JSA Series Secure Analytics Appliances with IBM Security X-Force Threat Intelligence

Product Overview

IBM Security X-Force Threat Intelligence augments the JSA Series Secure Analytics Appliances intelligence capabilities by feeding in proprietary threat insights, including data on malware hosts, spam sources, and anonymous proxies. This allows organizations to use up-to-the-minute threat intelligence to gain deeper insight and greater protection to prevent or minimize the impact of today's complex and serious security attacks.

Product Description

As security threats steadily increase in volume and sophistication, it's becoming more challenging to identify the most serious ones. Users must correlate threat information from multiple sources to make more informed decisions about which security issues pose the biggest threats to their organizations. This is particularly true on today's smarter planet, where instrumented, interconnected, and intelligent businesses collect, process, use, and store more information than ever before. With today's large variety of incoming attacks, it can be extremely difficult to detect and analyze ever-changing threats—much less turn collected threat data into actionable insights that consistently identify which threats are most dangerous.

A solid security foundation designed to meet this need is Juniper Networks® JSA Series Secure Analytics Appliances, an integrated family of products that helps detect and defend against threats by applying sophisticated analytics to more types of data. In doing so, the platform helps identify high-priority incidents that might otherwise get lost in the noise. And you can extend these comprehensive analytics still further, using IBM Security X-Force Threat Intelligence to augment the JSA Series Secure Analytics family's intelligence capabilities by feeding in proprietary threat insights, including data on malware hosts, spam sources, and anonymous proxies. Combining worldwide intelligence from IBM X-Force with security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management capabilities from Juniper's portfolio of solutions provides users with additional context on security incidents, helping improve prioritization of incidents that require additional examination—and enabling organizations to prevent or minimize damaging attacks.

Architecture and Key Components

Tens of thousands of malware samples are created every day, with new classes of threats continually added to and improved upon. Sophisticated hackers use polymorphic programs to alter malware into new form factors after each delivery. And all of this is exacerbated by the proliferation of mobile devices, cloud computing, and virtualization—in fact, the intersection of these technologies provides fertile new ground for threats and malware.

In addition, today's attacks are often not random, but targeted for maximum financial gain and impact. Rogue individuals and groups are constantly innovating new ways to attack organizations' critical data. As a result, traditional methods of dealing with Internet threats are no longer enough. Organizations need visibility into a much wider range of threat data than ever before in order to protect themselves most effectively. Adding X-Force Threat Intelligence to JSA Series Secure Analytics Appliances can provide the extra intelligence required to go up against these modern day threats.

Your ideas. Connected.™

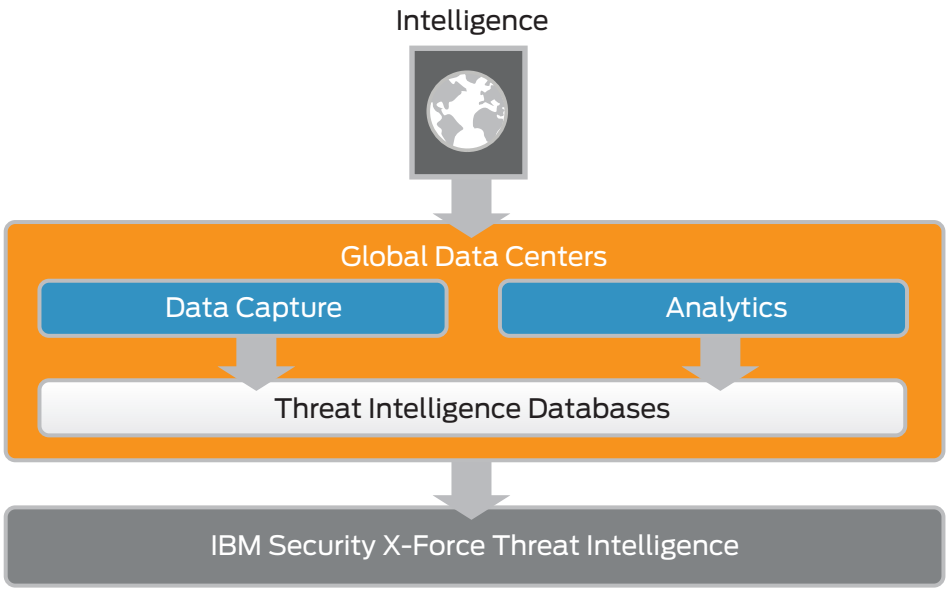

Figure 1. The X-Force research and development team inspects millions of new and updated Internet sites every day, collects information, categorizes content, and identifies those sites that pose a security danger to an organization.

Channel the Power of IBM X-Force

X-Force Threat Intelligence is much more than just a compilation of threat data. Behind it is the power of the IBM X-Force research and development team—one of the best-known commercial security research groups in the world. This team of security experts provides the foundation for the IBM preemptive approach to Internet security by focusing its attention on researching and evaluating vulnerabilities and security issues, developing assessments and countermeasure technologies for IBM products, and educating users about emerging Internet threats and trends.

X-Force is instrumental in protecting users against the threat of attack because IBM's knowledge base and data collection methods are unmatched in the industry. From a vulnerability perspective, the team maintains and analyzes one of the world's most comprehensive databases of known security vulnerabilities, with more than 70,000 entries, including detailed analyses of every notable public vulnerability disclosure since 1994. From a threat perspective, the team tracks billions of security incidents daily, monitors millions of spam and phishing attacks, and has analyzed billions of web pages and images. X-Force maintains a global research footprint that delivers unequaled security research and threat mitigation technology to JSA Series Secure Analytics portfolio users.

In addition to relying on its own findings, the X-Force team collects data from multiple research sources, researching all publicly disclosed vulnerabilities, consuming commercial vulnerability data, and monitoring the underground for zero-day vulnerabilities. It also collaborates with the world's leading businesses and governments, vertical sector information sharing and analysis centers, global coordination centers, and other product vendors to provide complete data. Finally, from an engineering perspective, the team analyzes proof of concepts and public exploit code. By monitoring global Internet threats around the clock and updating the IBM Internet Security Systems AlertCon resource center in real time, the X-Force team helps keep JSA Series Secure Analytics Appliances users abreast of the current global Internet threat level at all times.

Juniper users gain access to all of these benefits when they add the proprietary threat insights of X-Force Threat Intelligence to the JSA Series Secure Analytics portfolio of products.

Enhance Juniper Secure Analytics Capabilities with X-Force

X-Force Threat Intelligence leverages the X-Force research and development team's skills and infrastructure to provide additional insight into and context for security situations that involve IP addresses of a suspicious nature. By categorizing IP addresses into segments such as malware hosts, spam sources, and anonymous proxies, this IP reputation data can be incorporated into the JSA Series Secure Analytics Appliances' rules, offenses, and events. This allows for capturing events more quickly and accurately than previously possible, as well as for capturing them in a way that provides additional understanding for further analysis.

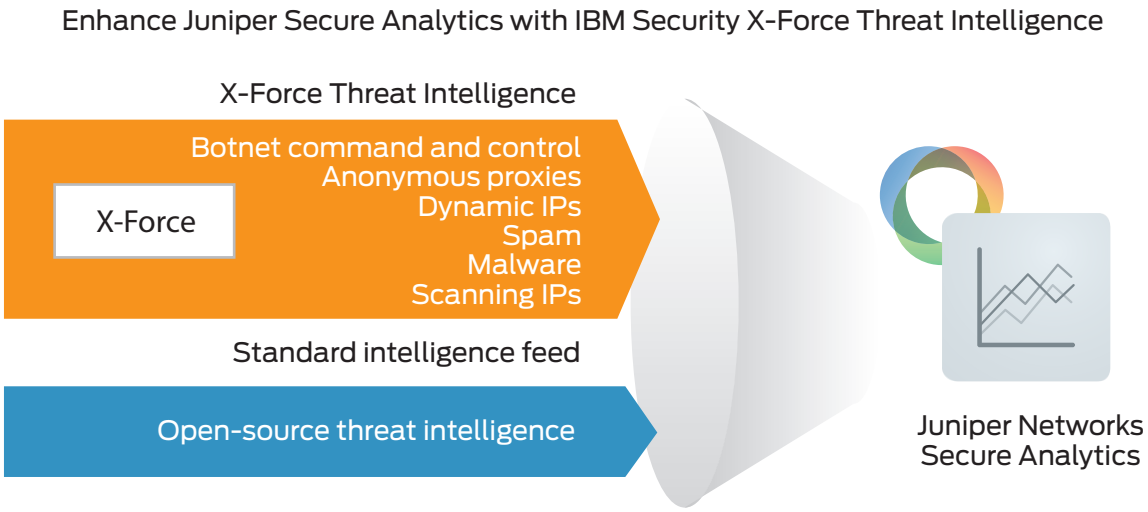

Figure 2. Using X-Force Threat Intelligence with JSA Series Secure Analytics Appliances provides valuable capabilities beyond those included in the standard Juniper intelligence feed, such as frequent updates, in-house analytics, confidence ranking, and comprehensive coverage.

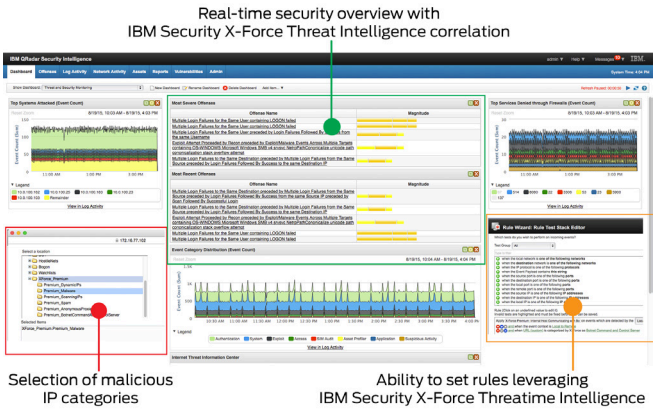

Figure 3. Leveraging X-Force Threat Intelligence in conjunction with the JSA Series Secure Analytics portfolio's rules enables users to more precisely detect dangerous network activity.

X-Force IP reputation data is constantly updated and maintained, and the content in these feeds is given relative threat scoring. This enables users of JSA Series Secure Analytics Appliances to prioritize incidents and offenses generated through this content. The data from these intelligence sources is automatically incorporated into the JSA Series Secure Analytics family's correlation and analysis functions and serves to greatly enrich threat detection capabilities with up-to-the-minute Internet threat data. Any security event or network activity data seen involving these addresses is automatically flagged, adding valuable context to security incident analyses and investigations.

Users can also incorporate the latest X-Force security threat advisories and informational updates into the JSA Series Secure Analytics dashboard. This dashboard includes the current X-Force AlertCon level, which provides users with a quick and concise indicator of current Internet threat conditions.

Using X-Force Threat Intelligence with JSA Series Secure Analytics Appliances is simple and fast—once users have added these threat insights, they will immediately begin receiving advanced threat data automatically and seamlessly.

Get the Most Value Out of Additional Threat Intelligence

X-Force Threat Intelligence provides vulnerability coverage across a wide range of use cases, including:

Security issue	Insight provided
A series of attempted logins from a dynamic range of IP addresses	Malicious attacker
An anonymous proxy connection to a business partner portal	Suspicious behavior
A connection from a non-mail server with a known spam host	Spam contamination
A connection between an internal endpoint and a known botnet command and control	Botnet infection
Communication between an endpoint and a known malware distribution site	Malware attack

By adding the dynamic information from X-Force Threat Intelligence to the analytical capabilities of JSA Series Secure Analytics Appliances, users can gain more intelligent and accurate security enforcement. This additional insight from X-Force Threat Intelligence enables Juniper users to apply this valuable data in real time to more closely monitor—and tightly secure—their environments.

Features and Benefits

- Automatically feed IBM X-Force data into JSA Series Secure Analytics Appliances
- Enrich Juniper's threat analysis capabilities with up-to-the-minute data on Internet threats
- Leverage the additional threat context provided by IBM Security X-Force Threat Intelligence to gain deeper insight—and greater protection
- Prevent or minimize the impact of today's complex and serious security attacks

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

To learn more about how IBM Security X-Force Threat Intelligence and Juniper Networks JSA Series Secure Analytics Appliances can benefit your organization, please contact your Juniper Networks representative and visit www.juniper.net.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

1000545-001-EN May 2016