RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

CHANGE
Challenge today's security thinking

SESSION ID: CIN-W07

Logically Securing a Public Cloud Service

Tim Mather

CISO
Cadence Design Systems
@mather_tim

Disclaimer:

AWS (Amazon Web Services) is referenced in this presentation extensively, only because it is the largest IaaS (Infrastructure-as-a-Service) CSP (cloud service provider). AWS is by no means the only IaaS CSP, nor do the repeated references to AWS imply an endorsement. However, they are the largest IaaS CSP by far (14x the size of their nearest competitor), and have the most sophisticated security capabilities (in the humble professional assessment of your presenter).

Additionally, mention of specific 3rd party vendors does not imply a specific endorsement. Mention of thee vendors is intended to present specific, credible information only.

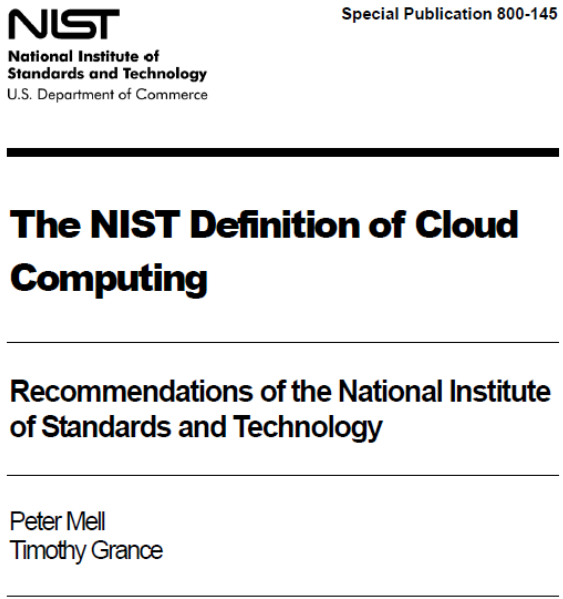
Batch mode = boring

Interactive mode = interesting

cadence™

A formal definition of cloud computing – from NIST

- NIST SP 800-145, The NIST Definition of Cloud Computing
  - NIST: (U.S.) National Institute of Standards & Technology, part of the Department of Commerce
  - SP: Special Publication
  - Published in September 2011


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

Essential characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Physical separation of data:

Multi-tenancy is important:

- Multi-tenancy at all levels:
  - Physical facility
  - Physical servers (virtual machines)
  - Application instances (unlike ASPs)

- With multi-tenancy at all levels, **all data separation is now *logical*; data separation is no longer physical**
  - This has important security ramifications
  - Data tagging is now required to enforce data separation

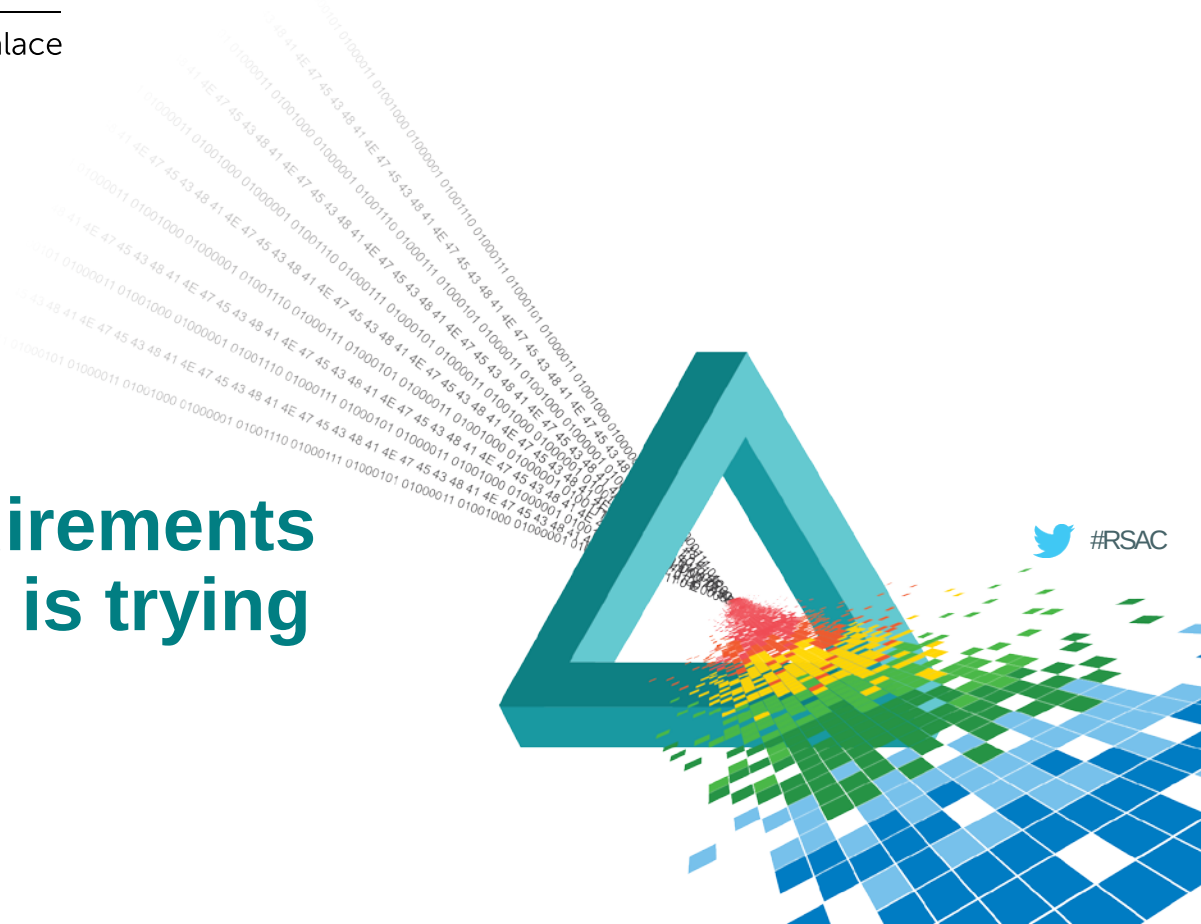
Agenda

- What are the requirements your organization is trying to meet?
- What does your cloud service provider (CSP) actually provide?
- What should you be doing to supplement those CSP efforts?

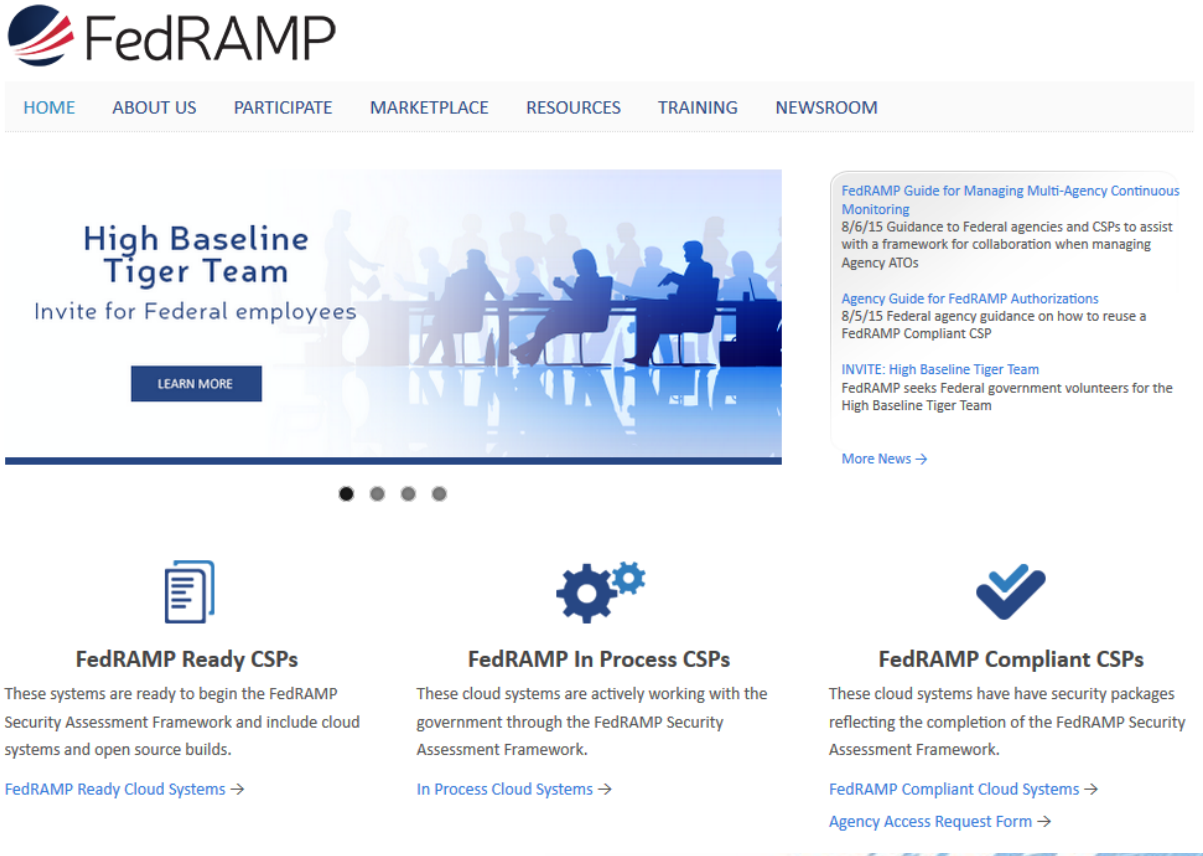
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

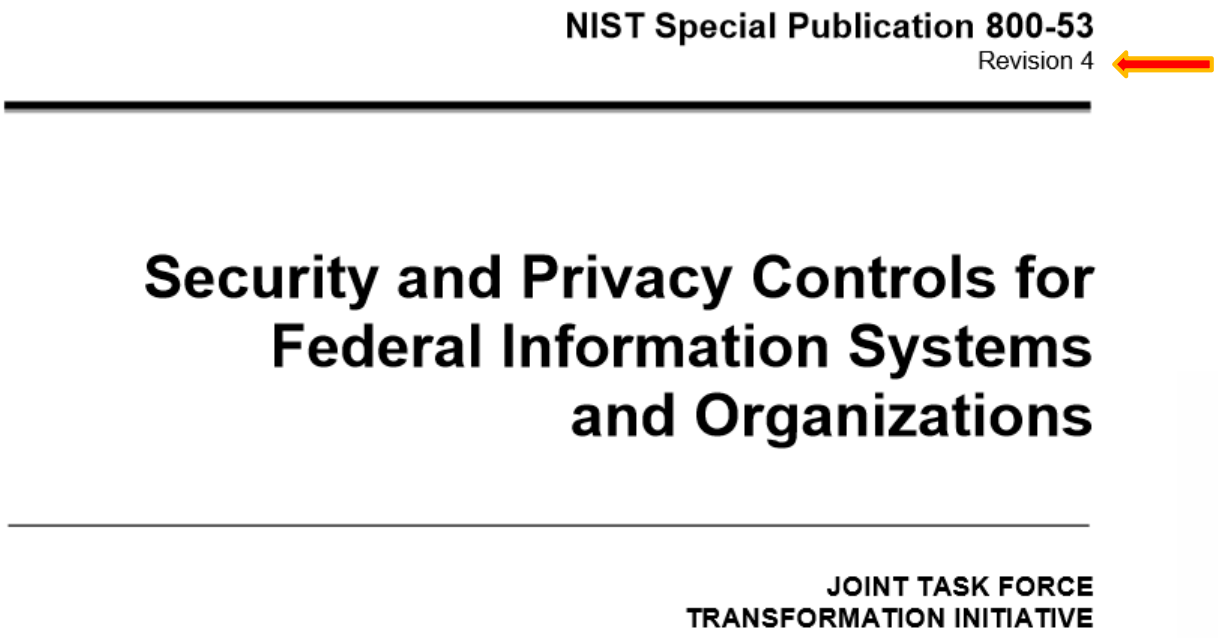
What are the requirements your organization is trying to meet?



What does the U.S. Government say?



FedRAMP is based on NIST SP 800-53R4



("Only" 462 pages long; "brevity" by U.S. Government standards)

Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM)

What is the CSA CCM?

CSA CCM is the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM)

CCM is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance.

CSA CCM is vendor agnostic 

reference: https://cloudsecurityalliance.org/research/ccm/

CSA CCM

133 controls in 16 domains

AIS Application & Interface Security	HRS Human Resources Security
AAC Audit Assurance & Compliance	IAM Identity & Access Management
BCR Business Continuity Mgmt & Op Resilience	IVS Infrastructure & Virtualization
CCC Change Control & Configuration Management	IPY Interoperability & Portability
DSI Data Security & Information Lifecycle Mgmt	MOS Mobile Security
DSC Datacenter Security	SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
EKM Encryption & Key Management	STA Supply Chain Mgmt, Transparency & Accountability
GRM Governance & Risk Management	TVM Threat & Vulnerability Management

cloud security alliance®

cadence™

CSA CCM Maps to Other Regulations

- CObIT
- ENISA Cloud Information Assurance Framework
- FedRAMP (NIST SP 800-53 R4)
- FISMA (NIST SP 800-53 R3)
- HIPAA / HITECH
- ISO / IEC 27001
- ITAR
- PCI DSS
- others

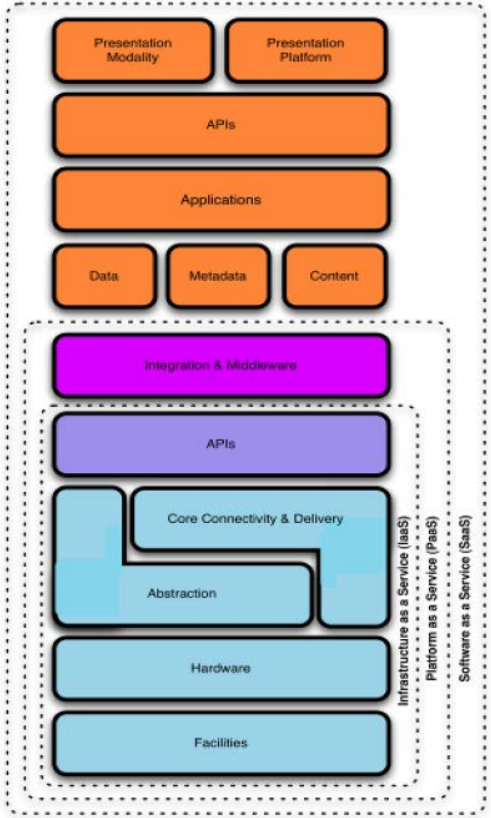
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

What does your cloud service provider (CSP) actually provide?

#RSAC

Shared security model:



This “eye chart” can be found on page #15 of the CSA (Cloud Security Alliance) “Security Guidance for Critical Areas of Focus in Cloud Computing v3.0”.

The CSP alone is *not* responsible for cloud security:

AWS Shared Responsibility Model

When evaluating the security of a cloud solution, it is important for customers to understand and distinguish between:

- Security measures that the cloud service provider (AWS) implements and operates – "security of the cloud"
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – "security in the cloud"

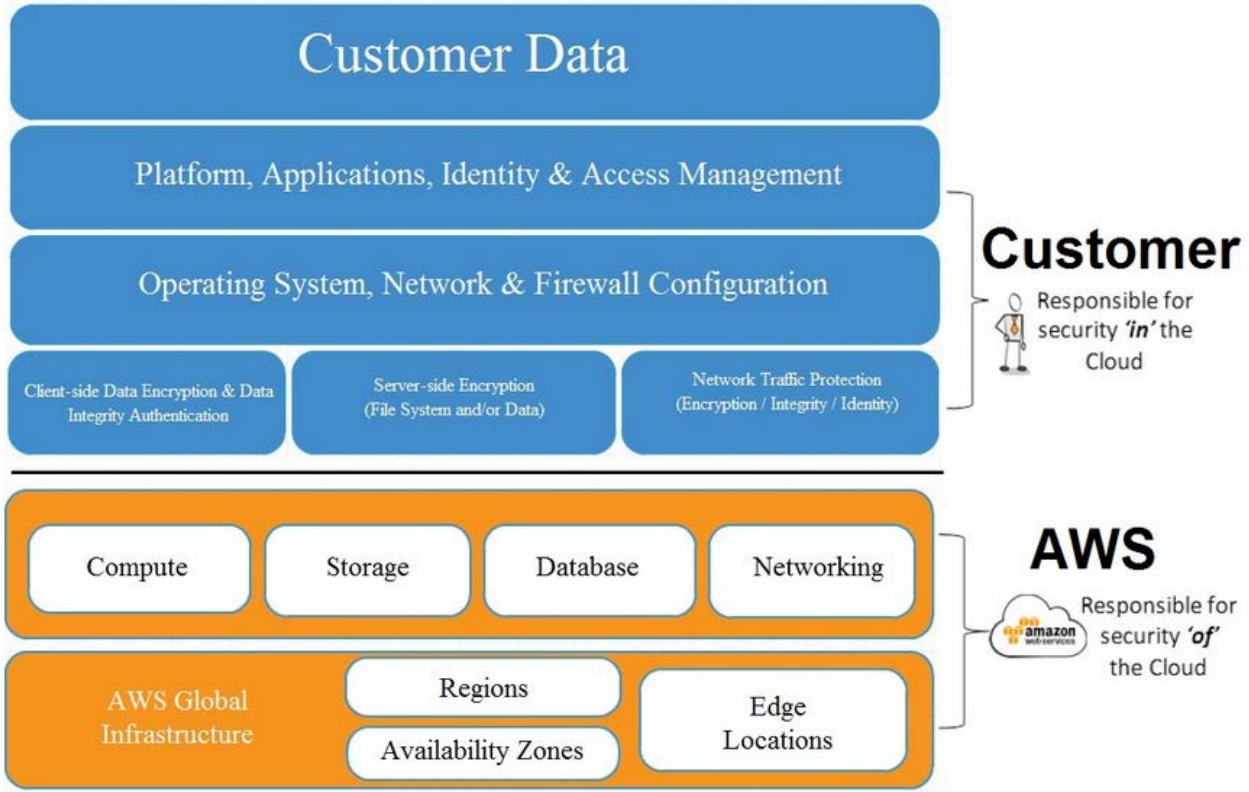
Video: AWS Compliance Shared Responsibility Model

While AWS manages security **of** the cloud, security **in** the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter.

Shared Responsibility Model Chart:

cadence™

What does that model look like – according to (IaaS) AWS:



Your manager should at least read:

Introduction to AWS Security

July 2015

https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
(It's all of seven (7) pages long.)

As an InfoSec professional, you should be interested in the more complete version:

Amazon Web Services: Overview of Security Processes

August 2015

https://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
(This version is 68 pages long.)

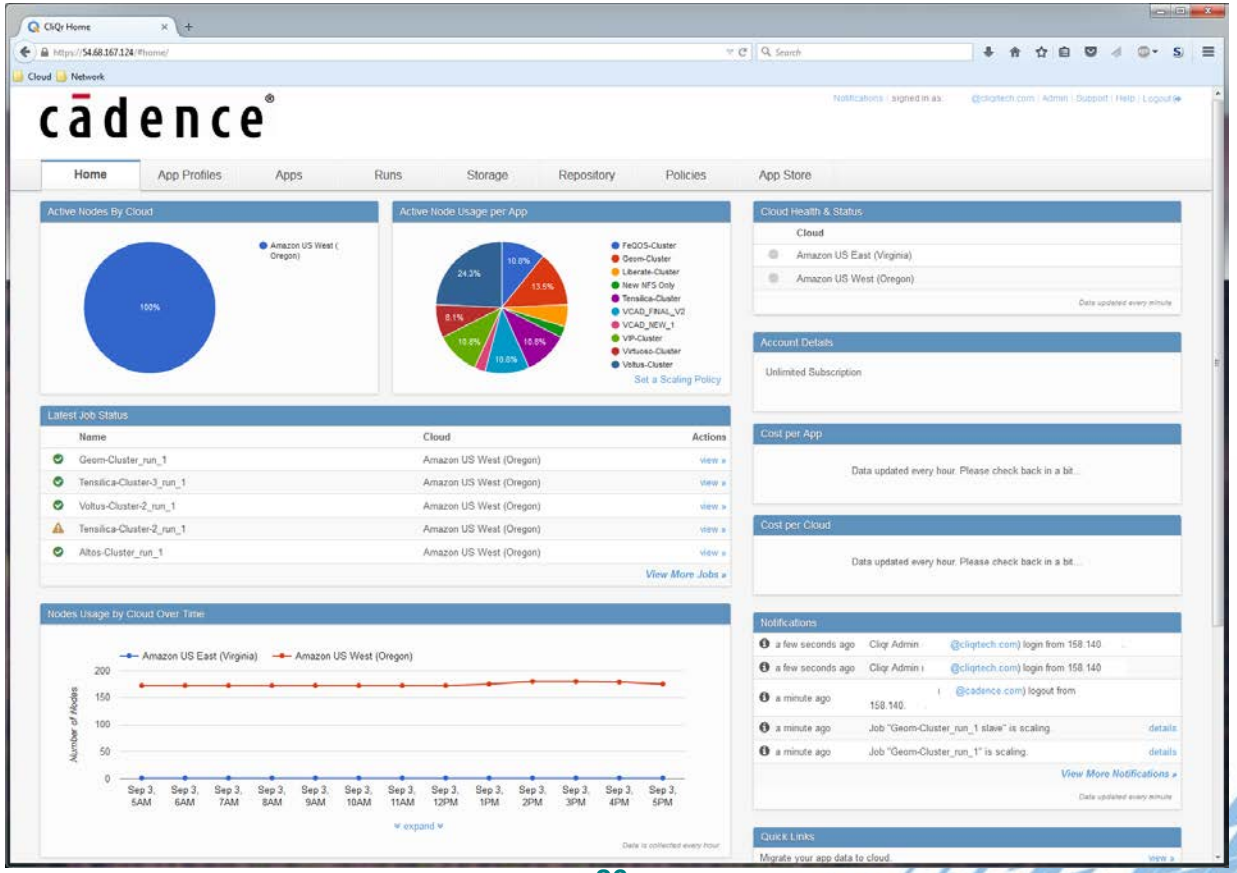
As explained by AWS in this video:

Or, watch this video:

AWS documentation:
http://aws.amazon.com/compliance/

What should you be doing to supplement those CSP efforts?

To begin with, an orchestration platform:



On AWS, for security, start with:

Upgrade to Business-Level Support to Access Trusted Advisor

AWS Trusted Advisor is available to customers with Business-level or Enterprise-level support. To access your Trusted Advisor report, **upgrade** your support subscription.

In addition to Trusted Advisor, here are some of the benefits of Business-level support:

- Communication with engineers by phone or online chat
- Response to web cases within 1 hour
- Live screen sharing
- Third-party software support
- IAM control of user access to support
- Availability of infrastructure event management

For more information about support features and pricing, visit the AWS Support page.

Trusted Advisor @ re:Invent 2013

https://aws.amazon.com/premiumsupport/trustedadvisor/

For security on Force.com, be sure to use:

Force.com Security Source Scanner Help

Introduction

The Force.com Security Source Scanner is a cloud based source code analysis tool built directly into our Force.com offering. Salesforce.com has made it available to developers, for free, as a high value addition, which will help to enable our community to build trusted applications.

Code is scanned based on a queuing system in which smaller scans receive priority over larger scans.

Requirements

In order for the scan to be successfully processed, the following must be true:

- The organization must contain less than 500,000 lines of code (excluding static resources and packages which are not scanned)
- You must have access to the email address associated to the username provided
- You must have metadata api enabled for the organization
- The account with username provided must have the "Author Apex" permission enabled.
- Code must not be contained within a package that has been installed in the org being tested. Source code that lives inside of managed or unmanaged packages is not scanned to avoid inadvertently scanning code unrelated to your application.
- Each organization must wait for the results of all pending jobs to complete before submitting another job.
- Each user must comply with the throttling rules: no more than 3 scans per security review and no more than 30,000 lines of code scanned per month

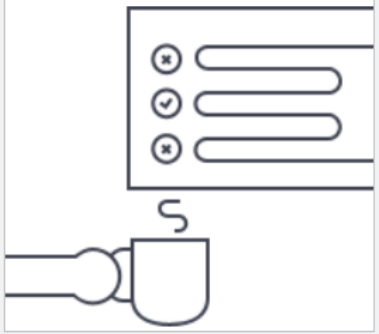
http://security.force.com/security/tools/forcecom/scannerhelp

Not home grown; it's actually CHECKMARX:

Integrated Part of The Software Development Life Cycle

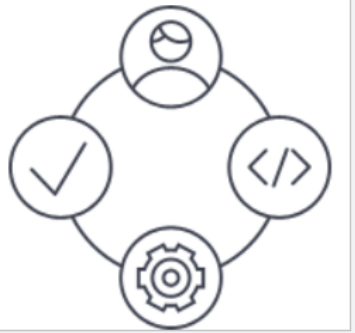
Scan your uncompiled source code and detect application-layer vulnerabilities early in the SDLC to speed up the remediation process.

Easy to Use



Scan & Fix Early

Full SDLC Integration



Accurate Results

cadence

Back on AWS, do a free 14 day trial of:

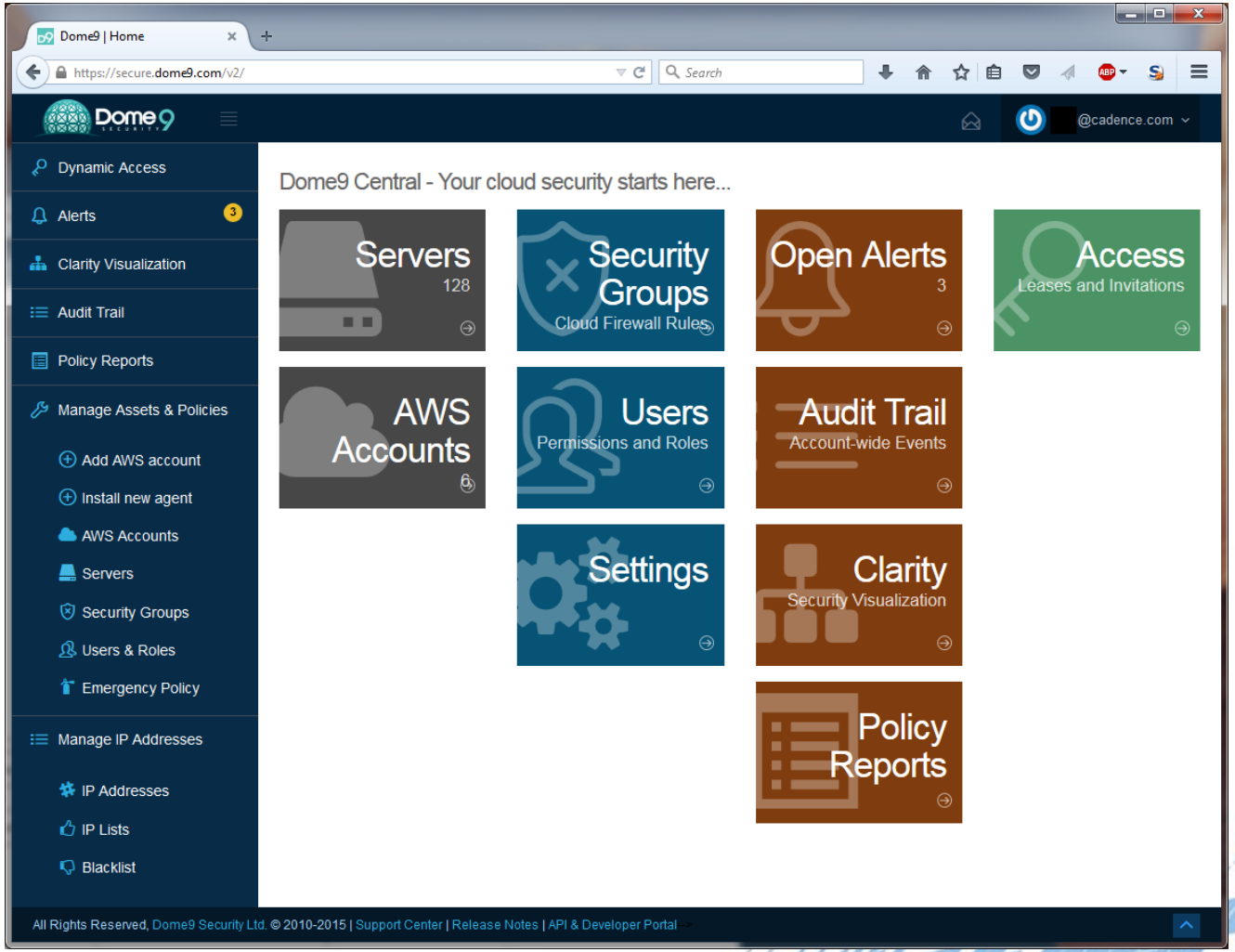
Why do you even need a 3rd party tool? (Something about a “reduced attack surface”?)

GmailFS

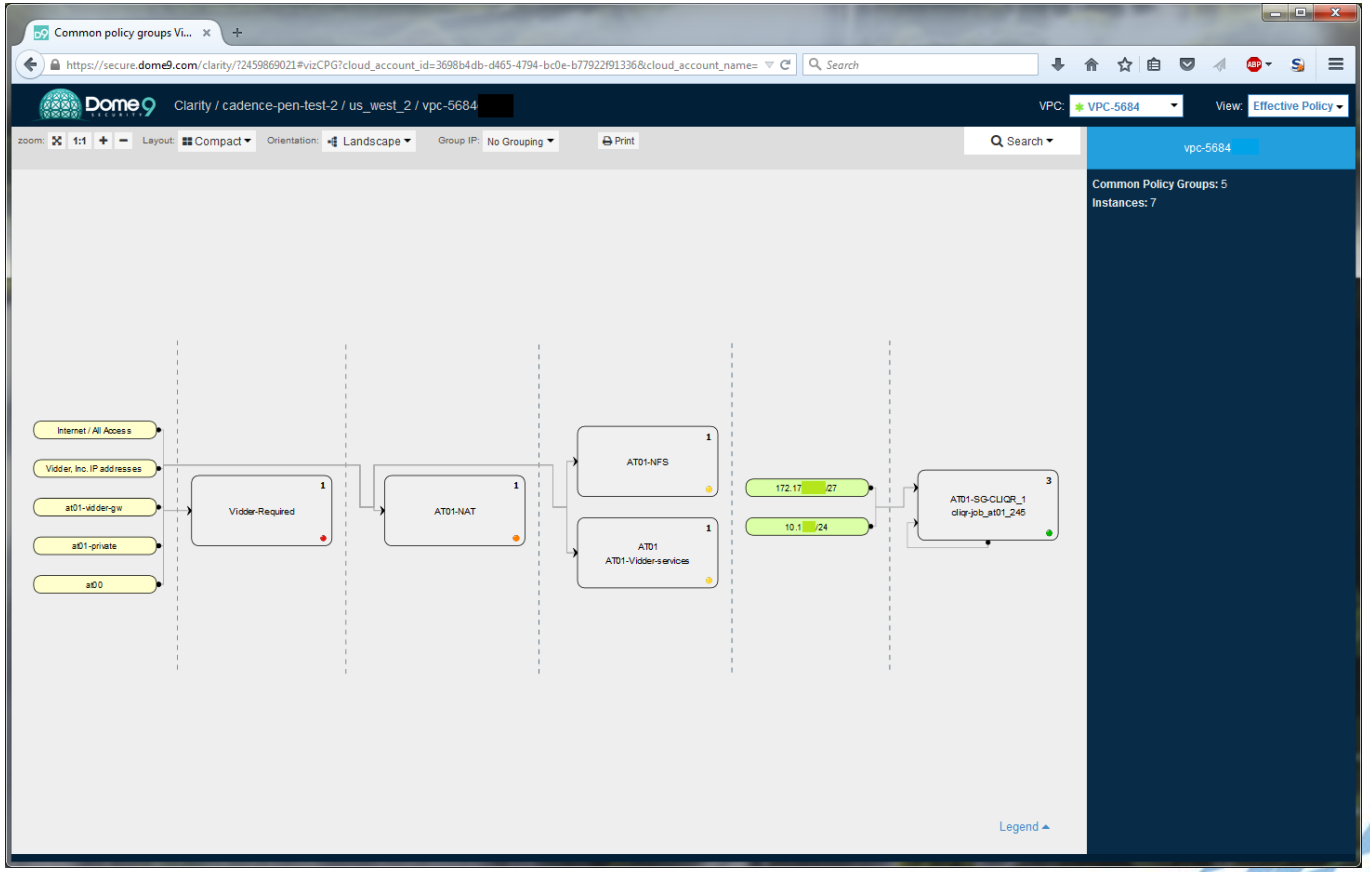
Dropship

Remember: EC2 *alone* has 148 APIs

Dome9



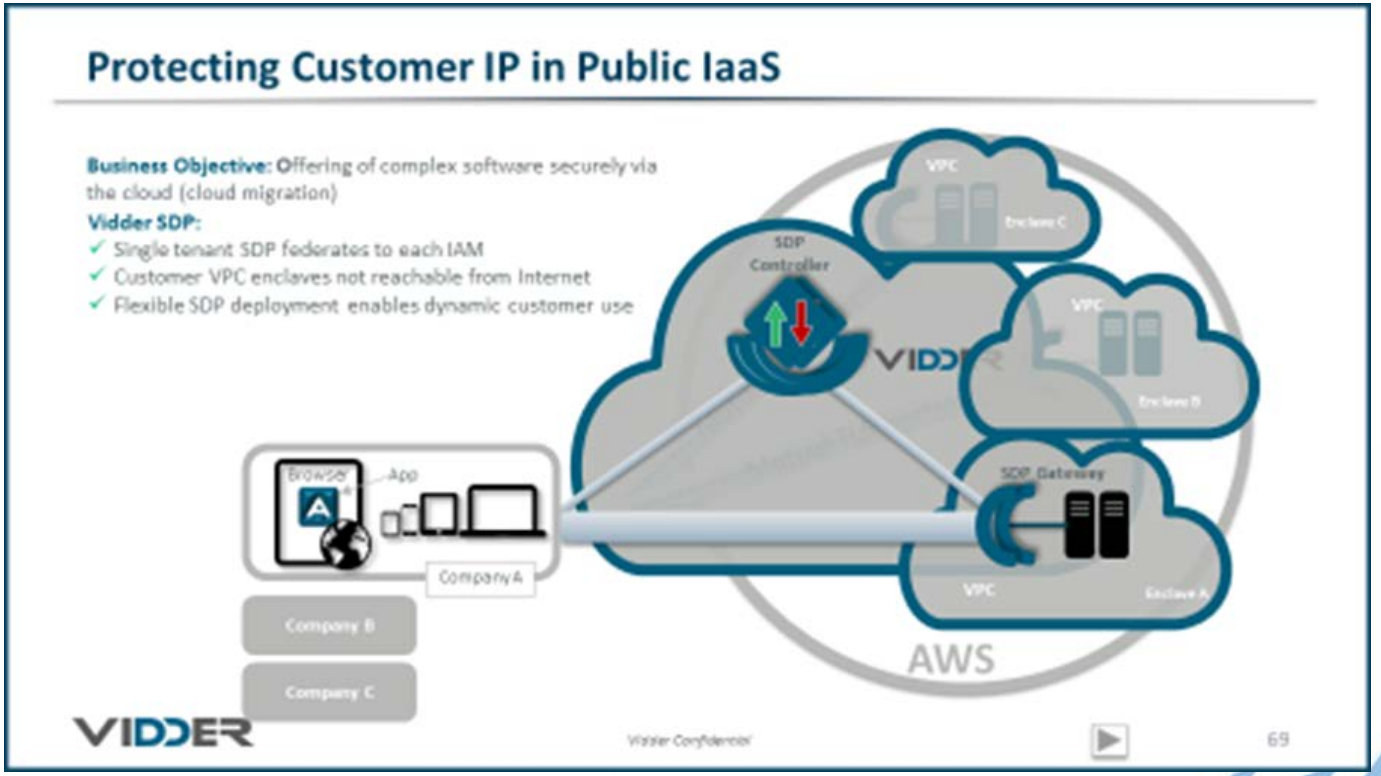
Dome9



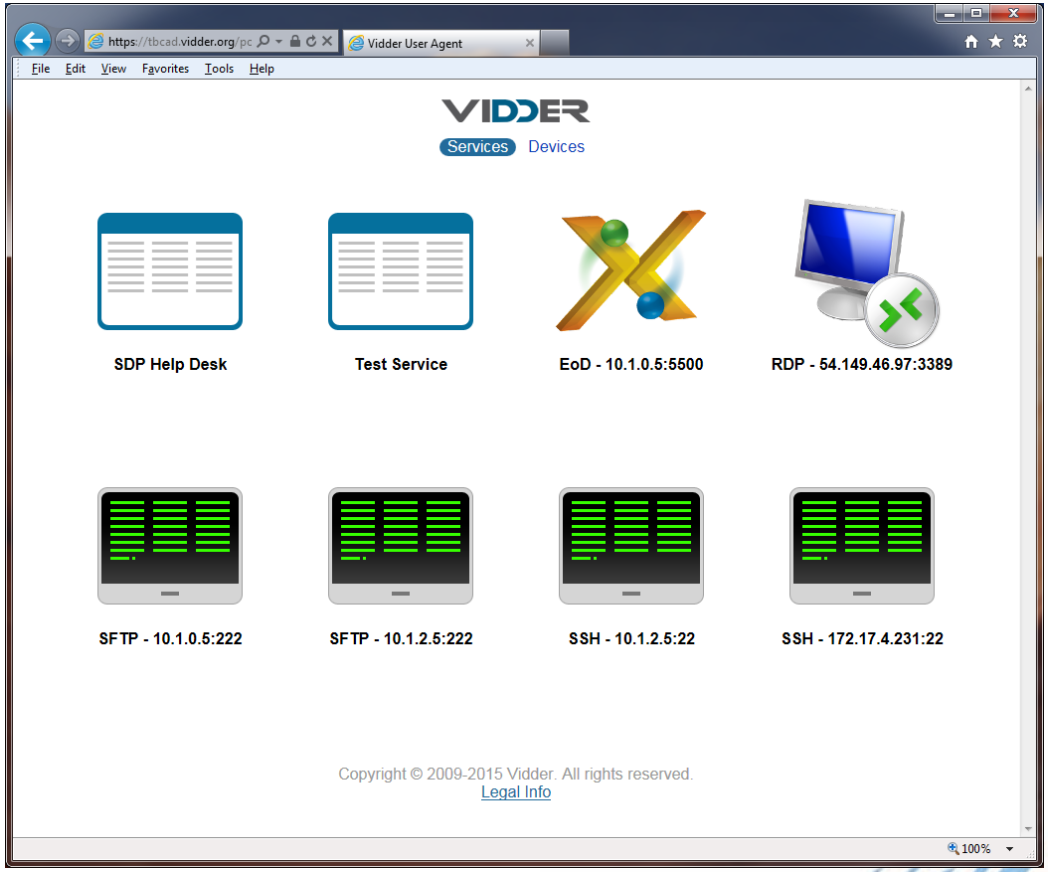
cadence™

RSA Conference 2015
Abu Dhabi

Software Defined Perimeter (SDP) architecture



SDP in use

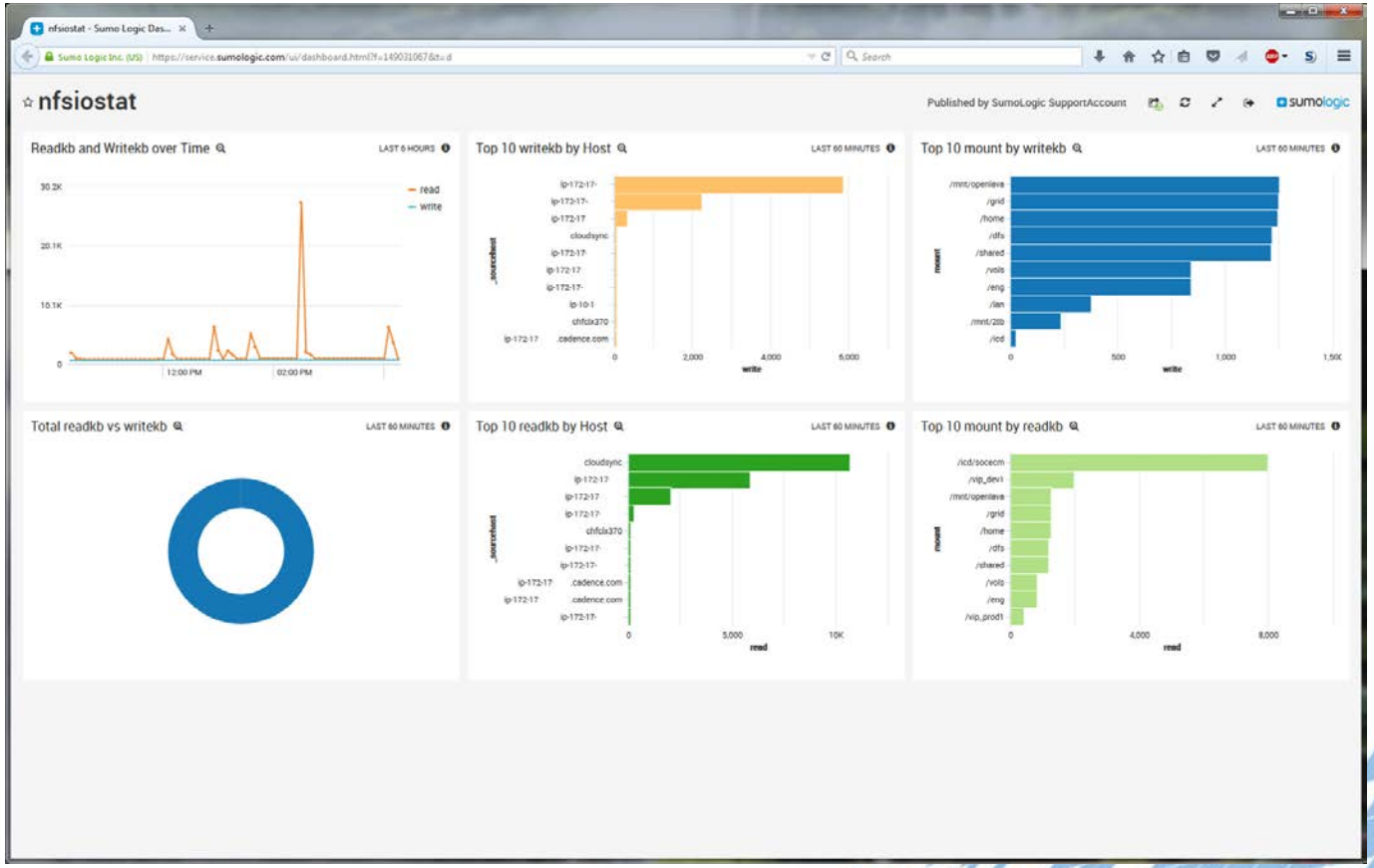

https://tbcad.vidder.org/pc
Vidder User Agent
File Edit View Favorites Tools Help
VIDDER
Services Devices
SDP Help Desk
Test Service
EoD - 10.1.0.5:5500
RDP - 54.149.46.97:3389
SFTP - 10.1.0.5:222
SFTP - 10.1.2.5:222
SSH - 10.1.2.5:22
SSH - 172.17.4.231:22
Copyright © 2009-2015 Vidder. All rights reserved.
Legal Info
100%

Sumo Logic

Sumo Logic is an enterprise cloud-based log management and analytics service.

Sumo Logic not only provides a secure (digitally signed) audit trail of system and user actions, but also provides operational and security analytics.

Secure logging, event correlation



But wait – there's more: "auditing"

Bugcrowd was founded in 2012 by CEO Casey Ellis and CTO Chris Raethke to help level the vulnerability assessment playing field. By leveraging the economic, expertise, and sheer numbers of the crowd, the company is redefining the cybersecurity market.

Apply what you've learned!

- Determine what security requirements you need to meet:
  - FedRAMP?
  - CSA CCM?
  - Other?
- Determine what security your CSP commits to providing:
  - Probably only availability in the SLA
  - What about confidentiality and integrity? Ask!
    - Most likely, confidentiality and integrity are your customer responsibility. So what tools are you going to use for such?
  - What free or included security tools or capabilities does your CSP provide? Use them!

Apply what you've learned!

- Do **not** *assume* that your CSP provided services are secure as is!
- Now, there are many cloud security tools available to improve CSP offerings. Match your security requirements against CSP capabilities, then how CSP capabilities can be supplemented with 3rd party tools to meet your security requirements.
- How do you ensure that the CSP is actually meeting what it says it is doing? Tools are available to help you with that to.
- Factor the costs of such tools into your cloud budget – not just the CSP's charges!

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you for attending!

#RSAC

Provide an "Apply" Slide – Part 1

Complete the "equation" for attendees:

Educate + Learn = Apply

- Your Role as Instructor
- Attendee Role as Student
- How to Apply this in the office = Critical to justify attendance

Every presentation must contain an Apply slide!

Provide an "Apply" Slide – Part 2

- Sessions focused primarily on people, process and technology issues (e.g., Data Security & Privacy, GRC, Identity, etc. sessions), should provide:
  - 1 – 2 specific immediate actions for attendees to take as a result of your session (e.g., issues to identify in their own environment, other individuals to collaborate with, etc.)
  - 2 – 5 specific actions that attendees could implement within 3 months of returning to the office
  - NOTE: all can include specific considerations necessary (e.g., type of OS, type of network topology, specific protocols impacted, organizational structure, processes, etc.) to implement specific actions

Provide an "Apply" Slide – Part 2 continued…

- Sessions focused primarily on potential threats (e.g., Hackers & Threats sessions), should provide:
  - Specific information about the threat(s) that attendees can use to validate their organization's exposure to the threat(s) discussed
  - Specific remediation actions for the threat(s) discussed

Provide an “Apply” Slide – Example:

Apply What You Have Learned Today

- Next week you should:
  - Identify critical database(s) within your organization
- In the first three months following this presentation you should:
  - Understand who is accessing the database(s), from where and why
  - Define appropriate controls for the database
- Within six months you should:
  - Select a security system which allows proactive policy to be set according to your organization’s needs
  - Drive an implementation project to protect all critical databases