FIREEYE iSIGHT INTELLIGENCE API & SDK

INTEGRATE ACTIONABLE INTELLIGENCE INTO YOUR SECURITY TECHNOLOGIES

OVERVIEW

The Application Programming Interface (API) and Software Development Kit (SDK) for FireEye iSIGHT Intelligence lets you fuse our intelligence with your security infrastructure and compliance management technologies. The iSIGHT API & SDK links your security technologies to the FireEye iSIGHT Intelligence cloud which houses nearly a decade of the most comprehensive, globally mined cyber threat intelligence available.

iSIGHT API & SDK makes it simple to integrate intelligence into your protection, detection, investigation, and response processes. Work smarter, not harder with iSIGHT intelligence inside your key result security systems.

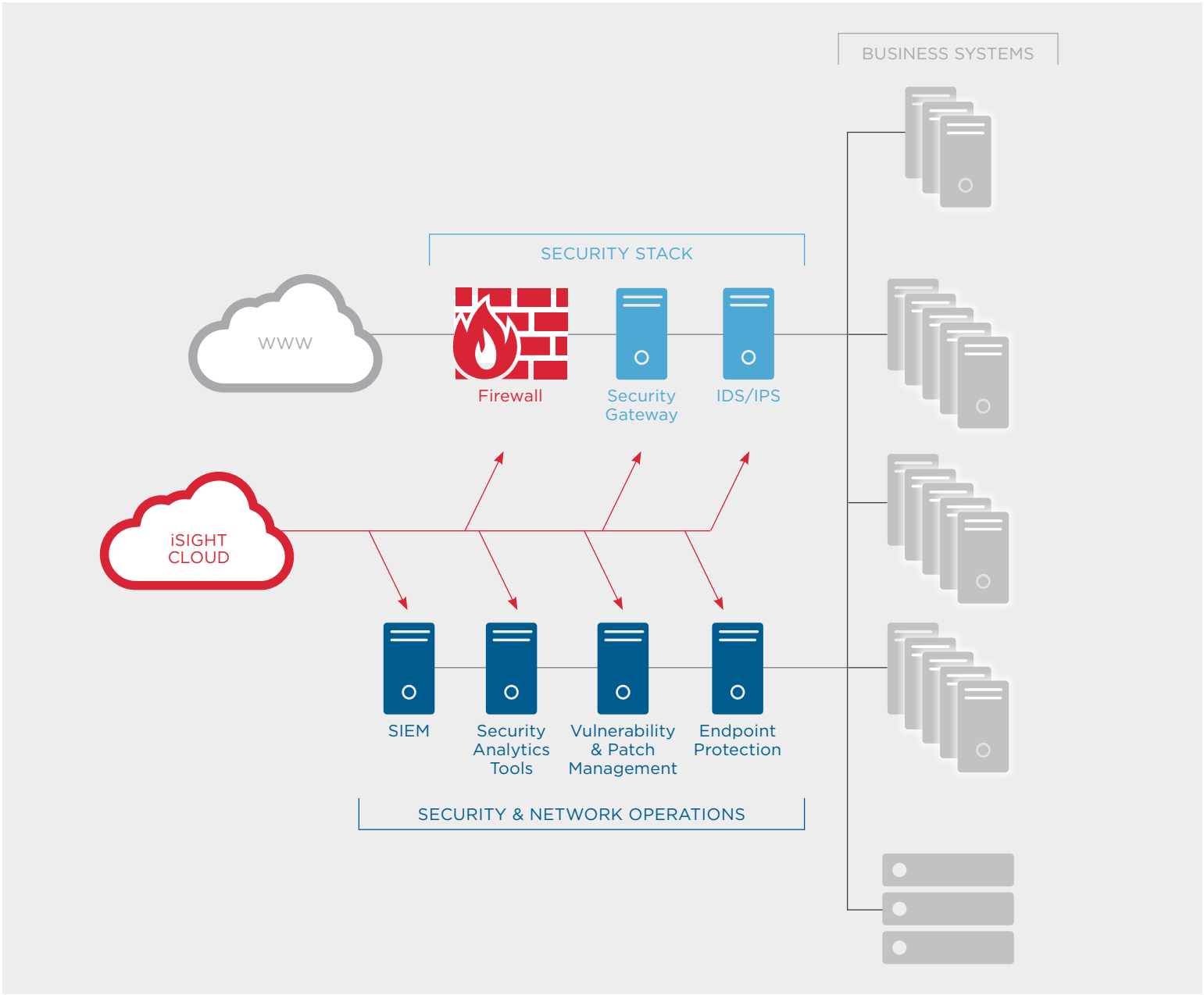
THE RESULT

"iSIGHT API & SDK provide unlimited opportunities to match previously disparate event data with rich intelligence context so that "actionable intelligence" is actionable at machine speed."

FireEye

Adding Intelligence To Your Security Tools

A large and growing list of security vendors have developed out of the box integrations using the iSIGHT API & SDK. Whether you want to enrich existing tools and processes, implement new intelligence-driven solutions or integrate intelligence into your homegrown system, we've got you covered.



Some of our Technology Integration Partners

In addition to these out-of-the-box integrations, iSIGHT API & SDK are easily connected with custom or homegrown platforms and technologies that support open industry standards.

iSIGHT API & SDK provide machine-to-machine-integration with the most contextually rich threat intelligence data available on the market today. The API & SDK provides automated access to much more than indicators of compromise (IOC) – IP addresses, domain names, URLs the bad guys are using – we also provide information on the adversary enriching the integration further.

iSIGHT API and SDK support industry standards. The API supports Python, Java, PHP, C++, and C# programming languages. The SDK supports the C, C++, C#, Perl & Python programming languages and will run on the three latest versions of Red Hat Enterprise Linux, Microsoft Windows Server, and Windows 7. For further information, you can check out the full documentation on our website.

What Can iSIGHT API & SDK Do For You?

Security Operations

The average organization generates thousands of security events every day but only has the human resources to investigate a few. How do you know which events to focus on? With iSIGHT API & SDK you can match IOCs with events in your SIEM or security analytics platforms, cut through the noise and automate the prioritization of the events that warrant scrutiny. You can also drastically accelerate triage with context that helps you understand what you are facing. Are you dealing with cyber crime or espionage? Is this threat targeting our industry or is this likely "overspray" from a campaign targeting others?

Intelligence Streams

- Daily Threat Media Highlights emails
- Intel Portal – Access to all historical reporting and email/SMS alerts
- iSIGHT API and SDK
- iSIGHT Browser Plugin
- Out of the Box Integrations

Dedicated Client Support

- Three levels of Intelligence Enablement & Support to choose from:
- Level 1 – Self Service: equips you with the materials and basic engagement needed for the intelligence.
- Level 2 – Intelligence Coordination: enhances the operational relationship between you and FireEye with a designated Intelligence Account Manager.
- Level 3 – Intelligence Optimization: integrates the intelligence with your security operations via a designated Intelligence Account Manager and Threat Analyst. Includes three intelligence workshops a year.
- Analyst Access - direct access to analysts

FIREEYE ISIGHT API & SDK ENABLE YOU TO INTEGRATE THE WORLD'S BEST CYBER THREAT INTELLIGENCE, INTO YOUR EXISTING SECURITY AND COMPLIANCE MANAGEMENT PROCESSES AND TECHNOLOGIES.

FireEye iSIGHT Intelligence Product Technical Feature Set

TACTICAL THREAT INTELLIGENCE	NOTES
Intelligence Portal Access	NO
Indicators across all motivations	YES
API Endpoints: Basic Only	See Basic Description
API version available	Latest
Indicator API formats:	JSON, XML, CSV
Report API formats:	Not Offered
API Rate limit	1 query / 1 sec
Suitable for SIEM	Yes
Suitable for Threat Intel Platform	Potentially - Indicators only
API queries / day	1,000 / day
Analyst Access	Not Offered
Support Options	L1 - Self Help
Basic API Endpoints, limited to: API Endpoint: "/view/iocs" API Endpoint: "/search/basic" API Endpoint: "/pivot/indicator"	 YES YES YES

OPERATIONAL / FUSION THREAT INTELLIGENCE	NOTES
Intelligence Portal Access	YES - Contextual reports and tactical indicators
Indicators across all motivations	YES
All API Endpoints:	YES
API version available	Latest
Indicator API formats:	JSON, XML, CSV, SNORT
Report API formats:	JSON, XML, HTML, PDF, STIX v1.1.1
API Rate limit	4 queries / 1 sec
Suitable for SIEM	Yes
Suitable for Threat Intel Platform	Yes
API queries / day	Operational: 10,000 / day, Fusion: 20,000 / day
Analyst Access	Negotiated by Support Level
Support Options	L1 - Self Help, L2 - Intelligence Coordination, L3 Intelligence Optimization

Full access to intelligence web portal w/ contextual reporting
Full access to reporting API endpoints
Full access to pivoting API endpoints
Full access to log search
Full access to targets endpoint (malware / actor)
Threat Media Highlights
Browser Plugin Firefox / Chrome
Software Development Kit
Malware Overviews and Profiles
Actor Profiles
.....several other features

VULNERABILITY INTELLIGENCE	NOTES
Intelligence Portal Access	YES - Vulnerability reports
Indicators across all motivations	NO
API Endpoints: Basic Only	See Basic Description
API version available	Latest
Indicator API formats:	JSON, XML, CSV
Report API formats:	JSON, XML, HTML, PDF, STIX v1.1.1
API Rate limit	1 queries / 1 sec
Suitable for SIEM	Yes
Suitable for Threat Intel Platform	Yes
API queries / day	1,000 / day
Analyst Access	Negotiated by Support Level
Support Options	L1 - Self Help, L2 - Intelligence Coordination, L3 Intelligence Optimization
Full access to vulnerability product web portal w/ contextual reporting	
Basic API Endpoints, limited to:	
API Endpoint: "/view/vulnerability"	YES
API Endpoint: "/report"	YES
API Endpoint: "/report/index"	YES
API Endpoint: "/search/text"	YES
API Endpoint: "/search/basic"	YES

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye