Reaching for Cloud 9:

Key Enablers for Secure Cloud Computing

Dave Odom, CISSP

About Me

- **Occupation:** CISO - Naval Nuclear Laboratory
- **Background:** Naval Officer (Cryptology/IW)
  - Computer Network Operations – NSA
- **Technical Editor**
  - Grey Hat Hacking (1st Edition)
- **Security Operations Center Analyst**
  - IRS CSIRC
- **Technical Curriculum Developer**
- **Director Cyber Youth Boot Camp**

Topics of Discussion

- Cloud Landscape Overview
- Implementation Challenges
- Key Security Enablers
- Recommendations

Industry Statistics (1)

- Nearly 80% of companies plan to have 10% or more of their workloads in the public cloud[1].

- Gartner forecasted the public cloud services market to grow 21.4% in 2018.

- Cloud services expected to account for 50% of the market by 2020[2].

[1] Source: McKinsey global cloud cybersecurity research, 2017

[2] Source: Morgan Stanley (Brian Nowak) GeekWire Cloud Tech Summit

Industry Statistics (2)

Five Year Forecast for Public Cloud Services

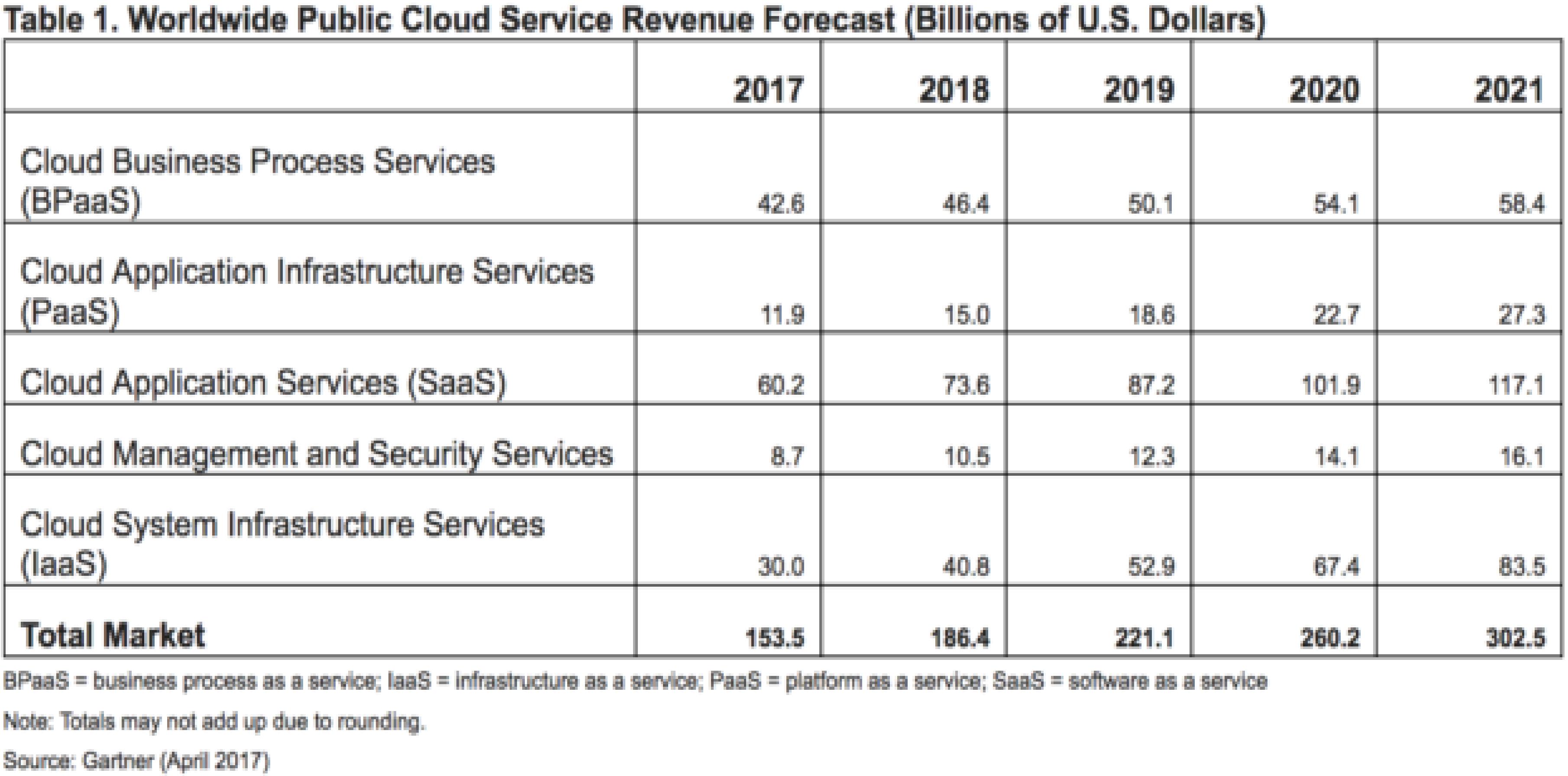


Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.6	46.4	50.1	54.1	58.4
Cloud Application Infrastructure Services (PaaS)	11.9	15.0	18.6	22.7	27.3
Cloud Application Services (SaaS)	60.2	73.6	87.2	101.9	117.1
Cloud Management and Security Services	8.7	10.5	12.3	14.1	16.1
Cloud System Infrastructure Services (IaaS)	30.0	40.8	52.9	67.4	83.5
Total Market	**153.5**	**186.4**	**221.1**	**260.2**	**302.5**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service

Note: Totals may not add up due to rounding.

Source: Gartner (April 2017)

Why Is Cloud Security Relevant?

- 91% of organizations are concerned about cloud security[1] and security is considered to be one of the top barriers to cloud migration[2].
- Migrations of workloads into cloud environments introduces unique security challenges.
- Only 16% of organizations reported that traditional security tools are sufficient to manage cloud security[1].
- Serious ramifications exist when adequate security controls are not enabled.

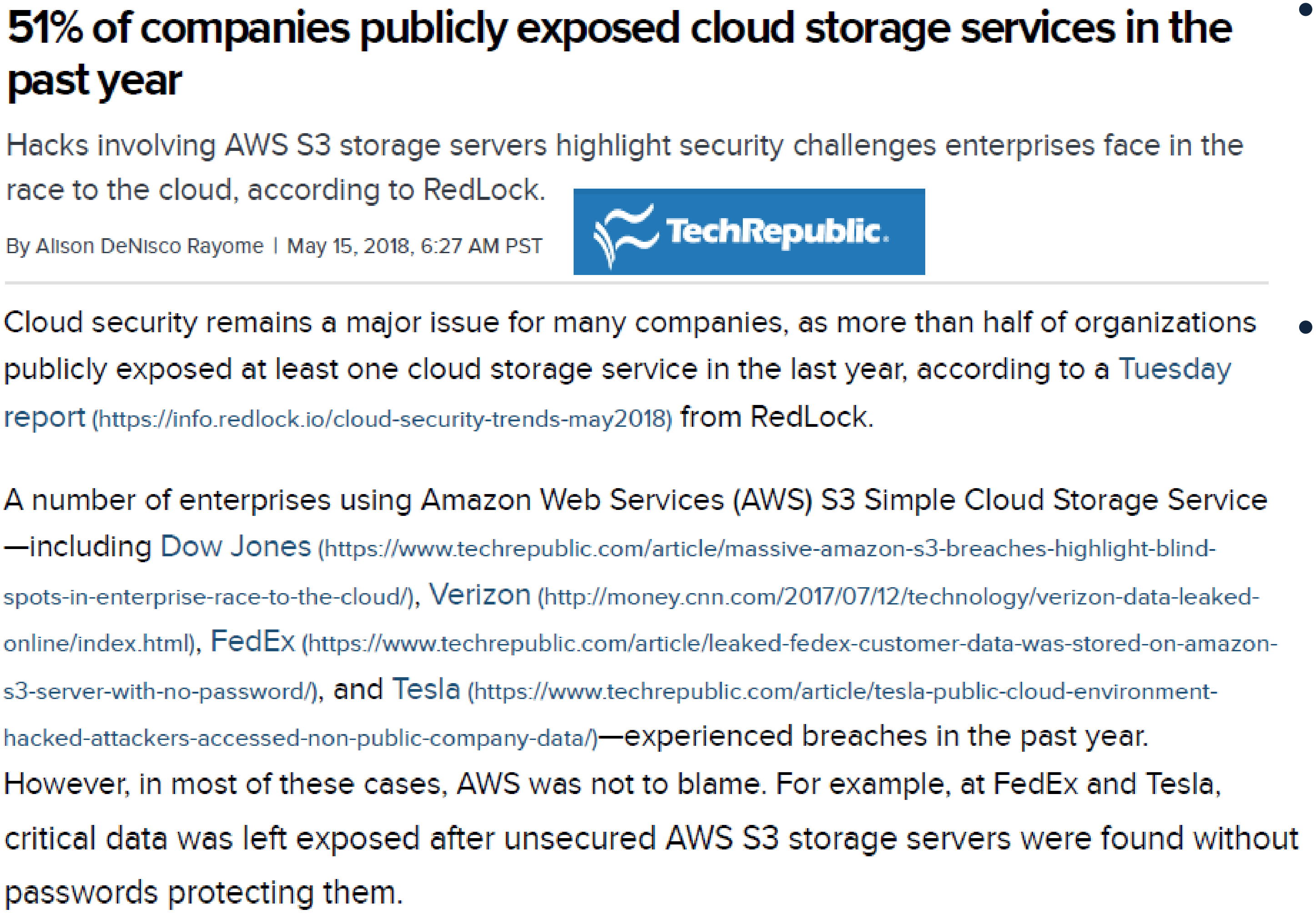
[1]Source: ISC^2 Cloud Security Report 2018, Source: McKinsey Global Cloud Cybersecurity Research, 2017[2]

Quote from a "Subject Matter Expert"

One does not simply configure an Amazon S3 bucket with

public read/write permissions and expect it to remain secure!

What Can Go Wrong?



51% of companies publicly exposed cloud storage services in the past year

Hacks involving AWS S3 storage servers highlight security challenges enterprises face in the race to the cloud, according to RedLock.

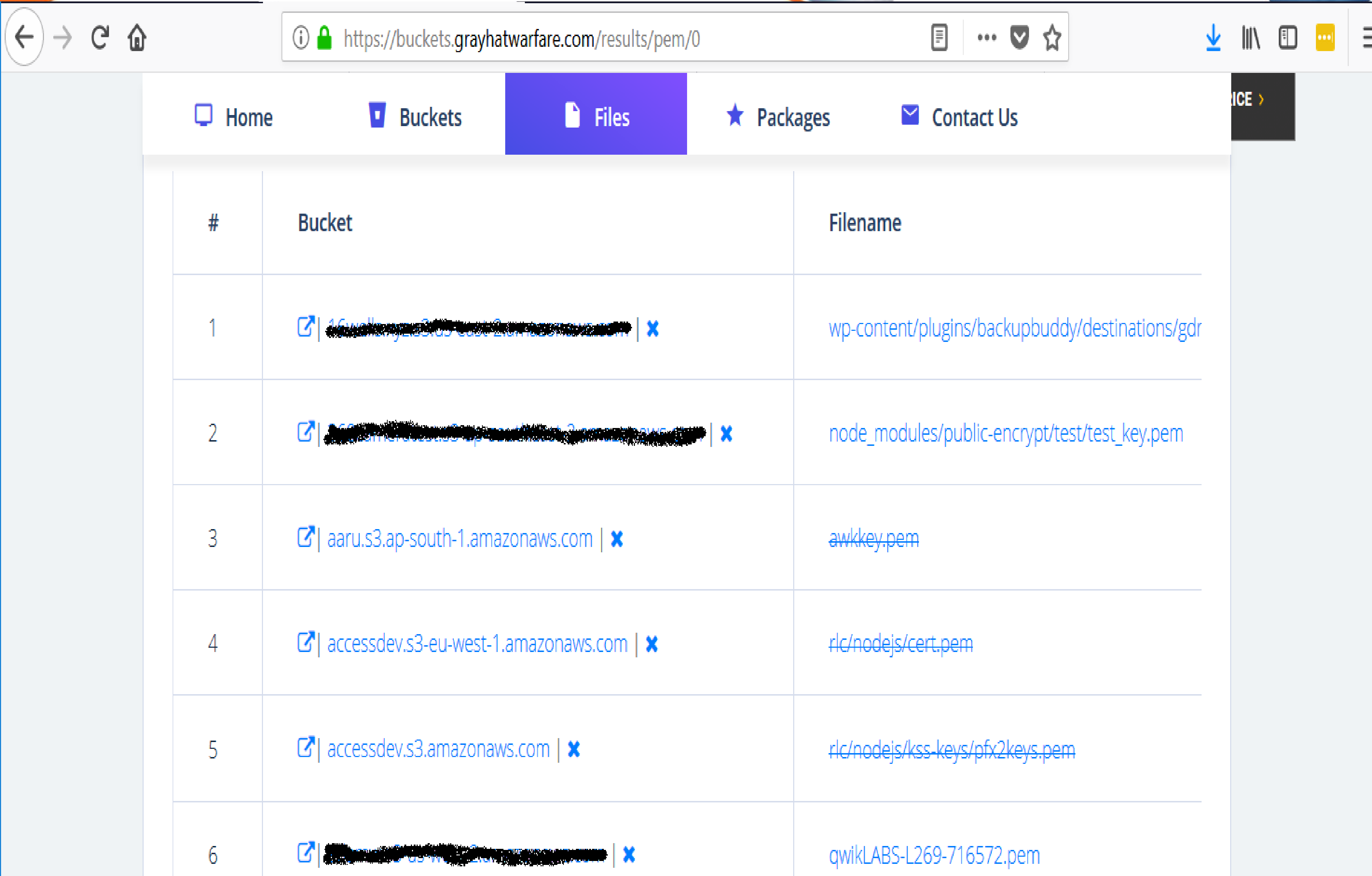
By Alison DeNisco Rayome | May 15, 2018, 6:27 AM PST

TechRepublic.

Cloud security remains a major issue for many companies, as more than half of organizations publicly exposed at least one cloud storage service in the last year, according to a Tuesday report (https://info.redlock.io/cloud-security-trends-may2018) from RedLock.

A number of enterprises using Amazon Web Services (AWS) S3 Simple Cloud Storage Service—including Dow Jones (https://www.techrepublic.com/article/massive-amazon-s3-breaches-highlight-blind-spots-in-enterprise-race-to-the-cloud/), Verizon (http://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html), FedEx (https://www.techrepublic.com/article/leaked-fedex-customer-data-was-stored-on-amazon-s3-server-with-no-password/), and Tesla (https://www.techrepublic.com/article/tesla-public-cloud-environment-hacked-attackers-accessed-non-public-company-data/)—experienced breaches in the past year. However, in most of these cases, AWS was not to blame. For example, at FedEx and Tesla, critical data was left exposed after unsecured AWS S3 storage servers were found without passwords protecting them.

- AWS S3 storage services are easy targets for cyber criminals.
- Dow Jones, Verizon, FedEx and Tesla all left critical data exposed on S3 storage services.



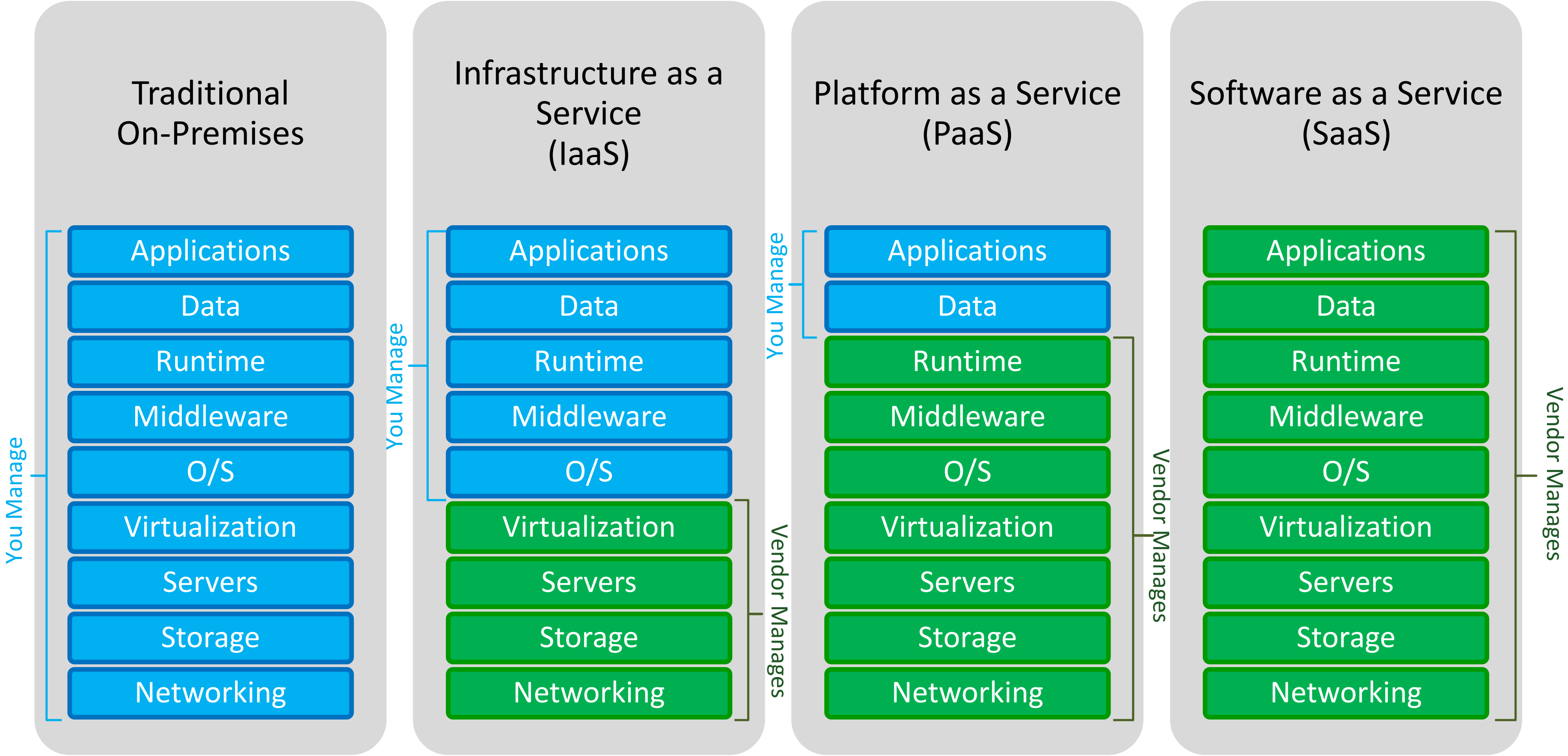
https://buckets.grayhatwarfare.com/results/pem/0

#	Bucket	Filename
1	[redacted]	wp-content/plugins/backupbuddy/destinations/gdr
2	[redacted]	node_modules/public-encrypt/test/test_key.pem
3	aaru.s3.ap-south-1.amazonaws.com	~~awkkey.pem~~
4	accessdev.s3-eu-west-1.amazonaws.com	~~rlc/nodejs/cert.pem~~
5	accessdev.s3.amazonaws.com	~~rlc/nodejs/kss-keys/pfx2keys.pem~~
6	[redacted]	qwikLABS-L269-716572.pem

Cloud Security Implications

- Limited Control and Visibility
- Multi-tenancy (shared environment)
- Multiple Management Interfaces
- Lack of Organizational Expertise
- Cloud based security requires a departure from traditional security models.

Cloud Service Responsibility Model



Traditional On-Premises

You Manage

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

Infrastructure as a Service (IaaS)

You Manage

Applications
Data
Runtime
Middleware
O/S

Vendor Manages

Virtualization
Servers
Storage
Networking

Platform as a Service (PaaS)

You Manage

Applications
Data

Vendor Manages

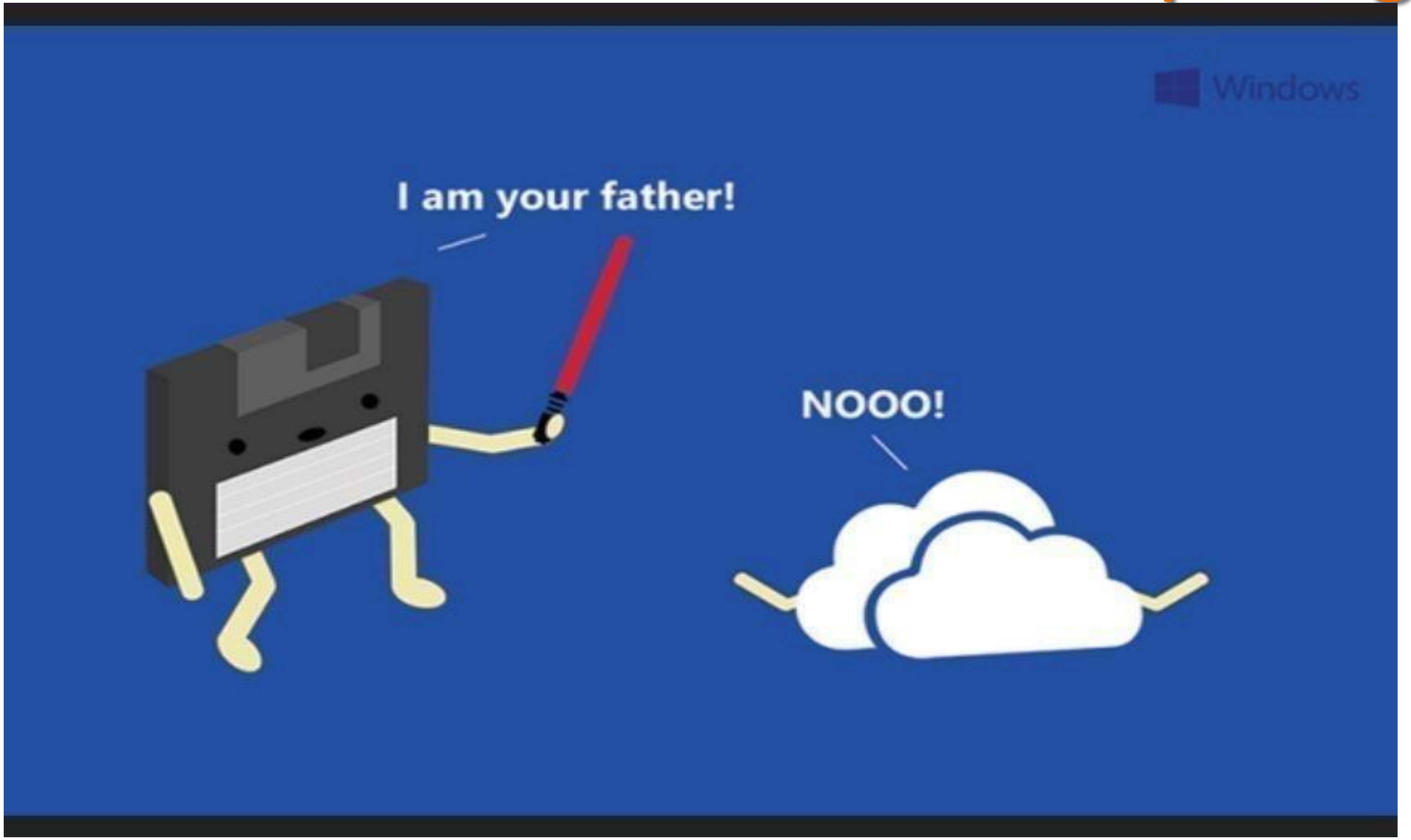
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

Software as a Service (SaaS)

Vendor Manages

Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

The "Dark Side" of Cloud Computing?



Identifying Implementation Challenges

Cloud Implementation Challenges

- Data Ownership and Accessibility
- Identity and Access Management
- Baseline Security Requirements
- Encryption & Key Management
- Perimeter Security
- Management Plane Restrictions
- Contractual Security Requirements

Data Ownership & Accessibility

- Data Ownership Concerns
  - Who owns what, where and how?
  - Multi-tenancy concerns?
- Defined conditions for data accessibility
  - For CSPs and MSPs
  - Post service considerations
- Data Center Requirements
  - Location
  - Physical Security

Identity & Access Management

- Management of credentials
  - Use of Multi-Factor Authentication
  - Role Segregation (privileged vs. non-privileged)
  - Credential Rotation
- API key management
  - Are your API keys embedded directly in code ☹
- Access permissions for resources (S3 buckets)

Baseline Security Requirements

- FedRAMP
  - Formally established in 2011
  - Requirements based on NIST 800-53
- Center for Internet Security (CIS)
  - CIS Controls and Benchmarks
- Cloud Security Alliance (CSA)
  - Security Guidance for Critical Areas of Focus in Cloud Computing (v4.0)
- NIST Cybersecurity Framework
- Others (SSAE 16 (SOC1/SOC2), HIPAA, PCI DSS, etc.)

FedRAMP
Federal Risk Authorization Management Program

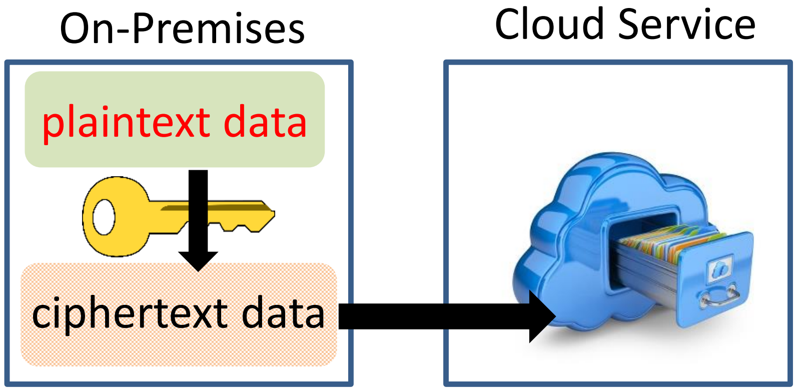
CIS™ Center for Internet Security®

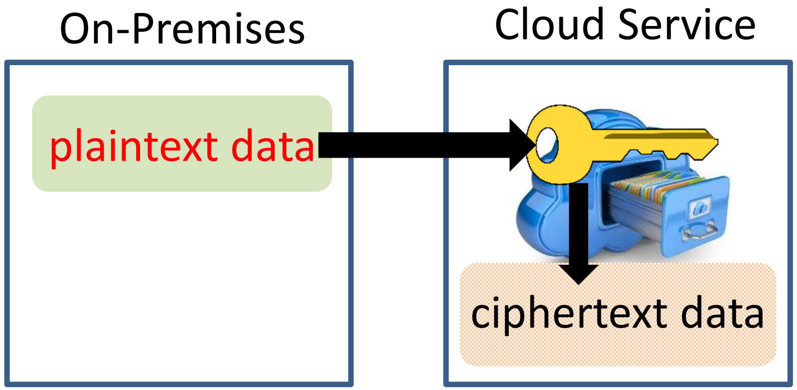
CSA cloud security alliance®

NIST CYBERSECURITY FRAMEWORK (CSF)
IDENTIFY PROTECT DETECT RESPOND RECOVER

Encryption & Key Management (1)

- Data in Transit Encryption (TLS, IPSec)
- Data at Rest Encryption
  - Client-Side
    - Data encrypted on-premises and transferred to cloud.
  - Server-Side
    - Data transferred to cloud and encrypted.





Encryption & Key Management (2)

- Data at Rest Encryption Considerations
  - Key Management Services (KMS)
    - Software-Based
    - Hardware-Based
    - Cloud-Based
  - Key Management Models
    - BYOK – customer supplies the encryption key
    - HYOK – provider leverages customer KMS
- Other Key Management Considerations
  - Protection of key pairs for cloud instance
  - Event driven key removal (compromised/lost keys)
  - Key rotation

Perimeter Security

- Traditional perimeter security or the "fortress concept" of cyber defense must be reconsidered.

- Ensuring security controls enforce effective network segmentation.
- Proper application of access controls within defined network security groups.
- Monitoring perimeter and "intracloud" network flow logs (ingress/egress traffic visibility)

Management Plane Restrictions

- Protection of management plane channels
  - SSH, SSL/TLS, IPSEC VPNs
  - Privileged Account Management
  - Multifactor Authentication

- Log Generation and Monitoring

Contractual Security Requirements

- Data Accessibility Requirements
- Data Destruction/Repatriation
- Incident Response/Breach Notification
- Indemnification Provisions
- Periodic Assessments and Continuous Monitoring

Key Security Enablers – General (1)

- Establish policy & governance for cloud computing (include provisions for DevOps)
- Adopt secure controls for cloud workloads based on categorization of data.
- Implement a secure configuration standard.
  - FedRAMP
  - CIS Controls/Benchmarks
  - CSA Controls Matrix

Key Security Enablers – General (2)

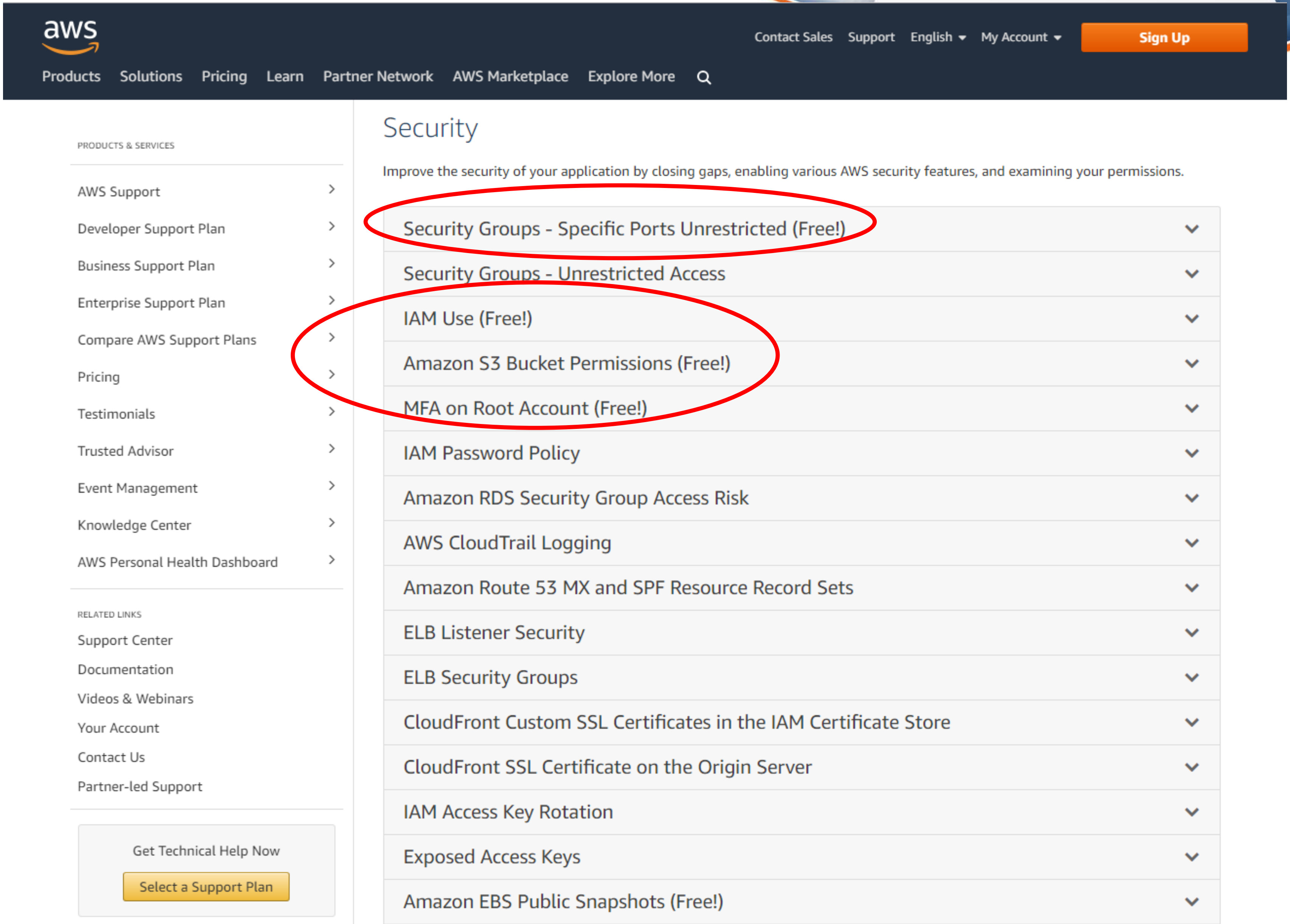
- Clearly define access roles for all cloud resources.
- Regularly monitor all user activity within the management plane.
- Ensure proper contractual requirements are established and understood.
- Ensure system/network diagrams are maintained for all cloud workloads.

Key Security Enablers – Technical (1)

- Enable logging on cloud resources (ex. AWS CloudTrail, O365 Audit Reporting Tool, etc.)
- Require multifactor authentication for privileged accounts and restrict access to the management plane.
- Ensure perimeter access security groups are configured with limited ports/protocols.
- Encrypt sensitive data repositories (e.g. PII)

Key Security Enablers – Technical (2)

- Rotate encryption and access keys regularly.
- Monitor and restrict creation of API keys (e.g. do not use AWS root account to create API keys).
- Enable access/object permissions on cloud based data resources
- Leverage CSP Free Security Tools!



Security

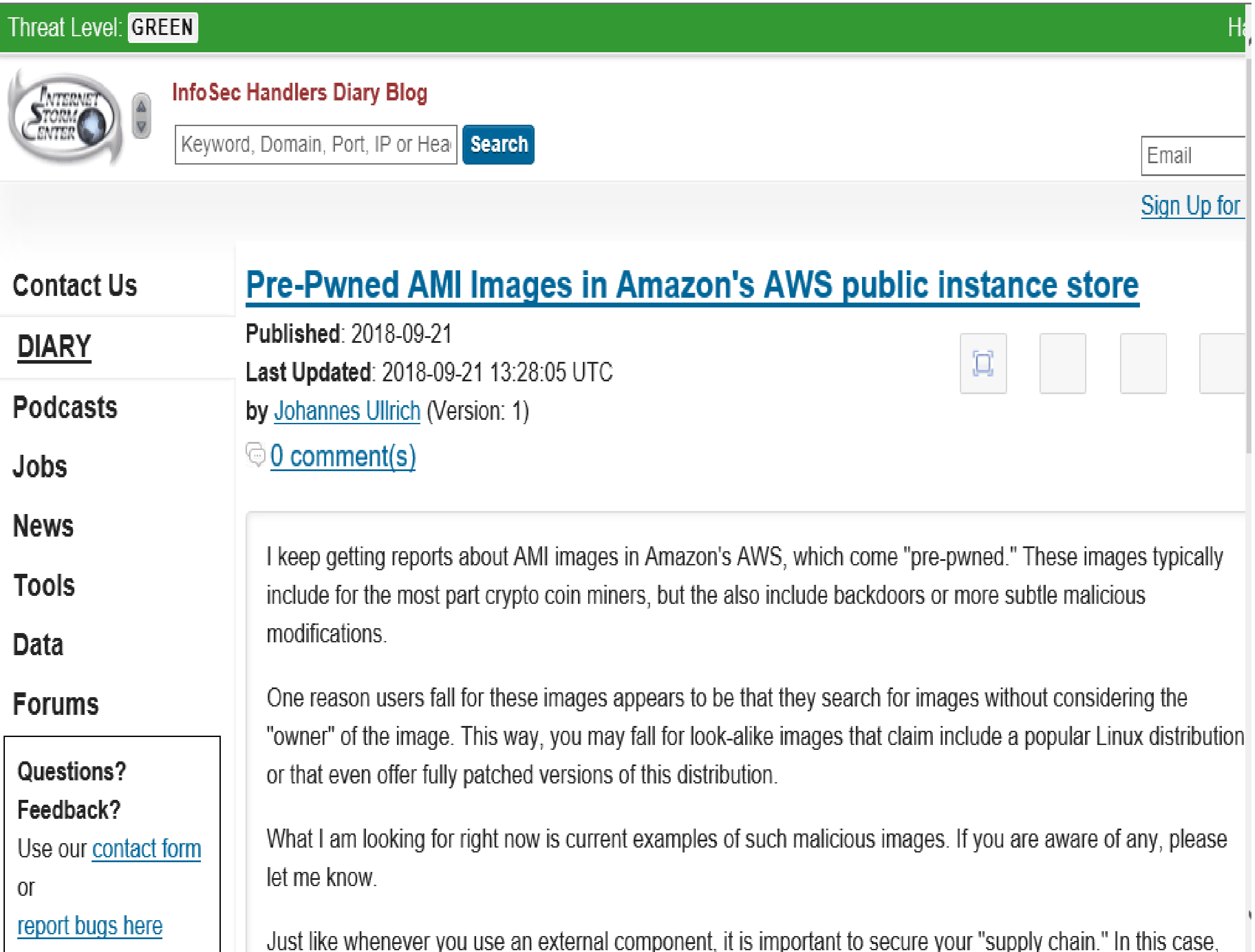
Improve the security of your application by closing gaps, enabling various AWS security features, and examining your permissions.

- Security Groups - Specific Ports Unrestricted (Free!)
- Security Groups - Unrestricted Access
- IAM Use (Free!)
- Amazon S3 Bucket Permissions (Free!)
- MFA on Root Account (Free!)
- IAM Password Policy
- Amazon RDS Security Group Access Risk
- AWS CloudTrail Logging
- Amazon Route 53 MX and SPF Resource Record Sets
- ELB Listener Security
- ELB Security Groups
- CloudFront Custom SSL Certificates in the IAM Certificate Store
- CloudFront SSL Certificate on the Origin Server
- IAM Access Key Rotation
- Exposed Access Keys
- Amazon EBS Public Snapshots (Free!)

Other Recommendations

- Evaluate security of Cloud Service Provider prior to signing contracts/production use.
- Leverage CASB services where applicable.
- Incorporate SLAs into your contracts with a right to terminate service.
- Verify integrity of marketplace instances!!!

Cloud Marketplace Integrity



Questions? Feedback?

Use our contact form or report bugs here

Pre-Pwned AMI Images in Amazon's AWS public instance store

Published: 2018-09-21
Last Updated: 2018-09-21 13:28:05 UTC
by Johannes Ullrich (Version: 1)

0 comment(s)

I keep getting reports about AMI images in Amazon's AWS, which come "pre-pwned." These images typically include for the most part crypto coin miners, but the also include backdoors or more subtle malicious modifications.

One reason users fall for these images appears to be that they search for images without considering the "owner" of the image. This way, you may fall for look-alike images that claim include a popular Linux distribution or that even offer fully patched versions of this distribution.

What I am looking for right now is current examples of such malicious images. If you are aware of any, please let me know.

Just like whenever you use an external component, it is important to secure your "supply chain." In this case,

- Reports about AMI images in AWS, that are "pre-pwned”.
- Buyer beware look-alike images that claim to come "pre-patched" often contain crypto coin-miners and backdoors.

Important Resources

- Center for Internet Security (CIS) Controls & Benchmarks

  https://www.cisecurity.org/controls/ https://www.cisecurity.org/cis-benchmarks/

- Cloud Security Alliance (CSA) - Security Guidance for Critical Areas of Focus in Cloud Computing (v4.0)

  https://cloudsecurityalliance.org/group/security-guidance/

- PCI SSC Cloud Computing Guidelines

  https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

- AWS Security Checklist

  https://pages.awscloud.com/Field_LN_NAMER_MTTC-Solutions-Campaign_2018.Migrating-to-the-cloud.html

- ISC^2 2018 Cloud Security Report

  https://www.isc2.org/Resource-Center/Reports/Cloud-Security-Report

amazon web services
Office 365
IBM Cloud
Dropbox
rackspace
ORACLE
Google Cloud Platform
Microsoft Azure
SAP Analytics Cloud
vmware vCloud

Questions