Security and Compliance Powered by the Cloud

Ben Friedman / Strategic Accounts Director /
bf@alertlogic.com

ALERTLOGIC

ALERTLOGIC

Founded:	2002
Headquarters:	Houston, TX
Ownership:	Privately Held
Customers:	1,200 +
Employees:	100 +
Technology:	Patented

viawest

ALERTLOGIC

Security and Compliance Challenge

- IT organizations are faced with mounting pressure

1. Compliance regulations
   - PCI DSS, SOX, HIPAA, GLBA, NIST, FISMA, FERC
2. Continued evolution of network threats
   - Look what Microsoft did just in the last month?

Responsibility of securing data is settling nicely on your shoulders and has been for a while

ALERTLOGIC

The Facts

ALERTLOGIC

The Facts

- 81% of companies breached in 2009 were not compliant with their required regulation
- 6% of the breaches were caught through event monitoring and logging
- 99% of all breached records were from compromised servers and applications

* All percentages are from the 2009 Verizon Business Data Breach Investigation

ALERTLOGIC

2009 Data Breaches

Who is breaching data?	
73%	External Sources
18%	Inside Sources
39%	Business Partners
30%	Multiple Partners

How do breaches occur?	
62%	Significant Error
59%	Hacking
31%	Malicious Code
22%	Exploited Vulnerability
15%	Physical Threats

What Commonalities Exist	
66%	Victim was unaware data was on the system
75%	Breaches were not discovered by the victim
83%	Attacks were not highly difficult
85%	Breaches were the result of opportunistic attacks
87%	Were considered avoidable through reasonable controls

*Statistics from 2009 Verizon Business Data Breach Investigation Report

ALERTLOGIC

Analyzing the Facts

- Companies aren't detecting solutions in an effective way
  - Why? Chasing false alarms, other priorities, etc…
- Companies are not focusing on continuous security
  - Too many companies check a box and move on
- 6% success rate is too low!
  - Companies need to be more vigilant in this area
- Most of the 99% of breaches could have been caught
  - With effective log management and daily review of log data

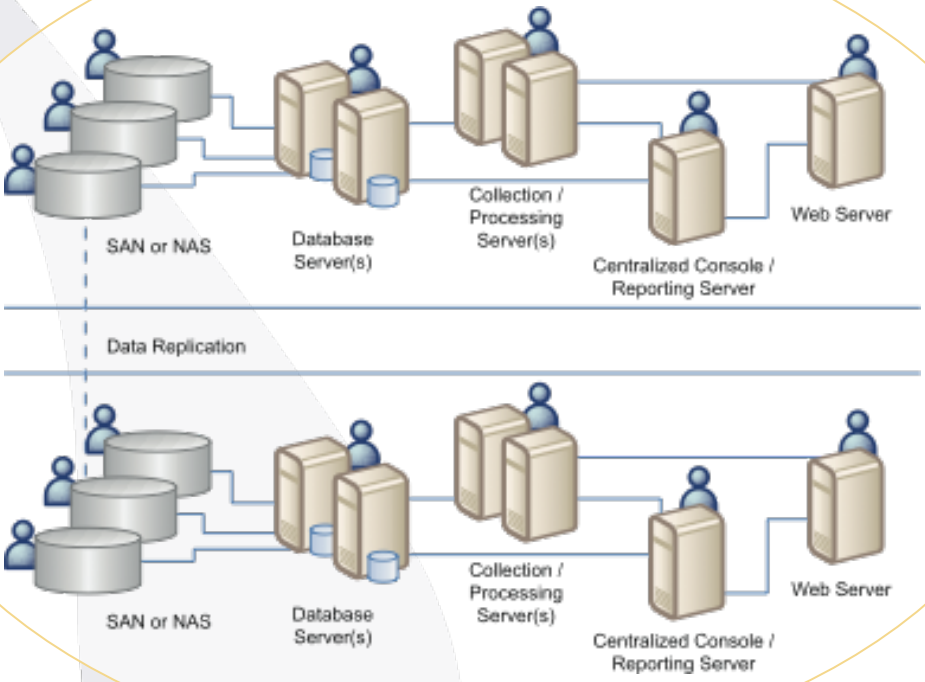
ALERTLOGIC

Cloud-Powered Security

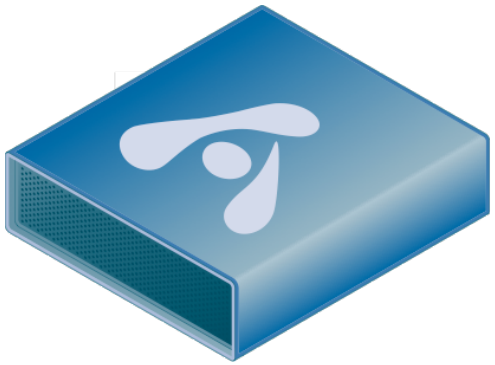
ALERTLOGIC

Traditional Deployment vs Cloud Model

Instead of Deploying This:

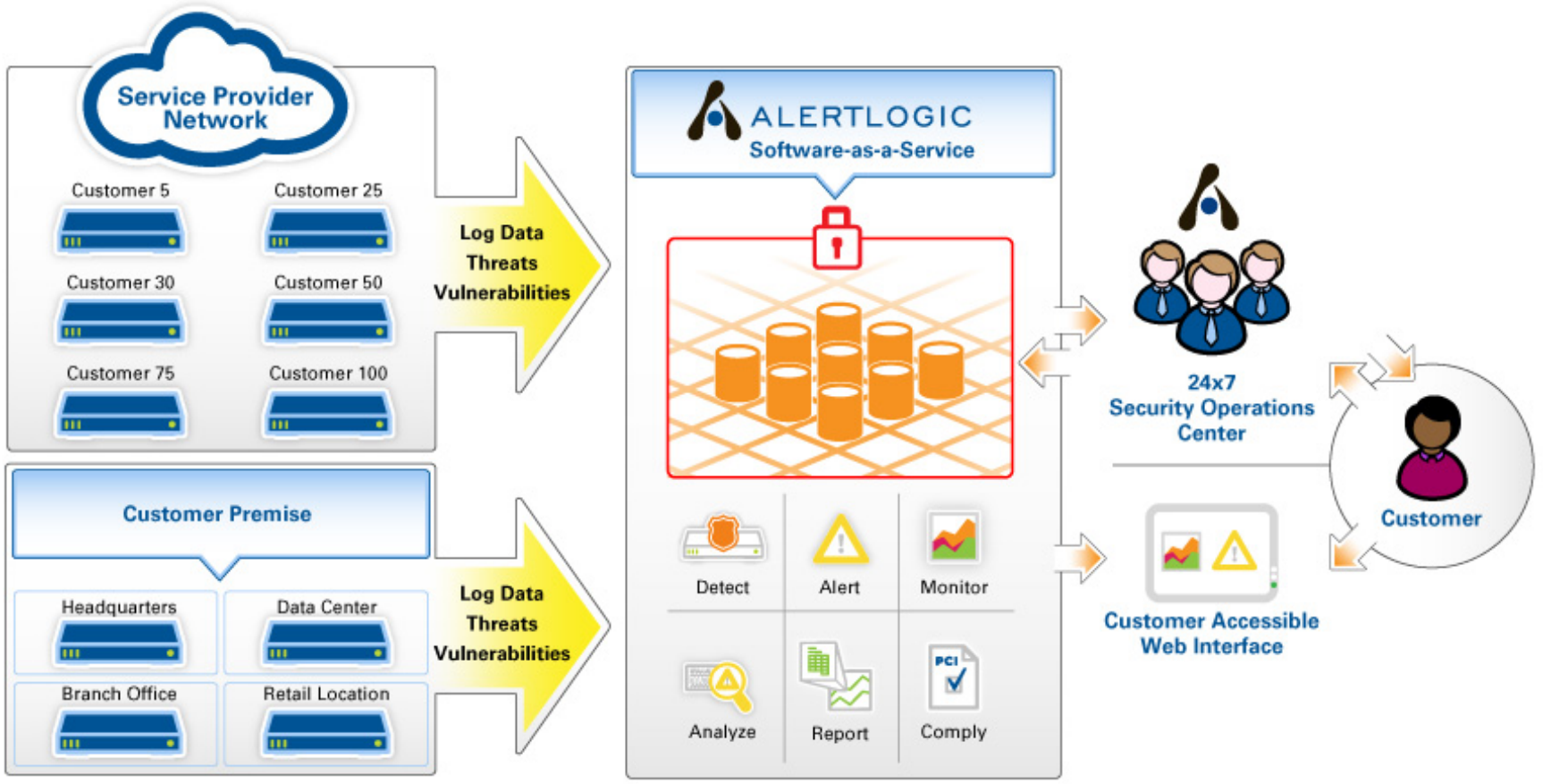


Deploy This:



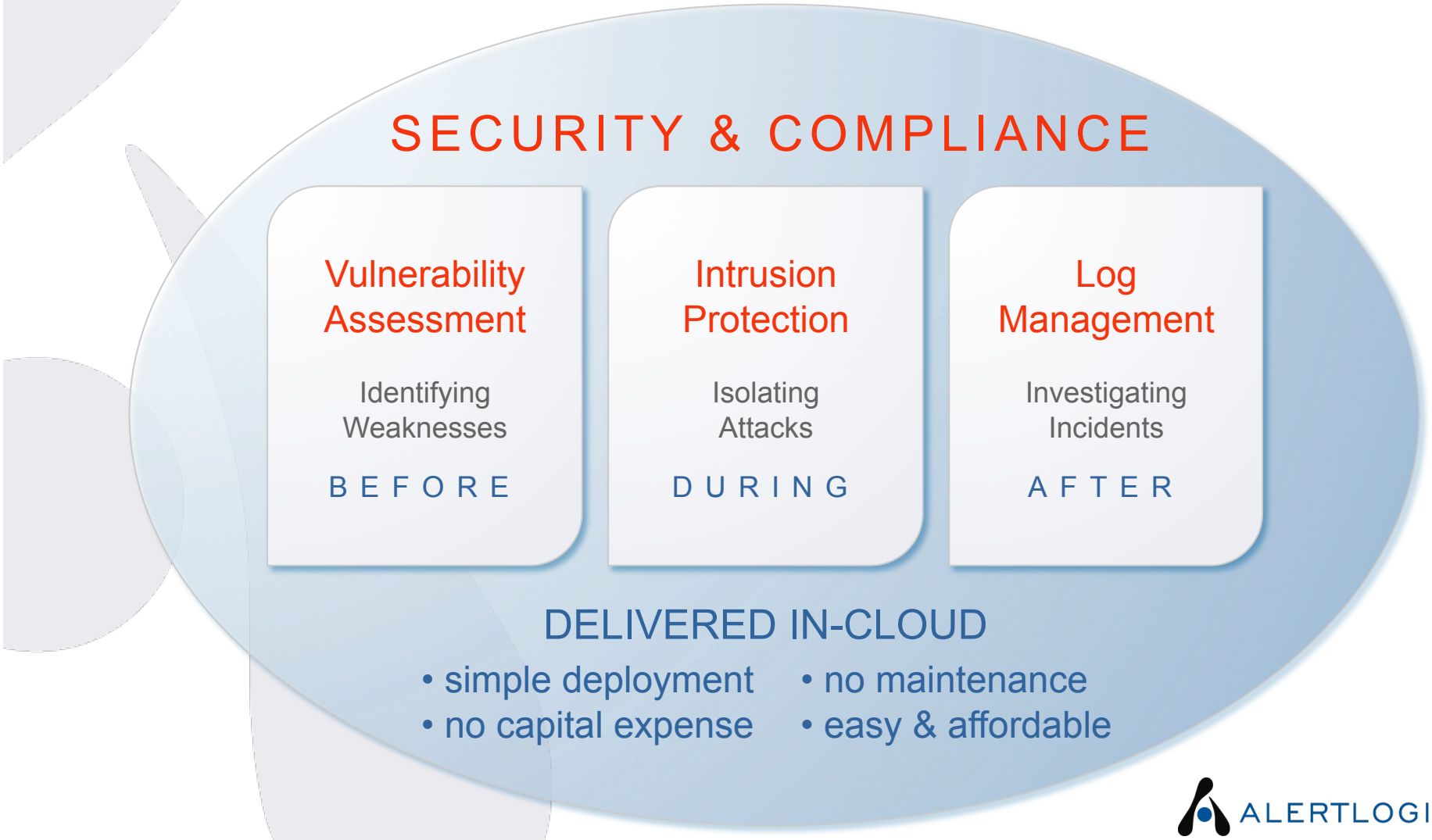
ALERTLOGIC

Cloud-Powered Delivery Model



ALERTLOGIC

Solving Key Problems



ALERTLOGIC

Software-as-a-Service Solutions

Log Manager

- What it does:
  - Automatically collect, store, correlate, search and report log data
- Why it's different and better:
  - Unique cloud-powered delivery model and cloud-ready technology
  - Patent-pending grid computing and storage architecture
  - High-speed searching and flexible parsing of log data
  - Correlates log, threat and vulnerability data to identify suspicious activity

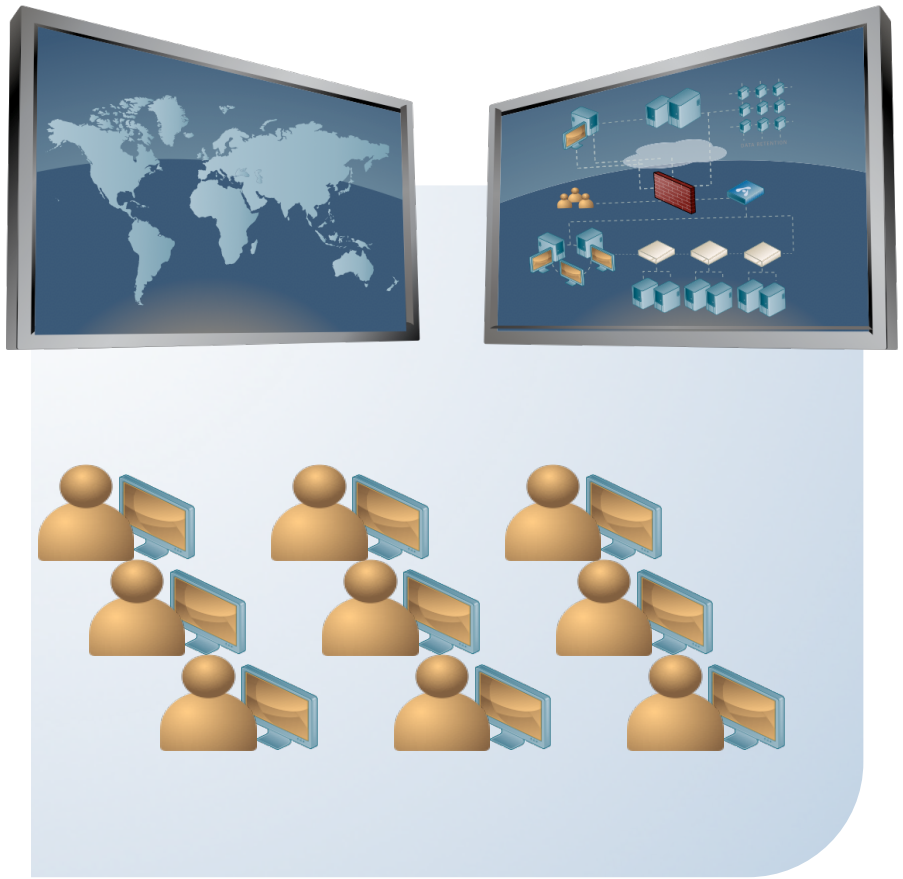
Threat Manager

- What it does:
  - Protects against threats and identifies internal/external vulnerabilities
  - PCI Approved Scanning Vendor
- Why it's different and better:
  - Unique cloud-powered delivery model and cloud-ready technology
  - Patent-pending grid computing and storage architecture
  - Patented expert system detects threats and defends against attacks
  - Security analysts provide monitoring, analysis and incident response services

ALERTLOGIC

Monitoring Services

- ActiveWatch
  - 24/7 threat monitoring for rapid incident response
  - Integrated incident and case management
- LogReview
  - Daily review of log data to comply with PCI DSS 10.6
  - Analysts alert customers on suspicious activity and possible security threats



ALERTLOGIC

Meeting Compliance Requirements

	PCI DSS **Penalties: fines, loss of credit card processing, and level 1 merchant requirements**	SOX (CobiT) **Penalties: fines up to $5M, up to 10 year imprisonment**
Vulnerability Assessment	6.2 Identify newly discovered security vulnerabilities 11.2 Perform network vulnerability scans quarterly by an ASV	DS 5.9 Malicious Software Prevention, Detection, and Correction "put preventive, detection, and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam)"
Intrusion Protection	5.1.1 Monitor zero day attacks not covered by Anti-Virus 11.4 Maintain IDS/IPS to monitor & alert personnel, keep engines up to date	DS 5.6 Security Incident Definition "clearly define and communicate the characteristics of potential security incidents so that they can be properly classified and treated by the incident and problem management process" DS 5.10 Network Security "use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks."
Log Management	10.2 Automated audit trails 10.3 Capture audit trails 10.5 Secure logs 10.6 Review logs at least daily 10.7 Maintain logs online for 3 months 10.7 Retain audit trail for at least 1 year	DS 5.5 Security Testing, Surveillance, and Monitoring "…a logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed."

ALERTLOGIC

Tangible Costs: Traditional vs. Cloud

Traditional Costs	Cloud-based Costs
Software Product or Appliance	Subscription Fee
Reporting Database	
Data Storage	
Redundant Data Storage	
Data Center Footprint	
Electricity	
Centralized Reporting Server	
Web Server	
Implementation Costs	
Maintenance Fees	
Consulting Fees	
Training	

Benefit Summary

Easy to buy, deploy and use

- Cloud-powered solutions deliver capabilities appliances can't match
- No capital equipment to purchase and maintain
- All costs included in one monthly fee

Enables regulatory compliance

- Identifies incidents and vulnerabilities that impact compliance
- Collects, reviews, and archives log data

Improves network security

- Helps detect and remedy threats and vulnerabilities
- Reviews log data daily to detect suspicious activity

ALERTLOGIC