

The Current and Future State of Cloud Security, Risk and Privacy

Jay Heiser

@GARTNER_INC

This presentation, including any supporting materials, is owned by Gartner, Inc. and/or its affiliates and is for the sole use of the intended Gartner audience or other authorized recipients. This presentation may contain information that is confidential, proprietary or otherwise legally protected, and it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.
© 2011 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner[®]

Gartner at a Glance



The Current and Future State of Cloud Security, Risk and Privacy

Jay Heiser

Security Breaches in the Cloud Are Rare

- Sony: 12 breaches impact 100,000,000 gamers?
- Epsilon email: 50 corporate customers?
- GoGrid: leaks customer lists and credit cards
- Gmail: Chinese dissident email context leaks
- NASDAQ OMX DirectorsDesk:
 - 300+ Corporate Boards possibly compromised
- Distribute.IT: 4000 web sites disappear
- HyperVM software hacked: 1000+ web sites gone

If a cloud leaked and nobody was aware of it, would it still be a breach?

Prominent Data Disappearance Incidents

- Aug. 2008: The LinkUp business fails after losing customer data
- Feb. 2009: Onsite3 files for bankruptcy
- March 2009: 7,000 Carbonite customers lose their backups
- July 2010: 6,327 Evernote customers permanently lose data.
- Feb. 2011: 35,000 Gmail accounts lose all data
 - Four days required to restore .02% of Gmail user base
- Apr 2011: Amazon ECs multiday outage; some loss of data
- Oct 2011: SaaS provider Mumboe provides 2-week warning before shutdown
- Jan 2012: DOJ Shutdown of Megaupload results in petabytes of lost data
- June 2012: FirstServer (Japan) 6,000 customers permanently lose data

Get Your Cloud Risks in the Proper Order!

1. Loss of data or service availability
 - Live upgrade causes widespread data corruption
 - Vendor ceases to operate
 - Technology failure
2. Control over form and status of vital application
 - Changes (wanted and unwanted)
 - Integration support
 - Migration and end-of-life cost
3. Regulatory violation
4. Loss of confidentiality

Cloud Computing turns software into a supply chain.

Gartner®

The Public Cloud Risk Gap

A blurred red and white train is passing a man in a suit waiting at a subway platform. The man is standing with his back to the camera, looking at a mobile device. The platform has a tiled floor and a curved wall. The train is moving quickly, creating a motion blur effect.

Incomplete Cloud Service Offerings

- Few security SLAs
- Minimal transparency

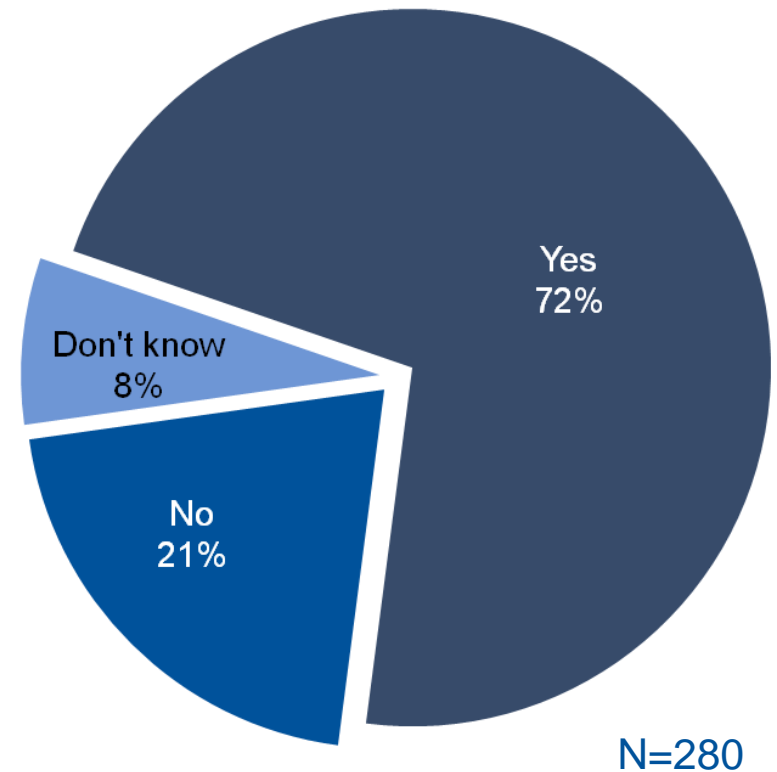
Inadequate Customer Requirements Definition

- Incomplete Data and Process Classification
- Unrecognized needs

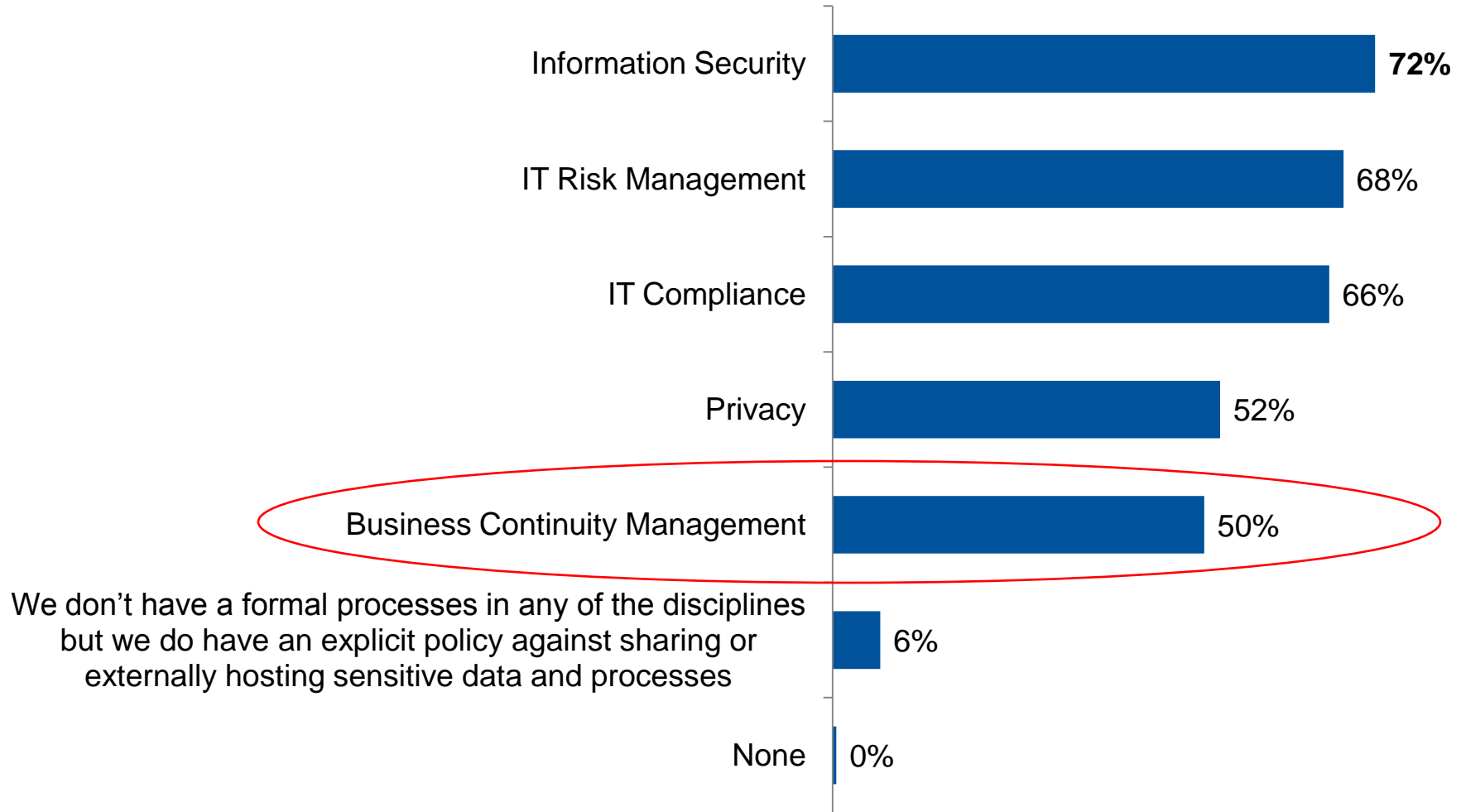
Standards & Certifications Are Still Weak

- AICPA
 - SOC 1 (SSAE 16) generic assessment replacing SAS 70
 - SOC 2 = SysTrust, addressing specific security risks
 - SOC 3 = SysTrust that you are allowed to use for marketing purposes
- Cloud Security Alliance
 - Reaching critical mass?
 - Many initiatives, questionable depth
- FedRAMP (operational 2014)
 - Control Standards complete
 - Still at experimental stage
- ISO/IEC 27017
 - Under development

Now that SAS 70 has been replaced by SOC 1, will you also require a SOC 2 audit from any of your service providers?



Latest Survey Results: Process in Place to Evaluate Provider Risk?



N=425

Major Findings From Three Years of Assessment Practices Survey Data

- Organizations of all sizes are increasingly willing to place their data externally
- They are increasingly likely to have formalized processes for the assessment of the associated risk.
- A questionnaire based primarily on published standard is the most common risk evaluation mechanism.
- Only half of organizations have a formal process in place for the assessment of external provider business continuity management programs.

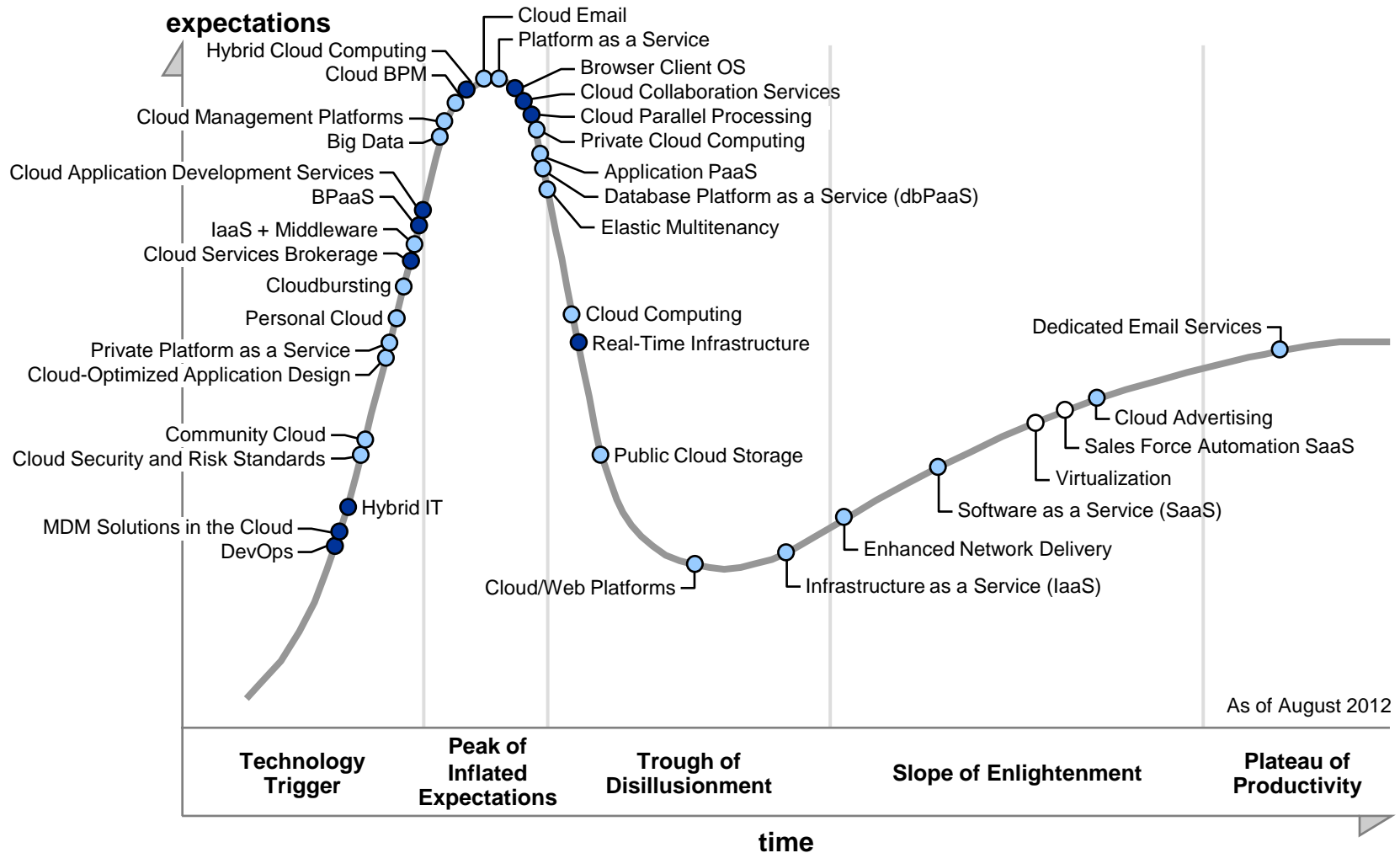
Today's Cloud Contracts Are Incomplete

Feature	Effectiveness	How common?
Downtime credits	Partial	Often
Disaster recovery	High, but difficult to verify	Not contract clauses
Evals: SOC1, SOC2?, 27001	Believed insufficient	Common
Internal controls reporting	Useful	Sometimes
Full indemnification for security failure impact	Theoretically high	Never
Hacking insurance	May cover cleanup cost	Rare, but growing
Customer audits on demand	Partial	Sometimes
Negotiate security clauses	No consensus on SLAs	Large customers
Vendor financial health reports	High	Sometimes
Data deletion certificate	Legally defensible	Not seen in the wild
Data return at contract end	High	Sometimes

SaaS Controls Primitive, but Improving

- Data continuity and recovery: usually available
 - Do not assume data is backed up offline
- IAM mechanisms
 - Federation and strong authentication often possible
 - Limited ability to use enterprise authorization and roles
 - Personal devices complicate SaaS authentication architecture
- Encryption on server or through gateway: sometimes available
 - How do you manage and securely store encryption keys?
- Logging, e-discovery, forensics: primitive
 - Logging getting better
 - E-discovery explicitly supported by some services
 - Ad-hoc forensics virtually impossible (no data or customer access)
- Activity monitoring and alerting: rarely available
 - Early DLP experiments, no database activity monitoring

Hype Cycle for Cloud Security, 2012



Plateau will be reached in:

○ less than 2 years

● 2 to 5 years

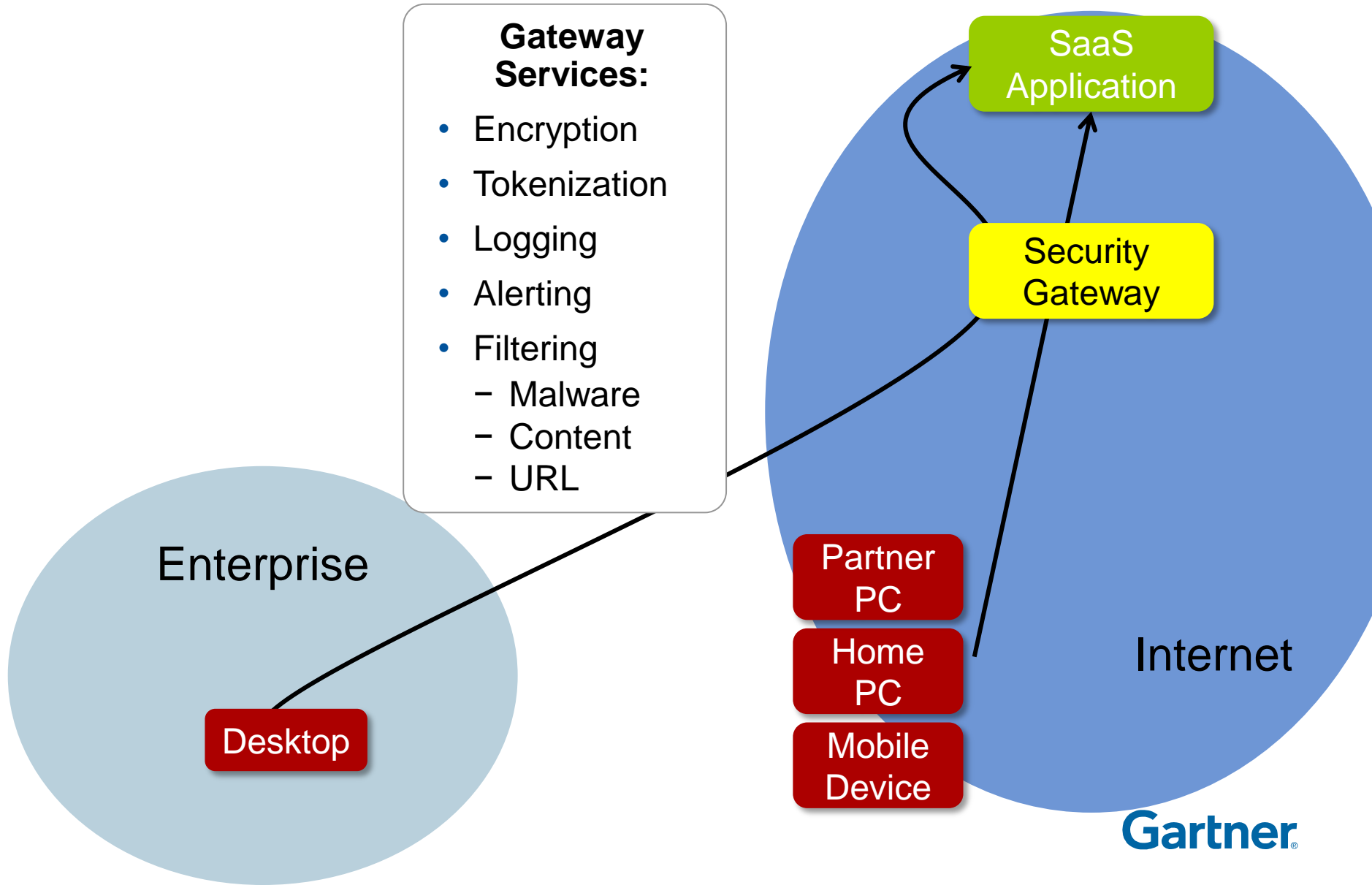
● 5 to 10 years

▲ more than 10 years

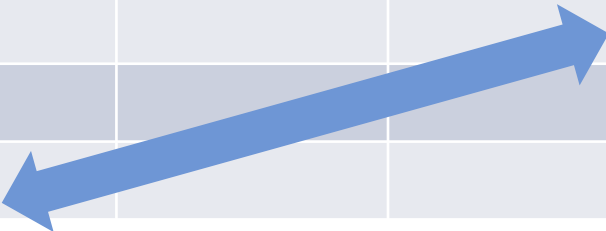
obsolete

⊗ before plateau

Gateway Controls: Modular and Practical



More Choices for Encryption at Rest

Key Manager	Where Applied				Most Secure
	None	Server	Gateway	End Point	
Individual	NA				
Enterprise					
Vendor					

Least Expensive

- Server encryption significantly complicates search
- The more parties that share a key, the bigger the risk
- Loss of key means loss of data

Choose Your Battles Over Data Control

- Changing conditions; cloud is just one factor
 - More data than ever, often ends up on end point
 - More leakage paths, including personal devices
 - Less control: their application, someone else's device
- Most data will have to protect itself
 - Improve the baseline level of protection
 - Give up on fantasy of precise, granular classification
 - Heroic efforts only for highly critical data
 - Encryption and rights management
 - Document Tracking
 - DLP (content-based automatic control)

Recommendations

- ✓ Base purchases on business requirements
- ✓ Use standards for service party risk assessments
- ✓ Protect highly sensitive data with control technology as it becomes practical/available
- ✓ Always have a contingency plan for supplier failure
- ✓ Seek business ownership for the business' use of information and technology

Poll: Do you evaluate cloud service providers?

1. We avoid using cloud services for anything critical.
2. We make use of cloud services, but don't have a defined process for evaluating providers.
3. We have a defined process for evaluating provider security.
4. We have defined processes for evaluating provider security and data recovery capabilities.
5. We have a comprehensive set of defined processes for evaluating provider security, recoverability and business viability.

Poll: What standard do you primarily use for evaluating cloud service providers?

1. Criteria developed in house (less than 50% comes from a single published standard)
2. Cloud Security Alliance
3. Shared Assessments
4. ISO 2700X
5. Other

Recommended Gartner Research

- ➔ **Survey Analysis: Assessment Practices for Cloud, SaaS and Partner Risks, 2012**
Jay Heiser (G00233399)
- ➔ **Hype Cycle for Cloud Security, 2012**
Jay Heiser (G00230524)
- ➔ **U.S. FedRAMP Program Brings Cloud Service Guidance, but Obstacles Too**
John Pescatore (G00229016)
- ➔ **Toolkit: SaaS Contract Negotiation**
Alexa Bona and Deborah Wilson (G00228313)

Events for Security & Risk Professionals

Experience live analyst expertise plus much more at a Gartner event.

Gartner Identity & Access Management Summit 2012

December 3 – 5, Las Vegas, NV

Gartner Security & Risk Management Summit 2013

June 10 – 13, National Harbor, MD

Visit gartner.com/events

For full details by region,
visit: gartner.com/symposium

Gartner®
SYMPOSIUM ITXPO® 2012



UNITED STATES
OCTOBER 21 – 25



SPAIN
NOVEMBER 5 – 8



**UNITED ARAB
EMIRATES**
MARCH 5 – 7, 2013



JAPAN
OCTOBER 3 – 5

INDIA
OCTOBER 10 – 12



BRAZIL
OCTOBER 29 – 31



SOUTH AFRICA
AUGUST 28 – 30



AUSTRALIA
NOVEMBER 12 – 15

The World's Most Important Gathering of **CIOs and Senior IT Executives**

Simple steps for increasing the value of today's webinar experience

- Visit gartner.com/webinars
 - Today's presentation will be available in 24 hours
 - Check out the schedule of upcoming Gartner webinars (plus on-demand webinars) and don't forget to share these resources with your colleagues
- Contact your Gartner account executive with any additional questions, comments or for a complimentary copy of today's presentation