

State of Cloud Security 2012 - Spring

Summary of Findings



ALERTLOGIC

Security. Compliance. Cloud.

Industry First Data-Driven Comparative Analysis of Threats in Hosted and Cloud vs. On-Premise IT Environments

REMOVING THE CLOUD OF INSECURITY

State of Cloud Security Report

Spring 2012

Unrelated lower frequency of security categories, differences in the observed stage of used incidents environment.

Number of on-related impacted roughly instances found, 4.0 however, rise experienced incident of service providers did.

INCIDENTS BY CUSTOMER TYPE



found in **malware/spoof**. On-premise environments were overwhelmingly more likely to encounter such incidents in their environments when compared to service provider managed environments with 43% of on-premise environments versus 2% of service provider managed environments.

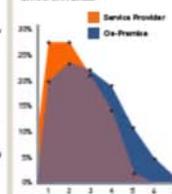
Both on-premise (71%) and service provider (85% customers are highly likely to have experienced **Web application attacks**, and impacted customers in both environments were likely to have experienced a high number of such attacks over the period of study (on-premise 44.3, service provider 32.4).

Brute force incidents are even more commonly experienced in an on-premise environment than Web application attacks, with 63% of customers receiving an average of 47.3 such attacks. While brute force incidents in the service provider realm are significant (44% of customers experienced them) the difference between the two environments is surprising. With more public-facing targets (websites) in the service provider environment, the reverse might have been expected.

Vulnerability scans are observed among 37% of service provider customers and 54% of on-premise customers.

Threat diversity is the third element that Alert Logic analyzed. While a lower threat diversity by itself does not mean an inherently less risky environment, a higher threat diversity indicates that a broader set of attack vectors are at play.

AVERAGE NUMBER OF THREAT CLASSES ENCOUNTERED



Alert Logic found lower threat diversity in service provider environments than in on-premise environments. During the period of this study, service provider customers averaged threats in 2.13 categories (out of the seven categories analyzed), while on-premise customers experienced 2.99.

less secure than on-premise environments, but this is simply not supported by Alert Logic data.

With so many organizations considering a move to the cloud, and making a service provider decision, it's important to address this concern. In this first in a series of twice-yearly reports analyzing security trends across on-premise and service provider environments, Alert Logic assessed the differences between the two, using its own extensive data from mission-critical business IT infrastructure environments.

Alert Logic analysis indicates that service provider environments tend to be less prone to a broad range of security incidents than the on-premise environments. Further, service provider environments tend to experience a narrower range of attack vectors. Possible explanations include the presence of more standardized system configurations in the service provider world, a narrower range of use cases among service provider customers and the relative maturity of the IaaS industry.

It's not that the cloud is inherently secure or insecure. It's really about the quality of management applied to any IT environment.

- NEIL MACDONALD, GARTNER FELLOW & VP

While this data certainly casts doubt on conventional wisdom and concerns about security in the service provider environment, Alert Logic does not believe that it leads to a simple "service provider vs. on-premise" conclusion. While we observed differences between the two environments, we believe that there are several factors that help explain these variances:

- The typical size of a customer/user in each environment
- The types of workloads found in each environment
- The diversity of each environment
- The presence of user endpoints in the on-premise environments

relationship between risk level and IT surface area in any environment.



FIG. 2 represents a conceptual framework for thinking about these differences. While service providers manage vast networks with tens of thousands of servers and applications, the relevant surface area a prospective buyer of IaaS solutions should consider is that of the individual customer environment. In Alert Logic's experience, those individual customer environments skew to a smaller and simpler footprint as measured by number of nodes and applications and breadth of operating systems. In contrast, on-premise environments managed by the typical enterprise span a much broader array of endpoints, applications and operating systems.

Service provider environments, with smaller deployments, inherently avoid some of that risk and therefore are a good choice for appropriate workloads.

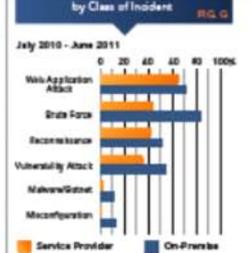
complex and involved security program to adequately protect assets.

ANALYSIS APPROACH

Analysis of these three factors shows that even in security conscious environments, virtually every environment will encounter meaningful threats. Further, service provider managed environments encountered more favorable results in all three of the criteria analyzed in this report. It should be noted that some of this could be explained by the differences in size and platform diversity of cloud vs. on-premise environments.

- The frequency of experienced incidents is higher for on-premise environments across most of the threat categories.
- The threat diversity for on-premise environments is greater than the threat diversity for service provider environments.

SECURITY INCIDENTS by Class of Incident



Methodology Overview

1500+ Customer Environments
12 Months of Threats
2.2 Billion Security Events

Expert System
+
Certified Analysts

62K Validated Security Incidents
7 Classes of Incidents

Risk Measurement

Prevalence
By Incident Class

Occurrence
How likely?

Frequency
How often?

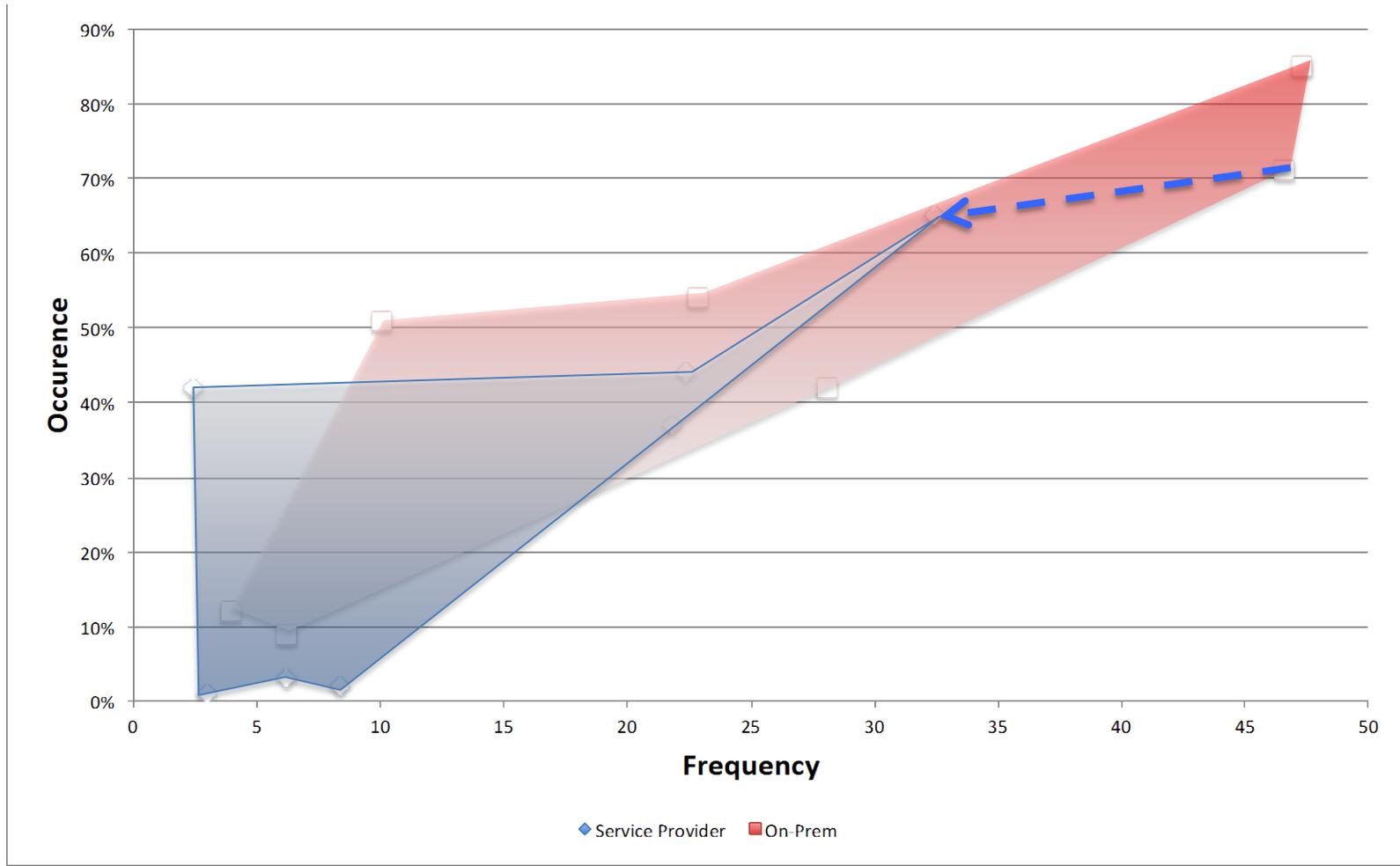
Diversity

How varied?

Data Collection



Delta in Prevalence



Prevalence & Diversity Gap

Prevalence Delta

Significant spread, but can largely be explained by IT footprint differences



Opportunity to improve risk posture through IaaS providers for Web apps

Though a smaller risk advantage, Misconfigurations are low hanging fruit to improve security posture

Threat Diversity Distribution

