



CloudSpan CloudControl

API Management for Cloud-based Service Providers

CloudSpan CloudControl offers:

API Abstraction

Enterprise-strength threat protection, access controls, and SLA enforcement in a dedicated hardware or software-based security appliance.

API Orchestration

Create multiple API subsets or aggregate APIs; then leverage policy to dynamically sequence API calls in order to help automate the allocation of computing resources.

API Lifecycle

Govern the API lifecycle from development through testing to production with automated versioning, rollback and the ability to mediate between API versions to ensure existing applications don't break.

Integration Capabilities

Out-of-the-box support for multiple transport protocols as well as robust management APIs simplifies integration with existing billing, reporting, portal and other enterprise systems.

vCloud Support

Pre-tested to work with VMware vCloud Director APIs.

To learn more about Layer 7 and how it can address your organization's needs, call 1-800-681-9377 (toll free within North America) or +1.604.681.9377. You can also email us at info@layer7.com; friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at layer7.com, or follow-us on [twitter @layer7](https://twitter.com/layer7)

Govern the consumption of your IaaS, PaaS and SaaS APIs, while gaining orchestration and remote management capabilities

Minimize Service Delivery Costs

Cloud-based service providers that offer products and services to customers on a pay per use or utility basis are concerned with automating the allocation of computing resources, ideally on a self-service basis in order to minimize cost of delivery. But before that can happen service providers will need some way to programmatically secure, manage and orchestrate their computing resource APIs in a cost-effective manner.

For this reason, Layer 7 created CloudSpan CloudControl. Deployable as hardware, software, VMware/ESX or Amazon Machine Image (AMI), CloudControl allows service providers to securely control their IaaS, PaaS and SaaS resources, as well as management, provisioning and configuration APIs using policy-driven controls.

CloudControl creates a layer of abstraction or indirection between what service providers expose internally and what third parties can see externally. Service providers can use policy-based controls to customize the message, identity and interface level security for their APIs; track usage, manage performance and monitor interface health.

API Abstraction, Orchestration and Lifecycle

CloudControl gives service providers the ability to manage the security for their APIs outside of API logic in order to ensure consistent, adaptable and verifiable policy-based security, including fine-grained access control and comprehensive threat protection. Policies can specify exactly how and in what ways your APIs are used by each stakeholder, metering and throttling access based on SLA, identity, time period, and so on, as appropriate.

CloudControl can also let you aggregate, recompose, or remap APIs, orchestrating how they get invoked. In this way, CloudControl can let service providers programmatically manage and control their systems, helping to automate the workflow associated with spinning up and down computing resources.

Finally, Layer 7 also provides the ability to manage the API lifecycle, facilitating the migration of APIs between development, testing and production by automatically resolving discrepancies between environments, and thereby reducing migration risk. As your APIs evolve, Layer 7 can mediate between API versions ensuring client applications don't break. This speeds time to market for new product and service offerings, since changes can be rolled out and accommodated for in infrastructure, rather than having to force APIs and client applications to evolve in lockstep.

Key Features	
API Protection & Control	
Threat Protection	<ul style="list-style-type: none"> Protect against Cross-Site Scripting (XSS), SQL Injection, XML content/structural threats & viruses Create custom threat profiles to extend built-in filters for message structure & XML-specific threats Track failed authentications and/or policy violations to identify patterns and potential threats Validate HTTP parameters, REST query/POST parameters, JSON data structures, XML schemas, etc
Access Control	<ul style="list-style-type: none"> Support for HTTP basic, digest, SSL client-side certificate authorization, Microsoft SPNEGO, etc Support for all major authentication and authorization standards, including SAML, Kerberos, digital signatures, X.509 certificates, LDAP, OAuth, etc, and leading identity and access management systems
Privacy	<ul style="list-style-type: none"> Powerful message content filtering and transformation tools help identify and suppress leakage of sensitive information (i.e. SSNs, credit card numbers, etc.) Support for multiple types of element or message level XML signing and encryption
API Abstraction & Management	
API Lifecycle	<ul style="list-style-type: none"> APIs can be smoothly migrated between environments (i.e., from Dev to Test, East to West, etc) with full dependency resolution and re-mapping Supports automatic API versioning including rollback to any previous version Global security settings, threat detection profiles, etc. can be reused across multiple APIs to save time and ensure consistency
API Composition	<ul style="list-style-type: none"> Point and click API composer supports quickly building composite virtual APIs from any combination and/or subset of existing APIs
Orchestration	<ul style="list-style-type: none"> Policy-driven API request sequencing based on administrator-defined conditions and logic Routing based on message content or service availability Run multiple back-end service calls concurrently, thereby reducing overall latency
SLA/Performance Control	<ul style="list-style-type: none"> Enforce availability through throttling and/or rate limiting to ensure SLAs and QoS priorities Advanced, carrier-grade traffic shaping to manage bandwidth to API servers Access to API methods can be filtered/restricted based on user, time of day, service level, etc. Route traffic based on geography, IP address, back-end response times, etc for optimum performance Integrated clustering provides scalability and automatic failover between multiple instances of APIs/services
API Metering & Reporting	
Metrics and Reporting	<ul style="list-style-type: none"> Configurable, out-of-the-box reports provide insight into API performance: meter and track API/method usage for per-user billing, capacity planning, SLA compliance etc. Real time monitoring dashboard provides fine-grained insight into API & network level performance
Customer Mapping	<ul style="list-style-type: none"> Report on service performance, policy violations and SLA conformance based on specific customers, composites (i.e., processes and transactions using a service) or clients to build a profile of user experience
Audit transactions	<ul style="list-style-type: none"> Log files provide a granular audit trail of all API connections mediated by CloudControl
Fit to Environment	
Mediation	<ul style="list-style-type: none"> Supports mapping between any combination of XML/REST/SOAP APIs simplifying customer adoption Supports multiple transport protocols, including mediation between HTTP, HTTPS, MQS, JMS, raw TCP Filter/customize back-end error messages to better fit customer deployment patterns
vCloud Support	<ul style="list-style-type: none"> Abstract vCloud APIs, simplifying management and control of vCloud Director in order to streamline automation Integrated security solution provides fine-grained authorization, as well as protection against denial-of-service (DoS) attacks

PCI-DSS	<ul style="list-style-type: none"> Layer 7's PCI-DSS installation and configuration guide allows customers to configure and deploy CloudControl as part of a PCI-compliant process
Management API	<ul style="list-style-type: none"> Remote management APIs allow customers to hook their existing, third-party management tools into CloudControl, simplifying asset management Command line, SOAP and Java-based APIs streamline integration with existing enterprise applications
Form Factors	
Hardware	<ul style="list-style-type: none"> Active-active clusterable, dual power supply, mirrored hot-swappable drives, multi-core 1U server
Software	<ul style="list-style-type: none"> Solaris 10 for x86 and Niagara, SUSE Linux, Red Hat Linux 4.0/5.0
Virtual Appliance	<ul style="list-style-type: none"> VMware/ESX (VMware Ready certified)
Cloud	<ul style="list-style-type: none"> Amazon EC2 AMI
Supported Standards	
XML, JSON, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, SAML, XACML, OAuth, PKCS, X.509 Certificates, FIPS 140-2, Kerberos, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, POP3, IMAP4, HTTP/HTTPS, JMS, MQ Series, Tibco EMS, Raw TCP, FTP/FTPS, WS-Security, WS-Trust, WS-Federation, WS-SecureExchange, WS-Addressing, WS-SecureConversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WS-PolicyAttachment, WSIL, WS-I, WS-I BSP, UDDI, WSRR, MTOM, IPv6, WCF	

To learn more about Layer 7 call us today at +1 800.681.9377 (toll free within North America) or +1.604.681.9377. You can also email us at info@layer7.com; friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at layer7.com, or follow-us on twitter [@layer7](https://twitter.com/layer7).