



# Layer 7 and HP ArcSight ETRM



## Layer 7 & HP ArcSight Deliver Enhanced Transaction Visibility Get Deeper Security Insight Across Mobile, Cloud and SOA

### Key Benefits

- Extend perimeter intelligence
- Get API-level security awareness
- Track external identities
- Ensure compliance
- Enhance cyber security

To learn more about Layer 7 and how it can address your organization's SOA and Web services 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](mailto:info@layer7.com); friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at [layer7.com](http://layer7.com), or follow-us on twitter [@layer7](https://twitter.com/layer7)

Layer 7 Technologies has certified its SecureSpan & CloudSpan Gateways for integration with HP ArcSight, giving ArcSight customers the ability to correlate and analyze application traffic from SOA, Cloud and mobile platforms. By deploying Layer 7 Gateways with the ArcSight Enterprise Threat and Risk Management (ETRM) platform, customers can understand how external identities interact with applications that expose programmatic APIs.

Layer 7's ArcSight Common Event Format (CEF) Certification provides seamless integration of events related to application requests originating from partners, Cloud deployments or mobile environments called through an API in the DMZ. By deploying SecureSpan or CloudSpan Gateways as a part of their on-premise or in-Cloud security perimeter, ArcSight customers can implement a solution that has global data collection and policy enforcement capabilities. These platforms are based on redundant, globally-distributed, session-aware gateway clusters distributed across physical, virtual and Cloud deployments.

By configuring Layer 7 Gateways to leverage the collection, analysis and assessment capabilities of ArcSight ETRM, Layer 7 provides organizations with the ability to deliver optimum perimeter security intelligence, even when the perimeter is extended to partners, Cloud and mobile devices.

### Challenges

Externalizing applications for partner, Cloud or mobile access creates novel business opportunities but also raises a number of new concerns about data security, enforcement of appropriate access control and visibility of application usage across the extended enterprise. Typical challenges include:

- **Access control** – How can you extend the strict limitations exerted upon known consumers within the enterprise to new external users – even when they use federated credentials?
- **Threat recognition** – How can you raise awareness of new attack vectors that may be specific to API or Cloud deployments?
- **End-to-end visibility** – How can you monitor all application traffic, internal and external, using a consistent event model for correlation and analysis?

Layer 7, in conjunction with ArcSight, can help you implement a solution to these challenges, enabling you to move towards a more comprehensive view of application transactions and associated threats based on outside identities.

### Solution

Using a combination of ArcSight's ETRM platform and the CEF event format specification, Layer 7 offers organizations the ability to gather application-aware API-level event logs relating to access control, data validation, cyber security threats, message routing and security infrastructure policy enforcement decisions. Enterprises will be able to deliver applications with secure, compliant, well-governed interfaces at the network, transport and application layers.

## Applications & Benefits

### Applications

Application Usage Records	Gateways deliver events to ArcSight for every incoming request, thereby providing a clear picture of application usage across all interfaces.
Application-Aware Event Summaries	Gateways extract data samples specific to the application being protected, providing a clear audit record of the service/operation executed by a specific user at a specific time, with supporting metadata for optimal correlation with other related events.
Threat Protection	Layer 7 protects against and notifies ArcSight about an exhaustive list of common threats, including infrastructure attacks (DoS or parser exploits), application attacks with malicious content/attachments/behavior and transactional attacks (session/identity hijacking).
Identity Mapping	Credentials for external requestors, including partner applications, end-user consumers and mobile “app” users, can be authenticated and authorized using a wide variety of standards-based and proprietary access control mechanisms, then mapped to internal identities or roles for analysis within ArcSight IdentityView.
End-to-End Application Visibility	Routing decisions, authentication/authorization lookups and orchestrated service calls will touch other portions of the enterprise infrastructure. Events can be delivered to ArcSight for each one of these additional callouts.
Infrastructure Health Notifications	Layer 7’s awareness of service response times, throughput statistics and expected SLAs can be used to notify ArcSight of sub-optimal conditions that could be threat-related.
Threat Remediation Enforcement	Threats detected by ArcSight can be incorporated into Layer 7 policies for protection against similar future attacks.

### Benefits

Extend Perimeter Intelligence	Extend the perimeter to partners, mobile apps and the Cloud.
API-Level Security Awareness	Guard against API-level application threats in SOA, Cloud and mobile not detected by traditional network-level firewalls or WAFs.
Track External Identities	Track transactions originating with outside identities; reconcile federated identities using SAML and OAuth.
Enhanced Compliance	Protect application traffic with Gateways that are Common Criteria EAL4+ and FIPS 140-2 certified, PCI-DSS compliant, as well as vulnerability tested for DoD STIG.
Enhanced Cyber Security	Enforce policies around fine-grained access control, data validation/ privacy/integrity, multi-faceted threat protection, credential chaining and service monitoring.

The screenshot displays the ArcSight Layer7 management interface. At the top, there's a navigation bar with the ArcSight logo and 'Layer7' title. Below it, a summary card for 'Layer7 (100%)' shows event counts: Very High: 0, High: 17, Medium: 35, Low: 135, Very Low: 0, and Total Events: 187. A play button icon indicates the data is updated. Below the summary is a bar chart showing event distribution. At the bottom, a table lists events with columns for Manager Receipt Time, End Time, Name, Device Vendor, Device Product, Device Severity, Device Action, Device Event Class ID, Device Host Name, and Device Address.

Manager Receipt Time	End Time	Name	Device Vendor	Device Product	Device Severity	Device Action	Device Event Class ID	Device Host Name	Device Address
9/13/2011 1:28:30 PM PDT	9/13/2011 1:28:18 PM PDT	Request Metrics Inbound	Layer7 Technologies Inc.	SecureSpan Gateway	2	Receive Request	100		127.0.0.1
9/13/2011 1:28:30 PM PDT	9/13/2011 1:28:18 PM PDT	Request Metrics Inbound	Layer7 Technologies Inc.	SecureSpan Gateway	2	Receive Request	100		127.0.0.1
9/13/2011 1:28:30 PM PDT	9/13/2011 1:28:18 PM PDT	Access Control	Layer7 Technologies Inc.	SecureSpan Gateway	4	Authentication	200	prod-01130	
9/13/2011 1:28:30 PM PDT	9/13/2011 1:28:18 PM PDT	Message Validation Violation	Layer7 Technologies Inc.	SecureSpan Gateway	8	Request processing aborted	540	prod-01130	

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](mailto:info@layer7.com), visit us at [layer7.com](http://layer7.com), friend us at [facebook.com/layer7](https://facebook.com/layer7) or follow-us on Twitter [@layer7](https://twitter.com/layer7).