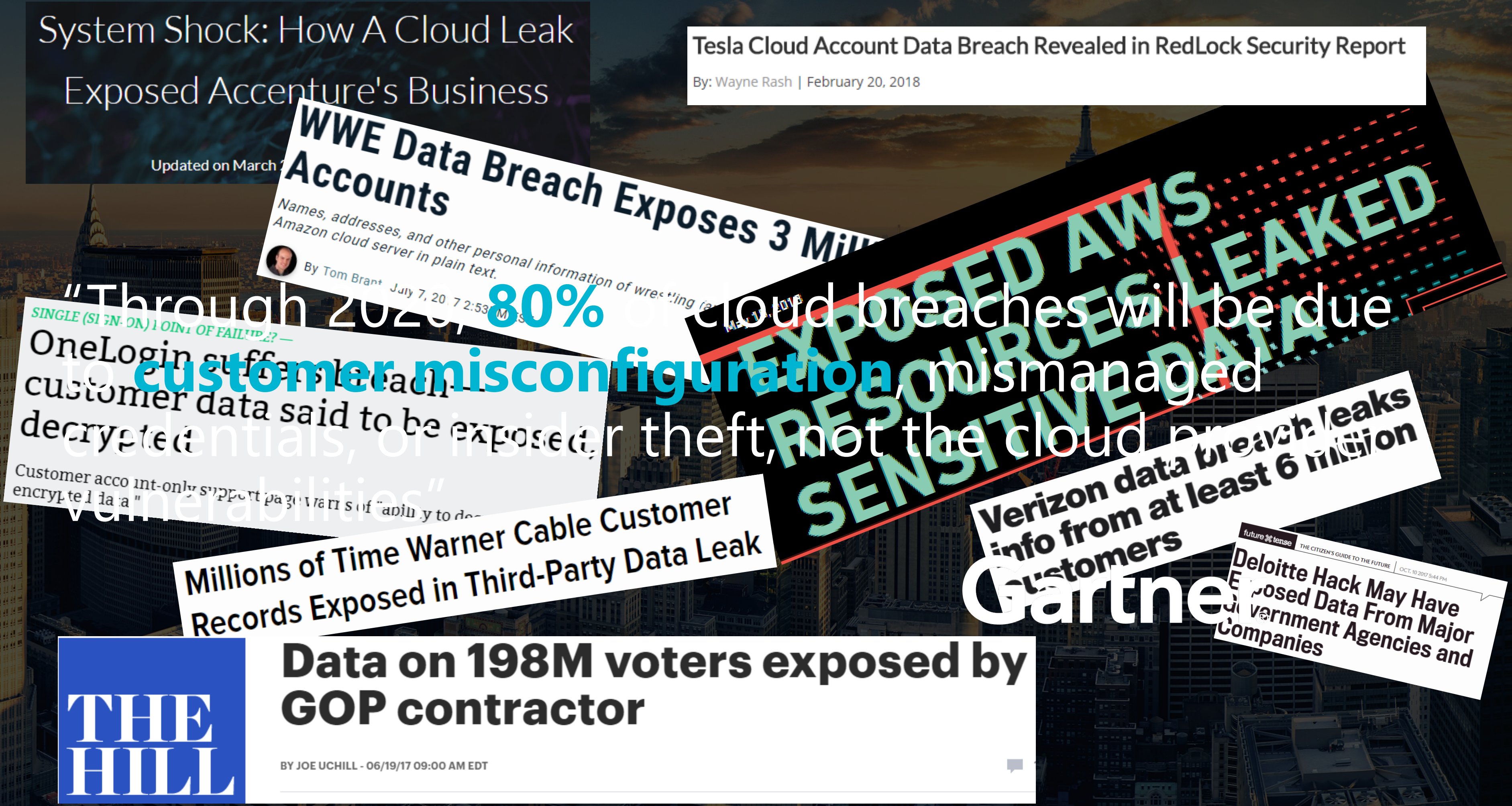
Number of new features added to services in 2018 that impact configurations

0?

Number of qualified Cloud Security Architects working for you

“Through 2020, **80%** of cloud breaches will be due to **customer misconfiguration**, mismanaged credentials, or insider theft, not the cloud provider vulnerabilities”

**Gartner**



System Shock: How A Cloud Leak Exposed Accenture's Business

Updated on March 2

Tesla Cloud Account Data Breach Revealed in RedLock Security Report

By: Wayne Rash | February 20, 2018

WWE Data Breach Exposes 3 Mil Accounts

Names, addresses, and other personal information of wrestling fa Amazon cloud server in plain text.

By Tom Brant July 7, 2017 2:53PM EST

MAY 14, 2018

EXPOSED AWS RESOURCES LEAKED SENSITIVE DATA

SINGLE (SIGN-ON) POINT OF FAILURE? —

OneLogin suffers breach—customer data said to be exposed, decrypted

Customer account-only support page warns of "ability to dec encrypted data"

Millions of Time Warner Cable Customer Records Exposed in Third-Party Data Leak

Verizon data breach leaks info from at least 6 million customers

future tense THE CITIZEN'S GUIDE TO THE FUTURE | OCT. 10 2017 5:44 PM

Deloitte Hack May Have Exposed Data From Major Government Agencies and Companies

THE HILL

Data on 198M voters exposed by GOP contractor

BY JOE UCHILL - 06/19/17 09:00 AM EDT

Builders want

**agility**

CISOs want

**control**

# “agility”}

- **Automation**
  Why can’t security just be built in?
- **Speed**
  Does security have to be a bottleneck?
- **Guardrails**
  How do I know the controls I’m using are the right ones?

# {“control”,

- **Visibility**
  What’s in our cloud? Is it secure?
- **Compliance**
  Are we automating policy assessment, enforcement and reporting?
- **Remediation**
  What happens when vulnerabilities appear or we drift out of compliance?

"Empty your mind...
be formless, shapeless...
like water."

- Bruce Lee

CIS Benchmarks™

# Securing Microsoft Azure: An objective, consensus-driven security guideline for the Public Cloud Providers

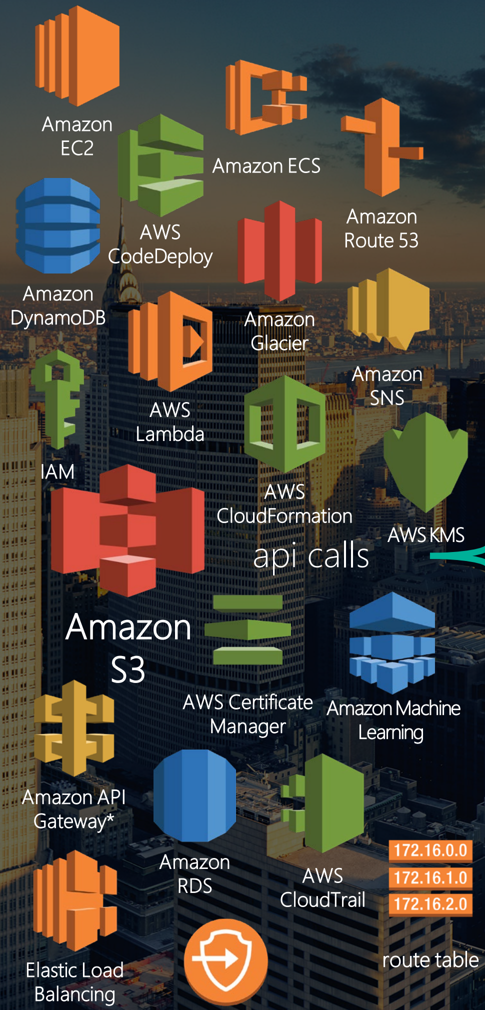
Examples:

1.18 Ensure that 'Users who can manage security groups' is set to 'None’

5.5 Ensure that Activity Log Alert exists for Delete Network Security Group

7.3 Ensure that 'Data disks' are encrypted

# Policing configuration state of every native service deployment



DeleteBucket

DeleteBucketPolicy

**DeleteObject**

DeleteObjectTagging

DeleteObjectVersion

GetBucketAcl

GetBucketLogging

GetBucketPolicy

GetEncryptionConfiguration

GetObject

GetObjectAcl

**GetObjectVersionAcl**

GetObjectVersion

**ListAllMyBuckets**

ListBucket

PutBucketAcl

PutBucketPloicy

PutBucketVersioning

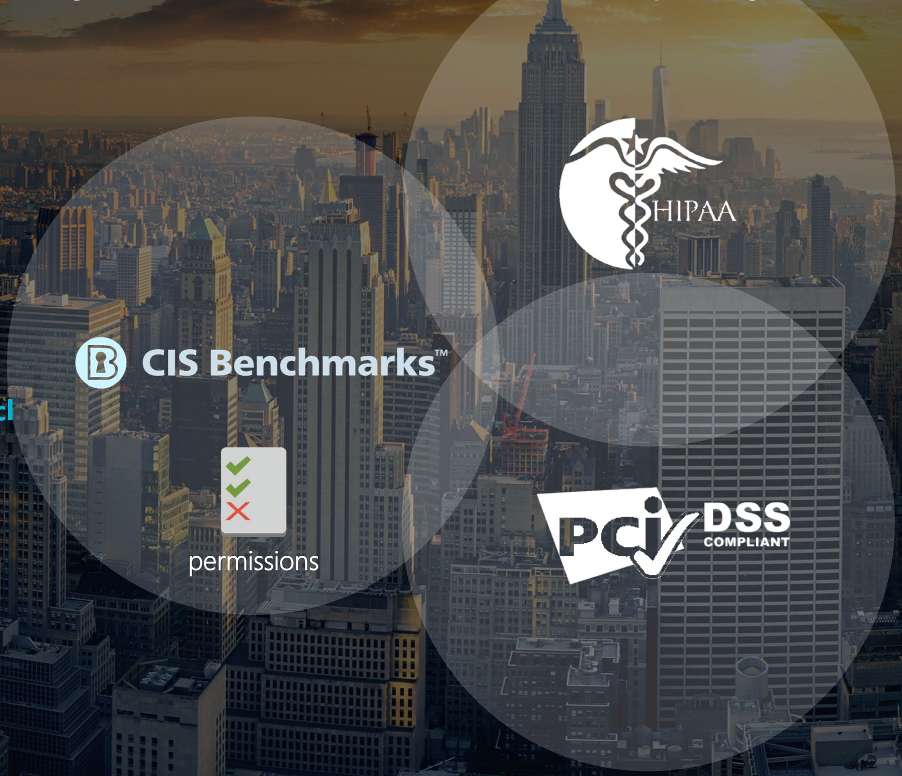
PutEncryptionConfiguration

PutInventoryConfiguration

PutObject

PutObjectAcl

...



# Example AWS cloud trail log

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
```

who and what made this call

What did they try to do and when

Requested action and response

# Policing configuration state of every native service deployment

Azure Active Directory

Azure Load Balancer

Azure Database for MySQL Servers

Azure alert

Azure Resource Group

Azure Cache for Redis

Azure Right Management (RMS)

Azure VPN Gateway

Cognitive Services

Azure DNS

Azure Sentinel

Azure Database (Generic)

Security Graph

https://.../security/alerts

https://.../security/alerts/{alert-id}

https://.../security/alerts/securityScores

https://.../security/alerts/secureScoreControlProfiles{id}

Resource Graph Explorer

https://management.azure.com/providers/Microsoft.ResourceGraph/resources?api-version=2019-04-01

HIPAA

CIS Benchmarks™

permissions

PCI DSS COMPLIANT

# Azure Security Graph Pub - CSG Alert

```
{
 "message": "List of alerts",
 "alerts": {
  "pagination": {
   "total_items": 1647,
   "items": 25,
   "limit": 25,
   "page": 1,
   "total_pages": 66
  },
  "compliance": [
   {
    "fail_reason": "Azure security center has detected incoming traffic from IP addresses, which have been identified as IP addresses that should be blocked by the Adaptive Network Hardening control",
    "description": "Traffic from unrecommended IP addresses was detected",
    "severity": "low",
    "offenders": {

    },
    "recommended_actions": [
     "1. Review the IP addresses and determine if they should be communicating with the virtual machine",
     "2. Enforce the hardening rule recommended by Security Center which will allow access only to recommended IP addresses. You can edit the rule's properties and change the IP addresses to be allowed, or alternatively edit the Network Security Group's rules directly"
    ],
    "source": {
     "alert_service": "Security Center",
```

Compliance alert and details

Recommendations

# Azure Security Graph Sub – 3$^{rd}$ Party Alert

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#Security/alerts",
  "@odata.nextLink": "https://graph.microsoft.com/v1.0/security/alerts?$top=1&$skip=1",
  "value": [
    {
      "id": "5AE9CC76-B587-4401-95C7-A8C878B7FFA5",
      "azureTenantId": "00000001-0001-0001-0001-000000000001",
      "azureSubscriptionId": "",
      "riskScore": null,
      "tags": [],
      "activityGroupName": null,
      "assignedTo": "",
      "category": "threat",
      "closedDateTime": "2019-07-13T00:00:02Z",
      "comments": [],
      "confidence": null,
      "createdDateTime": "2019-07-13T15:11:31Z",
      "description": "Traps: Malware Blocked",
      "detectionIds": [],
      "eventDateTime": "2019-07-13T15:58:31Z",
      "feedback": "unknown",
      "lastModifiedDateTime": "2019-07-13T15:11:31Z",
      "recommendedActions": [],
      "severity": "high",
      "sourceMaterials": [],
      "status": "newAlert",
      "title": "Traps: Malware Blocked",
      "vendorInformation": { …
```

Malware detected and blocked, guess who?

What? No recommendations?

# Barracuda Cloud Security Guardian

CSG

Barracuda
**Cloud Security Guardian**

# Build fast, stay secure

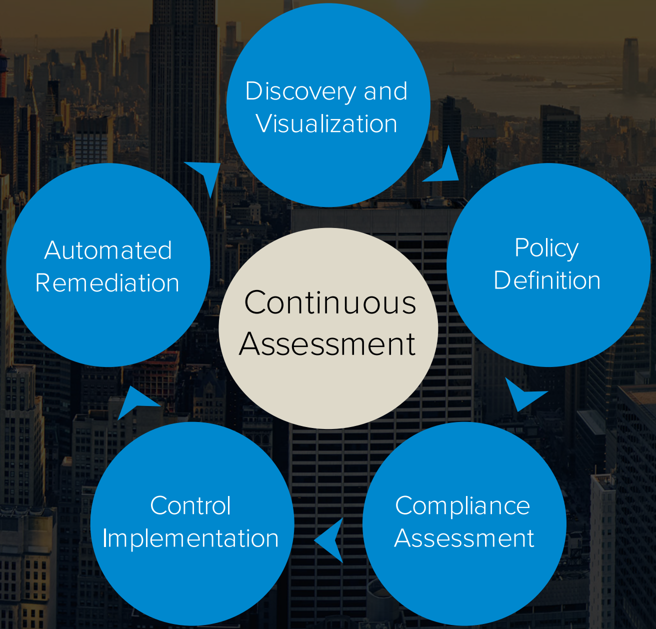
Easy-to-Use SaaS service

Watches over security and compliance

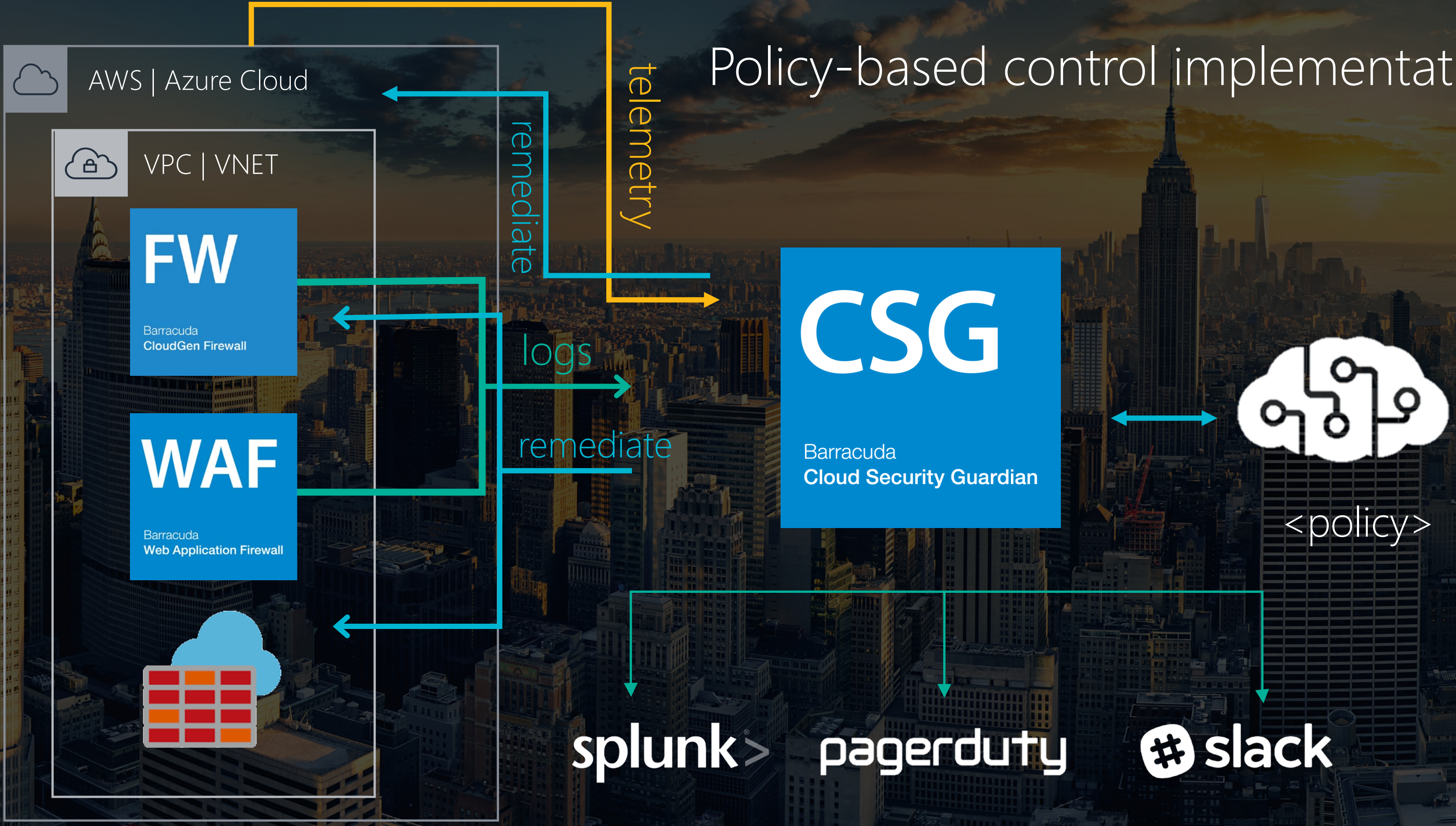
Built-in best practices - automates remediation of violations

No burden on developers - frees organizations to leverage cloud apps and remain secure

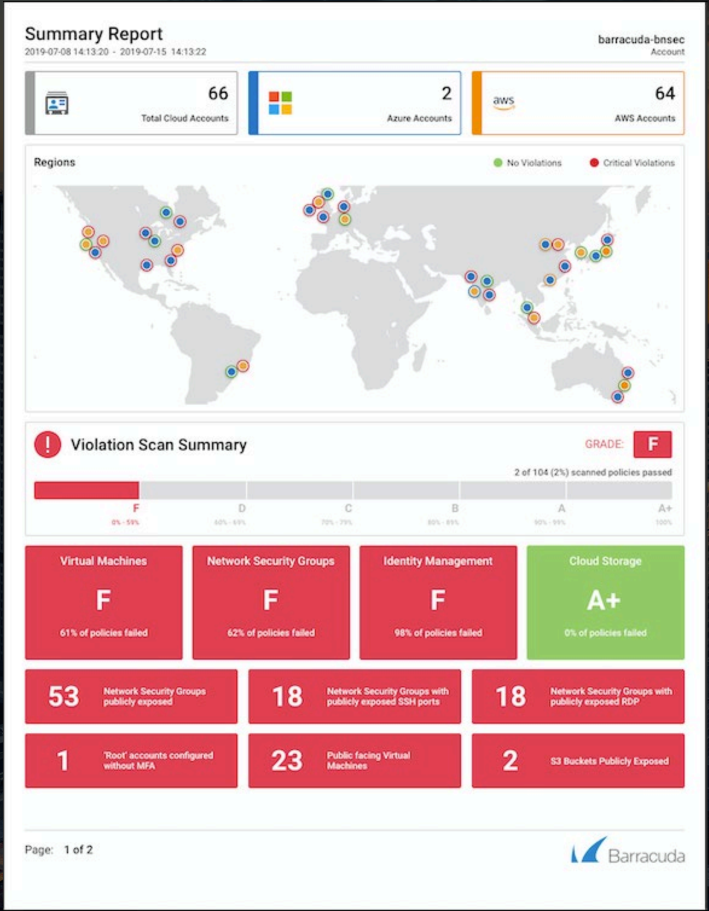
Build applications **faster** – while staying secure



# Policy-based control implementation



# A report that can help you start …



## Summary Report

2019-07-08 14:13:20 - 2019-07-15 14:13:22

barracuda-bnsec
Account

| | |
|---|---|
| 66 | Total Cloud Accounts |
| 2 | Azure Accounts |
| 64 | AWS Accounts |

Regions

● No Violations ● Critical Violations

### Violation Scan Summary

GRADE: F

2 of 104 (2%) scanned policies passed

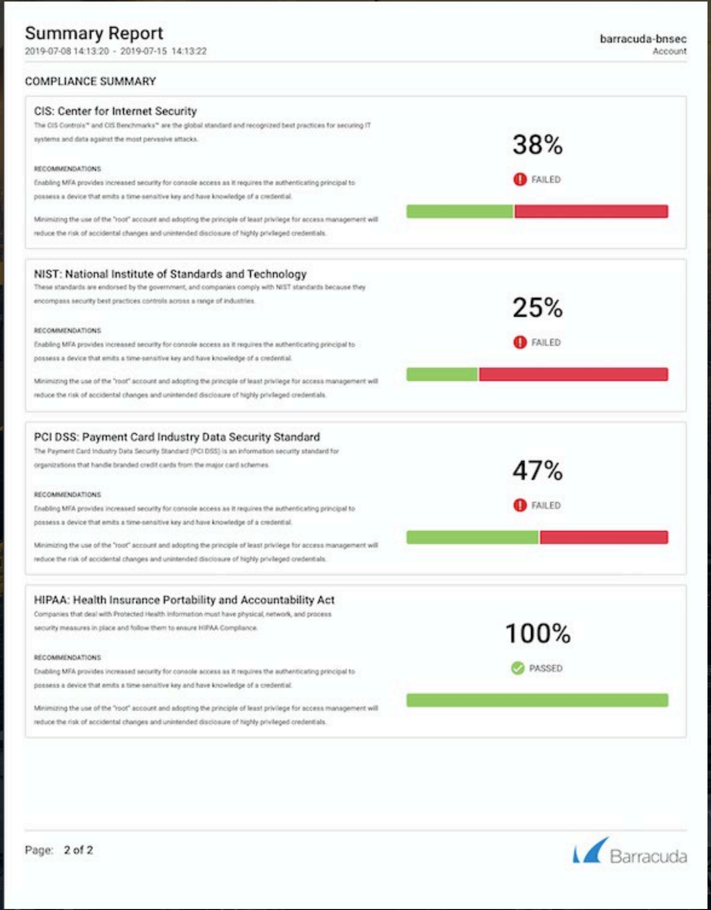
| F | D | C | B | A | A+ |
|---|---|---|---|---|---|
| 0% - 59% | 60% - 69% | 70% - 79% | 80% - 89% | 90% - 99% | 100% |

| Virtual Machines | Network Security Groups | Identity Management | Cloud Storage |
|---|---|---|---|
| F | F | F | A+ |
| 61% of policies failed | 62% of policies failed | 98% of policies failed | 0% of policies failed |

| | |
|---|---|
| 53 | Network Security Groups publicly exposed |
| 18 | Network Security Groups with publicly exposed SSH ports |
| 18 | Network Security Groups with publicly exposed RDP |
| 1 | 'Root' accounts configured without MFA |
| 23 | Public facing Virtual Machines |
| 2 | S3 Buckets Publicly Exposed |

Page: 1 of 2

Barracuda



## Summary Report

2019-07-08 14:13:20 - 2019-07-15 14:13:22

barracuda-bnsec
Account

COMPLIANCE SUMMARY

### CIS: Center for Internet Security

The CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks.

RECOMMENDATIONS

Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

Minimizing the use of the "root" account and adopting the principle of least privilege for access management will reduce the risk of accidental changes and unintended disclosure of highly privileged credentials.

38%

FAILED

### NIST: National Institute of Standards and Technology

These standards are endorsed by the government, and companies comply with NIST standards because they encompass security best practices controls across a range of industries.

RECOMMENDATIONS

Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

Minimizing the use of the "root" account and adopting the principle of least privilege for access management will reduce the risk of accidental changes and unintended disclosure of highly privileged credentials.

25%

FAILED

### PCI DSS: Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

RECOMMENDATIONS

Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

Minimizing the use of the "root" account and adopting the principle of least privilege for access management will reduce the risk of accidental changes and unintended disclosure of highly privileged credentials.

47%

FAILED

### HIPAA: Health Insurance Portability and Accountability Act

Companies that deal with Protected Health Information must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance.

RECOMMENDATIONS

Enabling MFA provides increased security for console access as it requires the authenticating principal to possess a device that emits a time-sensitive key and have knowledge of a credential.

Minimizing the use of the "root" account and adopting the principle of least privilege for access management will reduce the risk of accidental changes and unintended disclosure of highly privileged credentials.

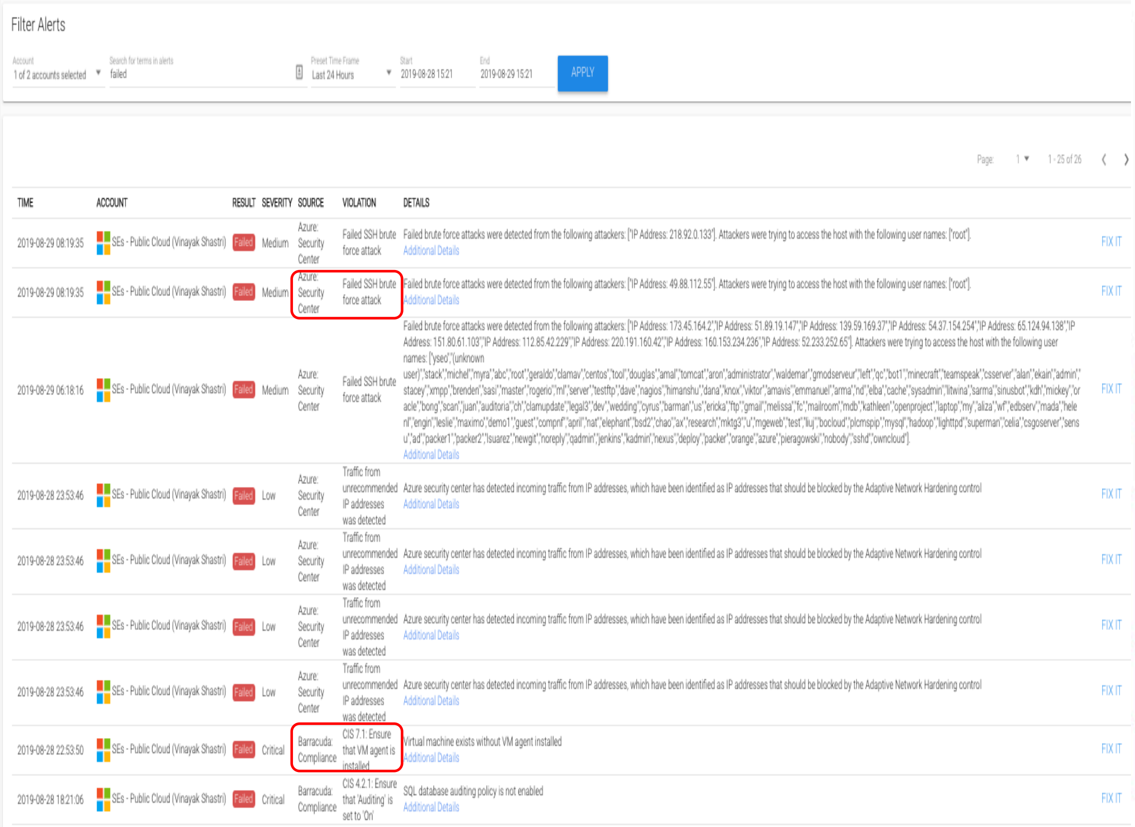
100%

✓ PASSED

Page: 2 of 2

Barracuda

# Monitor Security Violations

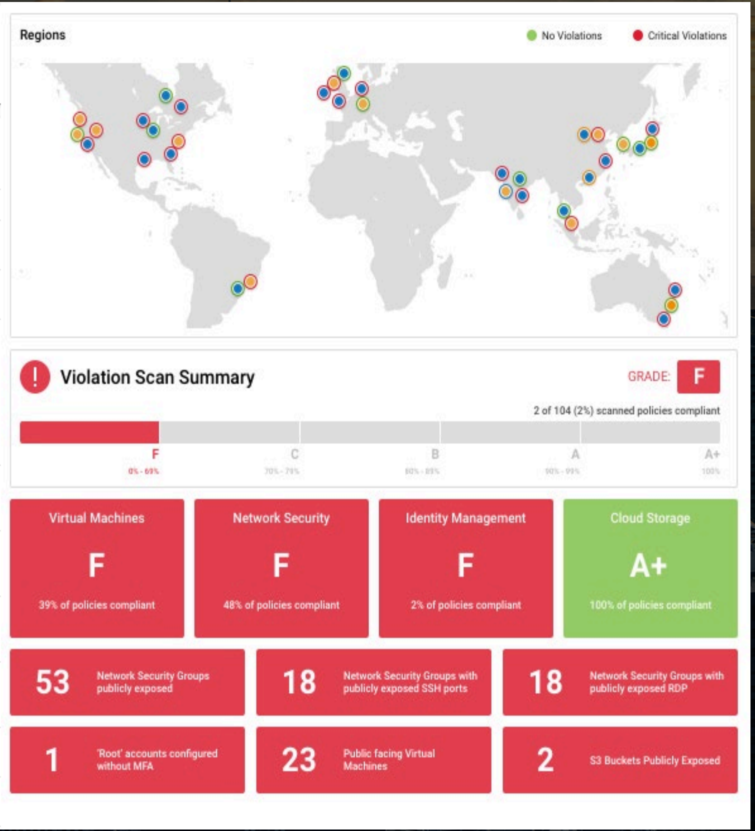


Filter Alerts

Account: 1 of 2 accounts selected
Search for terms in alerts: failed
Preset Time Frame: Last 24 Hours
Start: 2019-08-28 15:21
End: 2019-08-29 15:21

Page: 1 ▾ 1 - 25 of 26 ‹ ›

| TIME | ACCOUNT | RESULT | SEVERITY | SOURCE | VIOLATION | DETAILS | |
|---|---|---|---|---|---|---|---|
| 2019-08-29 08:19:35 | SEs - Public Cloud (Vinayak Shastri) | Failed | Medium | Azure: Security Center | Failed SSH brute force attack | Failed brute force attacks were detected from the following attackers: ['IP Address: 218.92.0.133']. Attackers were trying to access the host with the following user names: ['root'].<br>Additional Details | FIX IT |
| 2019-08-29 08:19:35 | SEs - Public Cloud (Vinayak Shastri) | Failed | Medium | Azure: Security Center | Failed SSH brute force attack | Failed brute force attacks were detected from the following attackers: ['IP Address: 49.88.112.55']. Attackers were trying to access the host with the following user names: ['root'].<br>Additional Details | FIX IT |
| 2019-08-29 06:18:16 | SEs - Public Cloud (Vinayak Shastri) | Failed | Medium | Azure: Security Center | Failed SSH brute force attack | Failed brute force attacks were detected from the following attackers: ['IP Address: 173.45.164.2','IP Address: 51.89.19.147','IP Address: 139.59.169.37','IP Address: 54.37.154.254','IP Address: 65.124.94.138','IP Address: 151.80.61.103','IP Address: 112.85.42.229','IP Address: 220.191.160.42','IP Address: 160.153.234.236','IP Address: 52.233.252.65']. Attackers were trying to access the host with the following user names: ['yseo','(unknown user)','stack','michel','myra','abc','root','geraldo','clamav','centos','tool','douglas','amal','tomcat','aron','administrator','waldemar','gmodserveur','left','qc','bot1','minecraft','teamspeak','csserver','alan','ekain','admin','stacey','xmpp','brenden','sasi','master','rogerio','ml','server','testftp','dave','nagios','himanshu','dana','knox','viktor','amavis','emmanuel','arma','nd','elba','cache','sysadmin','litwina','sarma','sinusbot','kdh','mickey','oracle','bong','scan','juan','auditoria','ch','clamupdate','legal3','dev','wedding','cyrus','barman','us','ericka','ftp','gmail','melissa','fc','mailroom','mdb','kathleen','openproject','laptop','my','aliza','wf','edbserv','mada','helenl','engin','leslie','maximo','demo1','guest','compnf','april','nat','elephant','bsd2','chao','ax','research','mktg3','u','mgeweb','test','liuj','bocloud','plcmspip','mysql','hadoop','lighttpd','superman','celia','csgoserver','sensu','ad','packer1','packer2','lsuarez','newgit','noreply','qadmin','jenkins','kadmin','nexus','deploy','packer','orange','azure','pieragowski','nobody','sshd','owncloud'].<br>Additional Details | FIX IT |
| 2019-08-28 23:53:46 | SEs - Public Cloud (Vinayak Shastri) | Failed | Low | Azure: Security Center | Traffic from unrecommended IP addresses was detected | Azure security center has detected incoming traffic from IP addresses, which have been identified as IP addresses that should be blocked by the Adaptive Network Hardening control<br>Additional Details | FIX IT |
| 2019-08-28 23:53:46 | SEs - Public Cloud (Vinayak Shastri) | Failed | Low | Azure: Security Center | Traffic from unrecommended IP addresses was detected | Azure security center has detected incoming traffic from IP addresses, which have been identified as IP addresses that should be blocked by the Adaptive Network Hardening control<br>Additional Details | FIX IT |
| 2019-08-28 23:53:46 | SEs - Public Cloud (Vinayak Shastri) | Failed | Low | Azure: Security Center | Traffic from unrecommended IP addresses was detected | Azure security center has detected incoming traffic from IP addresses, which have been identified as IP addresses that should be blocked by the Adaptive Network Hardening control<br>Additional Details | FIX IT |
| 2019-08-28 23:53:46 | SEs - Public Cloud (Vinayak Shastri) | Failed | Low | Azure: Security Center | Traffic from unrecommended IP addresses was detected | Azure security center has detected incoming traffic from IP addresses, which have been identified as IP addresses that should be blocked by the Adaptive Network Hardening control<br>Additional Details | FIX IT |
| 2019-08-28 22:53:50 | SEs - Public Cloud (Vinayak Shastri) | Failed | Critical | Barracuda: Compliance | CIS 7.1: Ensure that VM agent is installed | Virtual machine exists without VM agent installed<br>Additional Details | FIX IT |
| 2019-08-28 18:21:06 | SEs - Public Cloud (Vinayak Shastri) | Failed | Critical | Barracuda: Compliance | CIS 4.2.1: Ensure that 'Auditing' is set to 'On' | SQL database auditing policy is not enabled<br>Additional Details | FIX IT |



Violation Scan Summary

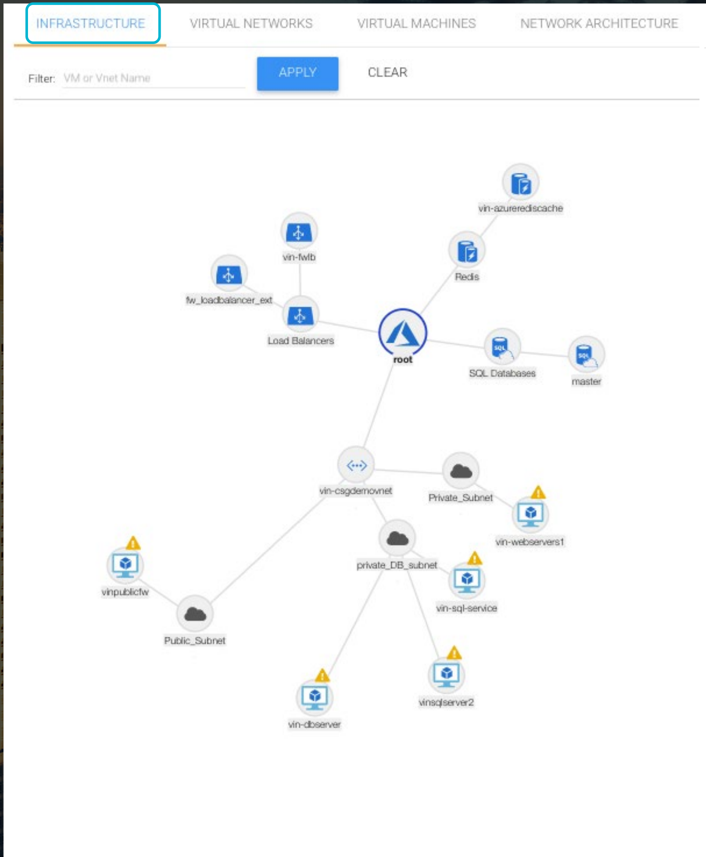
GRADE: F

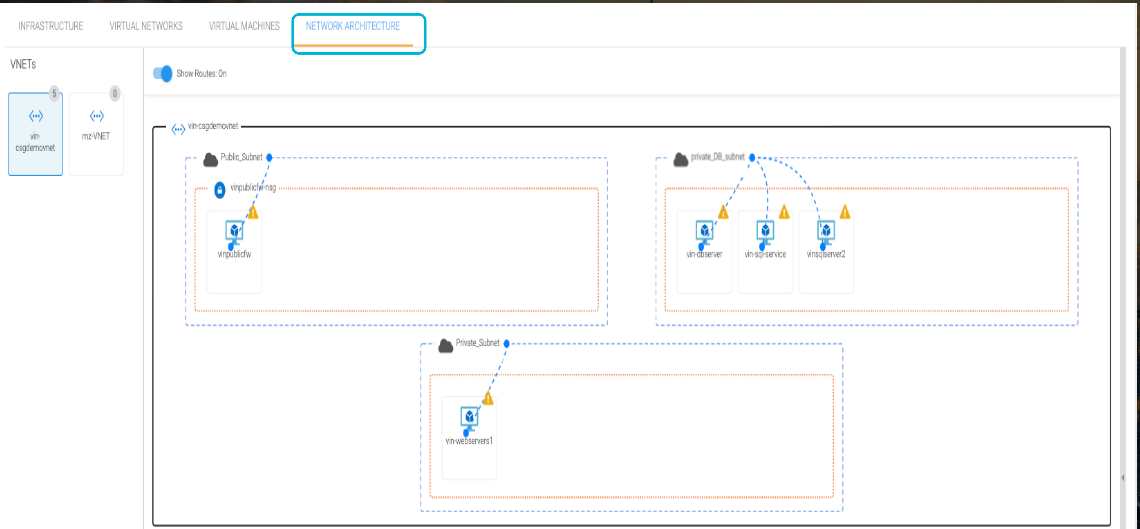
2 of 104 (2%) scanned policies compliant

| Virtual Machines | Network Security | Identity Management | Cloud Storage |
|---|---|---|---|
| F | F | F | A+ |
| 39% of policies compliant | 48% of policies compliant | 2% of policies compliant | 100% of policies compliant |

| | | | | | |
|---|---|---|---|---|---|
| 53 | Network Security Groups publicly exposed | 18 | Network Security Groups with publicly exposed SSH ports | 18 | Network Security Groups with publicly exposed RDP |
| 1 | 'Root' accounts configured without MFA | 23 | Public facing Virtual Machines | 2 | S3 Buckets Publicly Exposed |

# Gain Visibility of your Cloud Infrastructure





# Thank you

Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT