Cloud-based IT Log Analytics

Christian Beedgen
Kumar Saurabh

Agenda

Overview

Team

Market Size

Problem Statement

The Next Generation

Differentiators

Competition

Go To Market

Economics

Roadmap

Summary

Overview

Cloud-based IT Log Analytics

Service to manage and analyze IT logs

$2.5 Billion market size

Current products have high TCO, are services-heavy

Easy to get started, lower TCO, superior intelligence

Team of log management veterans, to be completed

Series A – customer-focused development process

Team

Christian Beedgen

- **ArcSight** since 2001, Chief Architect, Director of Engineering
- Lead ESM server developer
- Built ESM server team, managing 20 people in server and UI teams
- Named on 2 granted patents, 7 patent applications in process
- Past experience at **Amazon**, **Gigaton**, **Cleverlearn**

Kumar Saurabh

- Data Architect at **Mint.com**
- Single handedly built Mint's data analysis infrastructure
- **ArcSight** 2001-2008, Director of Engineering, managing 12 people
- Lead for Analytics and Solutions Team
- Named on 2 granted patents, 2 patent applications in process

Key Drivers

Compliance is not optional

"What is the primary motivation for adopting or using security information management (SIM) within your enterprise?"

Base: 1,335 North American and European enterprise and SMB security decision-makers who expressed interest in adopting SIM
(percentages do not total 100 because of rounding)

Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008

FORRESTER® April 2009 **"Market Overview: Security Information Management (SIM)"**

Problem Statement

Today's market leading products are:

Premise-based

Enterprise sales cycles, installation and upgrade hassles, expensive hardware, DBAs, sysadmins required

Not scalable

Not inherently clustered, scaling introduces tradeoffs and data fragmentation

Challenged with log parsing

Either simply don't parse or require parsing at collection time, need constant software upgrades

Not context-aware

Identities, network assets, service dependencies are all critical for correlation and prioritization

Customers operate in silos

Insight gathered by one customer is hard to share; no cross-customer data mining

Not community-aware

Exchanging of solutions is a manual process, there's no marketplace

The Next Generation

1 **Cloud-based service**

Easy sale, quick delivery, ongoing upgrades, no care and feeding

2 **Seamless scalability**

Built from scratch for big data, leverages large-scale processing

3 **Machine-driven log parsing**

Extracting structure from raw logs is foundation for analytics

4 **Context modeling**

Logs need to be analyzed in their real world environment

5 **Global IT log intelligence**

Data mining leads to insight shareable across all customers

6 **Built-in community**

Not everybody is an expert, and even experts exchange findings

Deliver superior log management for compliance, security and operations in a scalable, easy-to-adopt cloud-based service

Target Market

Medium Enterprises
Large Enterprise Departments

Large Enterprises

Use Cases

Compliance

- PCI, SOX, HIPAA, NERC
- Log Retention & Review
- User & Resource Access

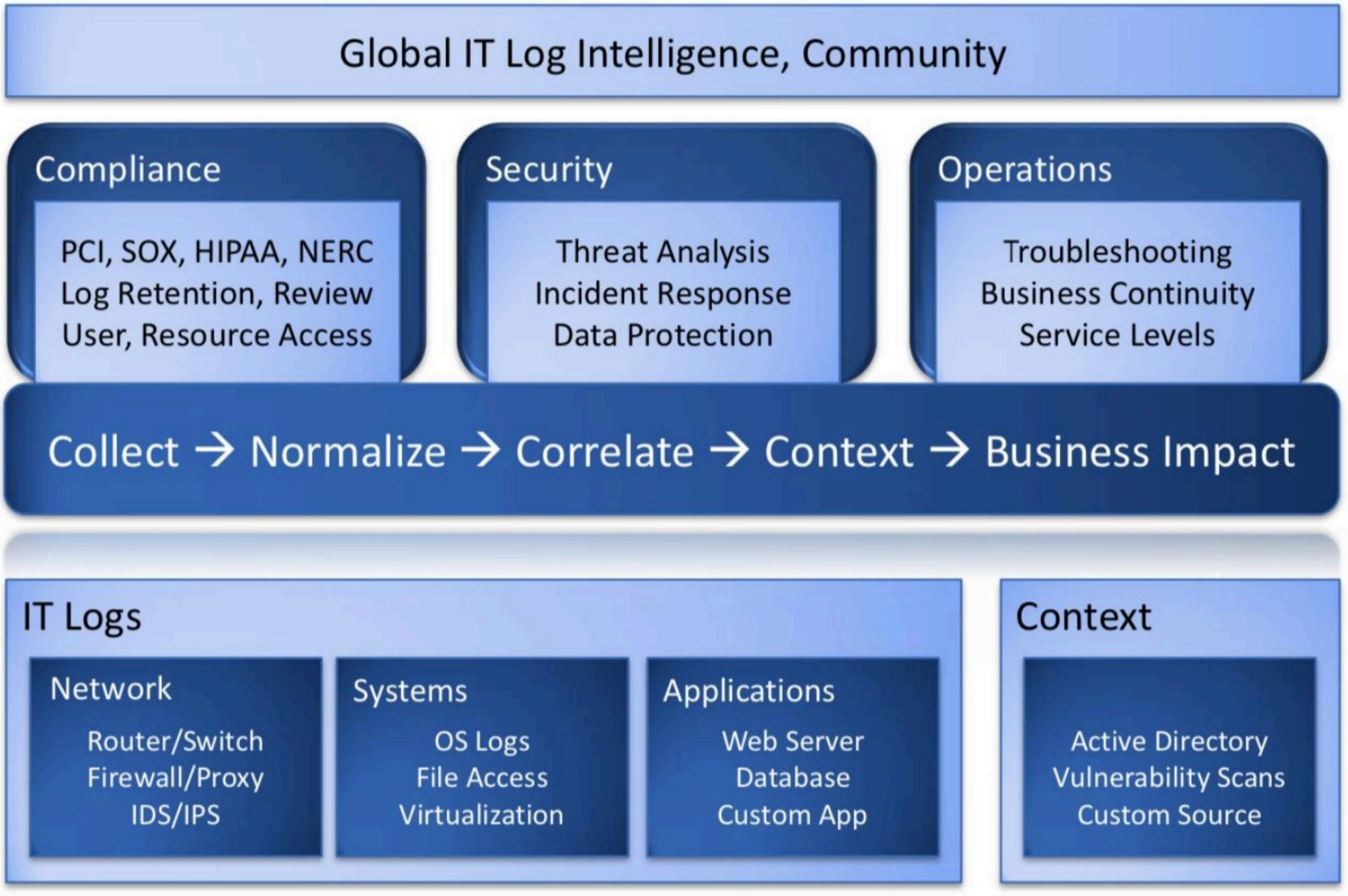
Security

- Incident Response
- Data Protection
- Threat Intelligence

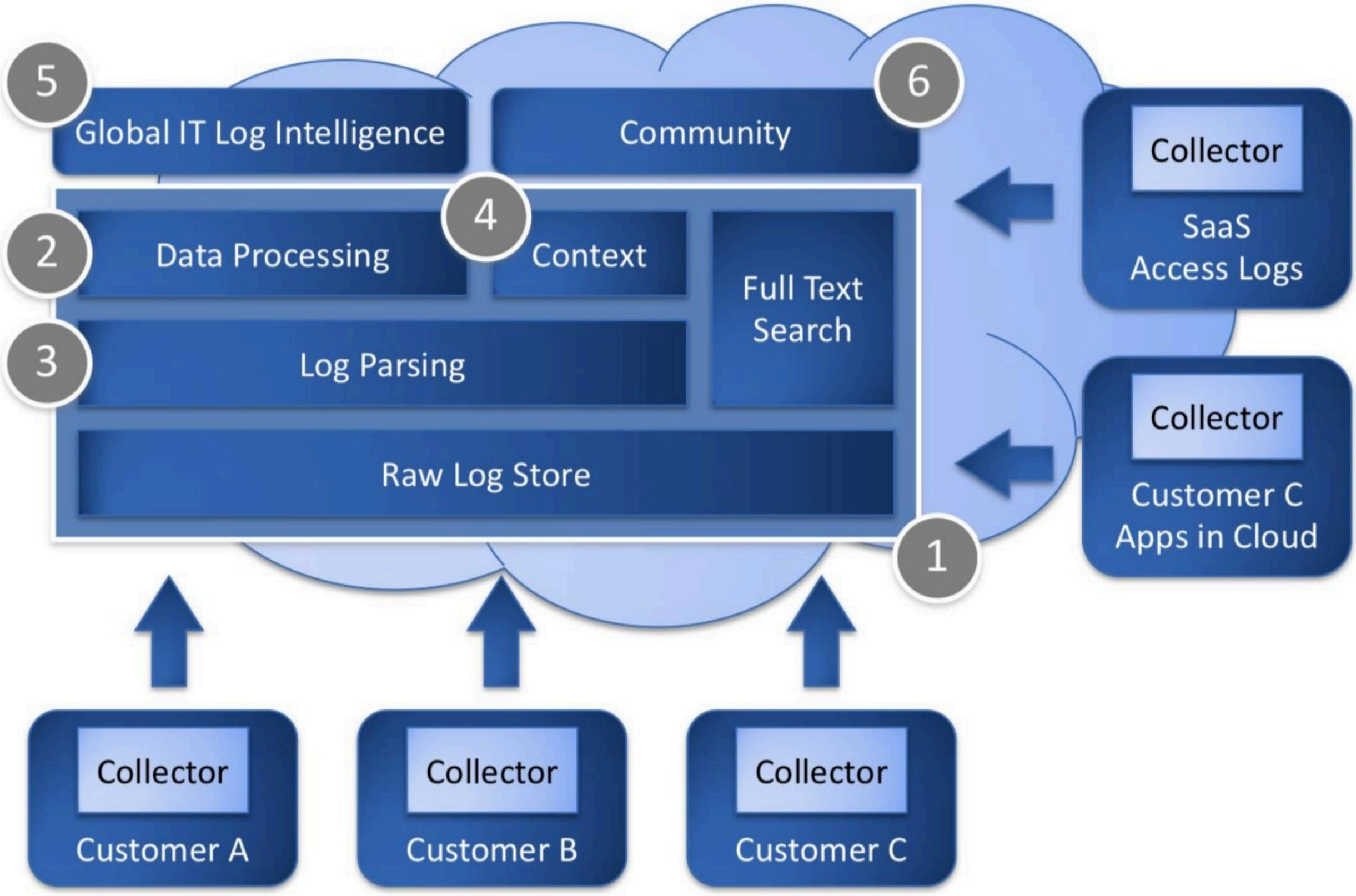
Operations

- Troubleshooting
- Business Continuity
- Service Levels

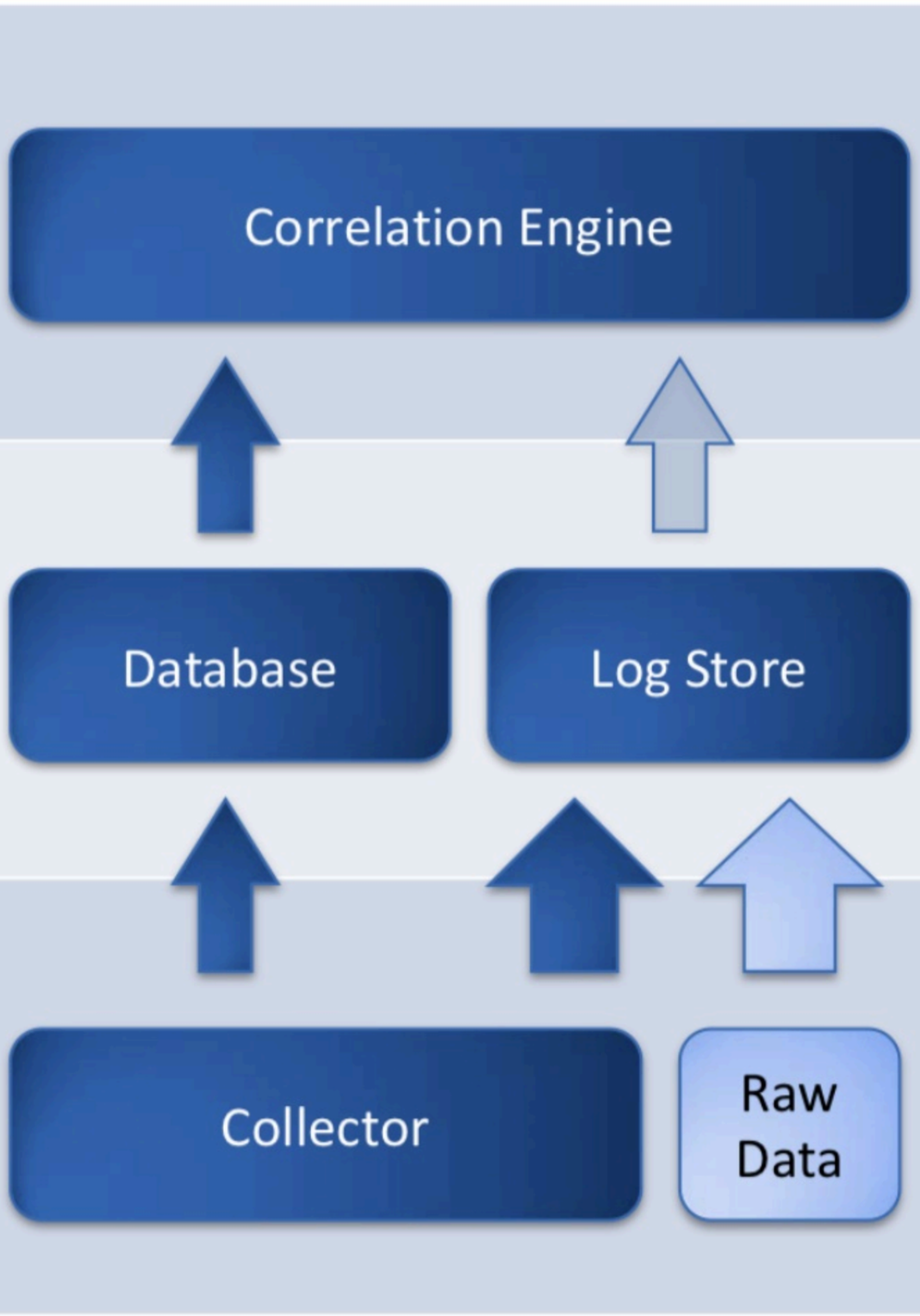
High-level Solutions Architecture



High-level Platform Architecture



Log Management Architecture Today



Analytics
Workflow

Compressed log store
Full-text search

Collection
Log parsing