

VORDEL CLOUD GATEWAY

Despite the agility and cost advantages of Cloud computing, IT departments have adopted Cloud slowly due to concerns over security, privacy, compliance, and reliability. While IT remains cautious, business users have fully embraced Cloud based services. Cloud usage in the enterprise today is widespread and uncontrolled, with neither security nor audit. Data is uploaded into Dropbox and LinkedIn, and applications are put up at Amazon and Force.com. Whether Cloud is strategic to IT or not, as long as Cloud based services are being used, IT must manage Cloud based risks. Using Vordel Cloud Gateway reduces Cloud related risks.

Make Approved Cloud Services Easier to Use

While it is impossible to completely eliminate rogue usage, most employees will try to comply with policies if a list of approved Cloud services is published. Simplifying the use of approved services will further reduce rogue usage. Single sign-on and usage reporting for cost center manager are two effective ways to encourage the use of approved services.

Secure and Monitor Cloud Usage

Security should not be left solely in the hands of the Cloud service providers. Enterprises must retain control over secure access to services and data traffic. Use Vordel Cloud Gateway to secure API keys, authenticate, authorize, and audit access to Cloud services. Also use the Gateway to monitor data traffic and enforce policies for security and compliance.

Integrate Cloud Services with On-premises Services

Cloud based services should not become silos of security and functionality. Use Vordel Cloud Gateway to integrate Cloud based services to on-premise services and infrastructure. Integrated Cloud services translate into best practice security, compliance, and governance. Integration also further encourages the use of approved services.

Feature Highlights

Using Vordel Cloud Gateway reduces risks associated with Cloud based services.

Access Security

Secure developer and end user access to the Cloud

- Security for API keys to Cloud services
- Authentication and single sign-on to Cloud services with enterprise credentials
- Integration to identity management platforms
- Authorization using enterprise fine grained authorization engine
- Security token mediation for identity federation

Data Security

Prevent data leakage and secure inbound messages

- Inspection of inbound and outbound Cloud traffic on the wire
- Enforce data security policy to remove, mask, or encrypt sensitive data
- Scan inbound requests to prevent message level attacks

Audit & Monitoring

Monitor, measure, and report Cloud usage and enforce SLAs

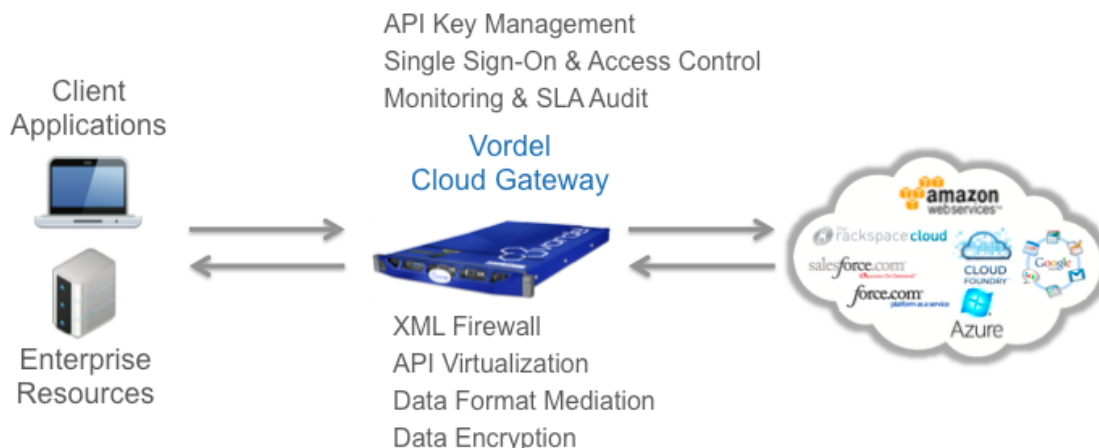
- Usage monitoring across all Cloud services
- User, client, view, data, & transaction level logging
- Detect rogue usage of non-approved Cloud services
- Usage measurement and reporting by cost centers
- Service quality measurement and service level agreement reporting
- Service monitoring & alerting

Integration

Integrate Cloud services to on-premise services

- Protocol translation, e.g. REST, SOAP, JSON, Java API
- Virtualization and mash-up of on-premise service APIs to Cloud services
- Virtualization and mash-up of Cloud service APIs to on-premise services
- Request routing, throttling, and response caching

Vordel Cloud Gateway Solution



 **vordel** “Applications Anywhere”

Copyright © 2011, Vordel Inc. and/or its affiliates. All rights reserved.

For more information or sales enquiries, contact sales@vordel.com

USA +1 866-460-0987 | Rest of World +44 203-427-5082

Single Sign-on From Enterprise Identity Management

Extending single sign-on (SSO) from the enterprise identity management platform to Cloud based services makes sense for user experience, support cost, and security best practice. Vordel Cloud Gateway simplifies Cloud SSO with out-of-the-box integration from all the leading identity management platforms to the most popular Cloud services such as Amazon, Google Apps, Microsoft Azure, and Salesforce.com.

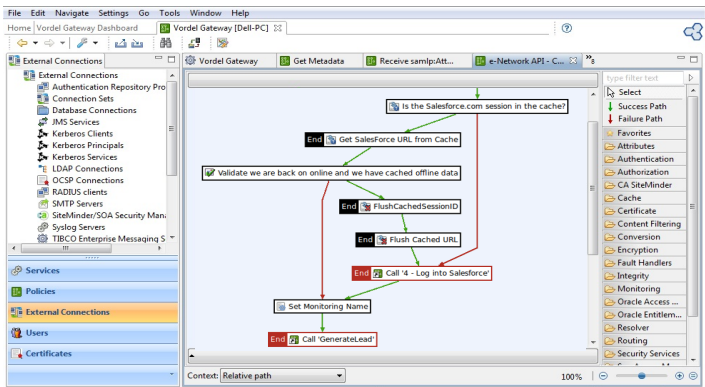


Centrally Protect and Manage API Keys

Cloud based services typically require an API key to identify the API caller. The key is also used for signing and encryption. Any application looking to integrate with the Cloud service will need access to the API key. Distributing API keys from the various Cloud services to all the on-premise applications is neither a scalable nor a secure practice. It is best to store the API key centrally at the Vordel Cloud Gateway. Thus API key insertion and encryption are delegated from the application to the Gateway. Vordel also supports on-board and network based HSM options for secured key storage.

Enforce Data Security Policies

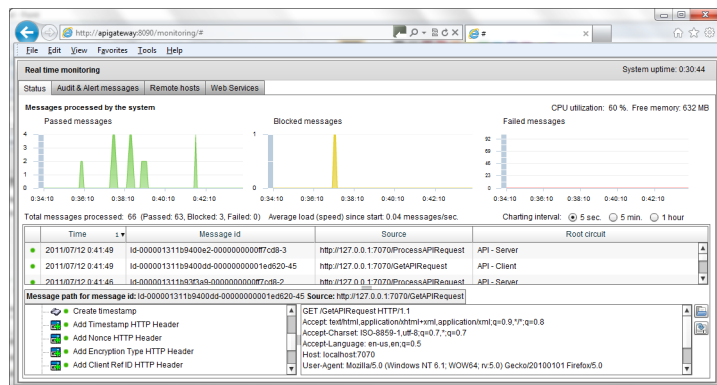
Business users and application developers do not understand the security risks associated with the Cloud. It is all too easy to have sensitive data uploaded into the Cloud, violating security policies and creating compliance issues. Vordel Cloud Gateway scans messages and data payloads bound for the Cloud against security and privacy policies. Based on the type of data and Cloud service, the Gateway can block, redact, remove, or encrypt data before they leave the premise.



Drag-and-Drop Policy Development

Audit & Monitor Cloud Usage

Cloud based services are easy to buy by design. Services can be purchased with credit cards anytime, usage can be increased instantaneously, and subscription automatically renews. Without monitoring, these conveniences can lead to waste and abuse. By monitoring and reporting on Cloud usage, enterprise can negotiate more favorable terms, release resources no longer used, and match expenses to projects. Vordel Cloud Gateway monitors what services are used, when are services used, and who use the services. Usage statistic can be automatically delivered to IT and cost center managers on a scheduled basis.



Monitor Cloud Usage

Monitor Service Quality and Audit Service Level Agreement (SLA)

Cloud based services are available at a multitude of price points and SLAs. High availability and high performance can be had for the right price, but the actual attained performance is subject to Internet and local network variables. Vordel Cloud Gateway monitors service quality both in the Cloud and on-premise. This analysis can be used to audit a provider's quality of service, as well as determine which service level is most appropriate. Paying a premium for a quality of service level that is not needed or cannot be achieved defeats the cost benefit of using Cloud based services in the first place. Vordel Cloud Gateway can also raise alerts when a service becomes unavailable or the service level no longer meets minimum quality thresholds.

Virtualize and Route Cloud Traffic

Cloud based services are being multi-sourced to provide redundancy, performance optimization, load management, and to match service levels to requirements. Vordel Cloud Gateway provides design-time and run-time management across multiple Cloud service providers. The Gateway virtualizes APIs across different services to provide isolation and standardization. The Gateway also routes run-time traffic among service providers, using policies based on client, location, transaction type, message size, service level, network condition and other attributes.