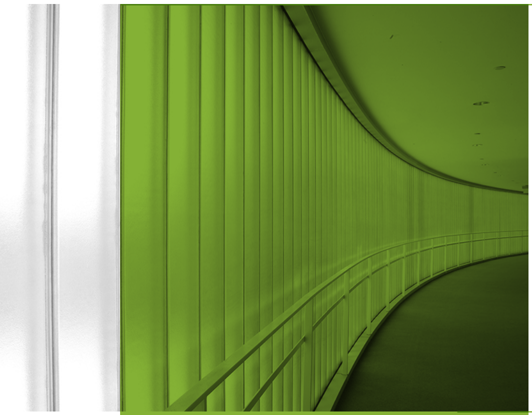

SECINTEL WITH AMAZON GUARDDUTY

Creating threat-aware networks with intelligence from SRX Series Services Gateways, Juniper SecIntel, and Amazon GuardDuty

Challenge

Building a truly threat-aware network requires comprehensive security intelligence when workloads are in AWS. To block malicious traffic, organizations that subscribe to services such as Amazon GuardDuty need a threat-aware network that continuously provides threat intelligence to all connection points.

Solution

Juniper SecIntel provides security threat intelligence feeds that aggregate data from multiple sources, including Juniper devices and Amazon GuardDuty, to deliver curated, consolidated, actionable intelligence.

Benefits

- *Leverages the security intelligence from the public cloud across all environments*
- *Enables the application of a uniform security policy on all SRX Series Services Gateways*
- *Assists in the evolution of a truly threat-aware network*

Comprehensive security intelligence is difficult when workloads are in Amazon Web Services (AWS). Organizations that subscribe to services such as Amazon GuardDuty can enrich their security intelligence with Juniper Networks® SRX Series Services Gateways and Juniper SecIntel, Juniper's security intelligence feed, to create a threat-aware network that blocks threats and delivers actionable insights.

The Challenge

Today, organizations with workloads in Amazon Web Services (AWS) count on the Amazon GuardDuty service to continuously monitor their AWS deployments for malicious activity and unauthorized behavior. Security teams rely on the threat intelligence provided by the service to either block or log access from the source. Now, this feed from Amazon GuardDuty can be ingested into the Juniper Networks SRX Series Services Gateways either directly from an Amazon S3 bucket or in the form of security intelligence (SecIntel) feeds from Juniper® Advanced Threat Prevention Cloud. In the latter scenario, the integration with SRX Series firewalls enables Amazon GuardDuty findings to be exported into Juniper ATP Cloud as a third-party feed. The virtual and physical SRX Series devices enrolled with Juniper ATP Cloud then receive the findings as part of the SecIntel feed. With this integration, network administrators can enforce uniform security policies across their SRX Series deployments, wherever those firewalls reside.

Juniper Networks SecIntel Solution with Amazon GuardDuty

Juniper SecIntel helps organizations create a threat-aware network by providing threat intelligence to all connection points across the network to block malicious traffic. An organization with workloads in a public cloud can subscribe to the Amazon GuardDuty service, which identifies unexpected and malicious activity within their AWS environment. The findings from Amazon GuardDuty can then be a part of the feeds provided by SecIntel. Using AWS Lambda scripts, the GuardDuty threat findings are exported to Juniper Advanced Threat Prevention cloud-based service, which consolidates the findings from GuardDuty and many other sources to provide updated and current protections that help secure networks from threats.

Features and Benefits

- **Curated threat intelligence**. SecIntel uses curated threat feeds provided by Juniper Threat Labs, including malicious IPs, URLs, domains, and GeoIP. The information included within SecIntel is scrubbed and validated while being constantly updated in real time. Now, augmented with the threat findings from Amazon GuardDuty, SecIntel delivers continuously updated and curated threat data to increase threat coverage and reduce false positives.
- **Uniform security policy across all clouds, public or private**. By ensuring that threat feeds are uniform across all SRX Series devices, be it the Juniper Networks vSRX Virtual Firewall deployed in AWS or a Juniper Networks SRX5400 Services Gateway deployed as a perimeter firewall on premises, the network security admin can ensure there is a single policy to block malicious IPs at all connected points across the network. This process is a key enabler of the threat-aware network.
- **Multiple integration options**. The findings from Amazon GuardDuty can be ingested directly into the SRX Series devices from an AWS S3 bucket or as part of the SecIntel feed from Juniper ATP Cloud, providing customers with flexible deployment options.
- **Automated solution**. Easily deployable AWS Lambda scripts with detailed workflows allow for an automated solution. Once enabled, the security operations team can rest easy knowing it has a completely automated, threat-aware, intelligent, and secure network.
- **Threat-aware network**. SecIntel provides the ability to identify and either passively monitor or block known threats. This process can be done at the network edge, throughout the network core, and at the access layer, which allows for the addition of security to the networking stack natively within the network infrastructure.

Solution Components

A truly secure network must be threat aware. Threat-aware networks require both deep network visibility and the ability to enforce policies at every connection point. Firewall orchestration—including Juniper's patented one-click automation—is one example of a simple management option that empowers administrators to safeguard users, applications, and infrastructure by enabling the automatic creation and distribution of policies that can block traffic at the port level. That is the power of SecIntel.

SecIntel provides security threat intelligence feeds that aggregate data from multiple sources, including Juniper devices, to deliver curated, consolidated, actionable intelligence. These feeds are delivered to SRX Series Services Gateways deployed across the organization. These threat intelligence feeds include threat information curated by Juniper Threat Labs and accessed via the Juniper Advanced Threat Prevention cloud-based service, as well as third-party threat data and threat information covering industry-specific threats that customers can integrate into their solutions.

Amazon GuardDuty provides this type of third-party threat information. Offered by Amazon for its customers, this service continuously monitors the organization's network for malicious activity and reports the threats in the form of security findings in the GuardDuty console. Now, using an AWS Lambda script and AWS CloudWatch events, these findings can be exported to the Juniper ATP Cloud as a third-party security feed. Juniper ATP Cloud consolidates this and findings from other sources and sends this security intelligence to SRX Series Services Gateways, which are subscribed to the threat feeds from Juniper ATP Cloud to benefit from the curated threat intelligence feed.

Verified by NSS Labs during the recent Data Center Security Gateway Test, Juniper achieved a recommended rating and scored greater than 99% for exploits and 100% on evasions identified and blocked. Juniper ATP Cloud, which includes SecIntel, is tested quarterly by ICSA Labs for Advanced Threat Defense. Juniper consistently achieves nearly 100% efficacy catch rates on the latest malicious threats.

Integrating the security findings from Amazon GuardDuty into the SRX Series gateways can be done in two different workflows. The AWS Lambda scripts that enable both workflows can be found at https://github.com/Juniper/vSRX-AWS/tree/master/SRX-GD-Threatfeed.

Directly Ingest the Threat Findings from an Amazon S3 Bucket

In this workflow, the threat findings from Amazon GuardDuty notify an AWS CloudWatch event that triggers a Lambda script. The script fetches the security findings from Amazon GuardDuty and posts them in the Amazon S3 bucket. Appropriate AWS IAM roles must be specified for the Lambda script to execute and access AWS GuardDuty and the AWS S3 bucket. The SRX Series devices must be configured to receive the feeds from the S3 bucket URL. The AWS S3 bucket must have appropriate read permissions for the SRX Series devices to access the threat feeds.

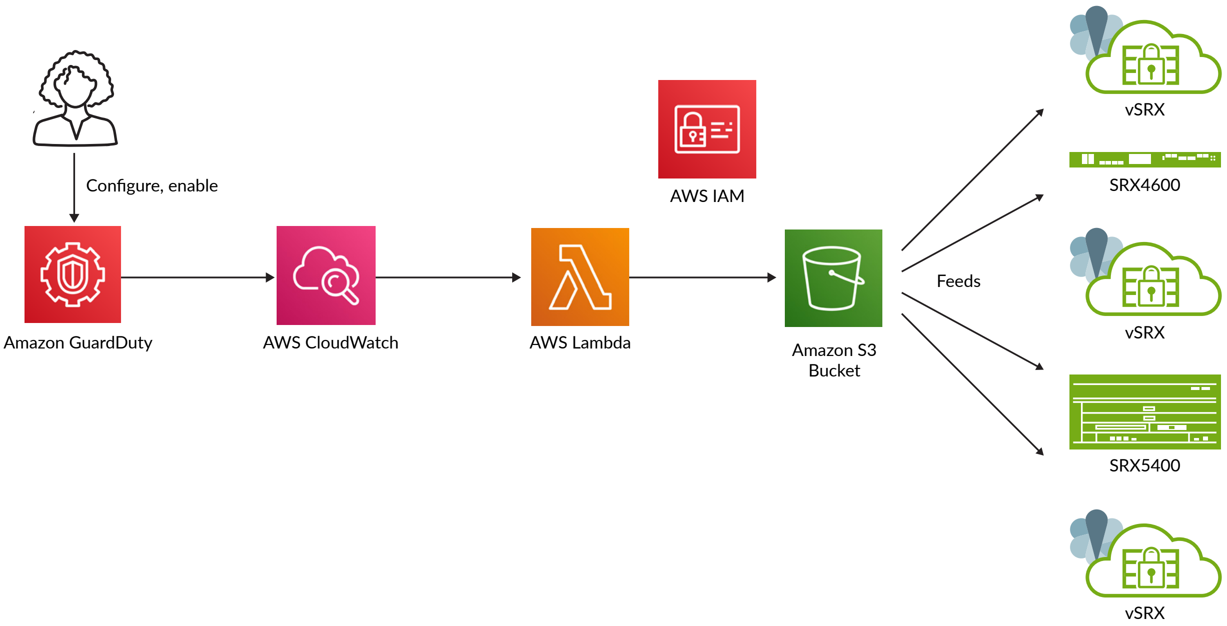

Figure 1: Workflow for direct ingestion of threat feeds into the SRX Series devices

Augment the Juniper ATP Cloud Threat Feeds with Amazon GuardDuty Findings

Alternatively, SRX Series devices that have enrolled with Juniper ATP Cloud can leverage threat findings from Amazon GuardDuty and can be downloaded as SecIntel feeds. In this scenario, the AWS Lambda script uses open APIs available from Juniper ATP Cloud to post the threat findings from Amazon GuardDuty as a third-party feed. The SRX Series devices fetch the feeds as part of their SecIntel updates that are downloaded at a preconfigured interval. The Juniper ATP Cloud is a licensed service provided by Juniper.

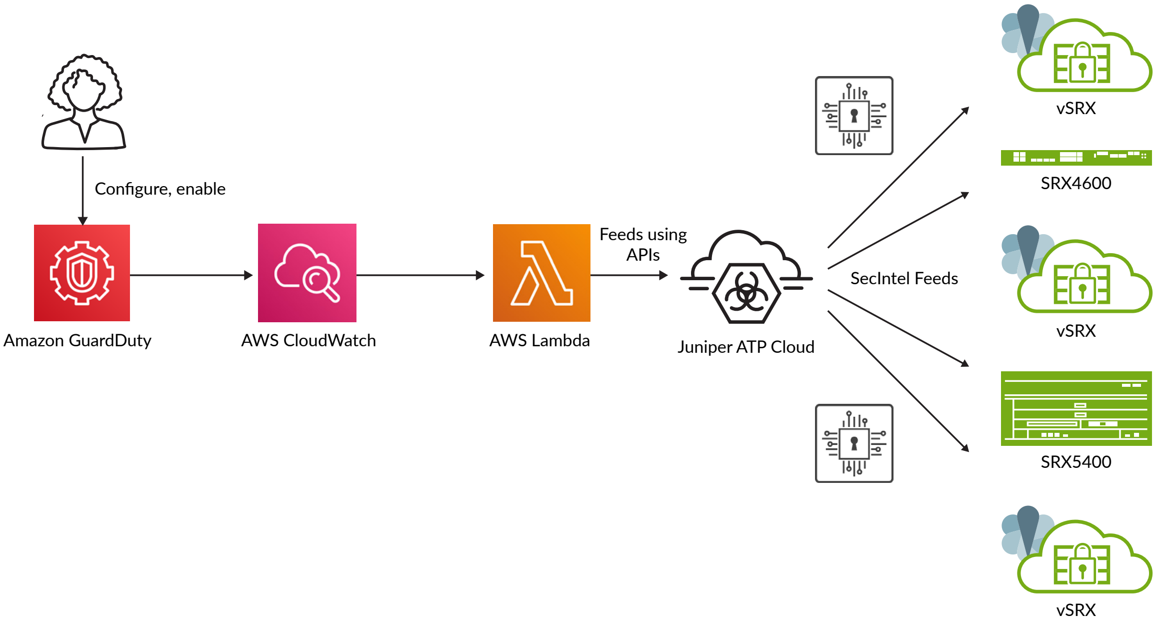

Figure 2: Augment Juniper ATP Cloud with findings from Amazon GuardDuty

To find more detailed information on the steps to enable SecIntel with Amazon GuardDuty for both workflows, please refer to the technical documentation.

Summary—SecIntel Enables a Threat-Aware Network by Providing Timely and Actionable Security Intelligence to SRX Series Gateways

The findings from Amazon GuardDuty now augment the threat feeds in SecIntel enabling visibility into threats from the network and cloud. Customers can enforce consistent policies wherever their applications may reside—on premises, in the cloud, or anywhere else. SecIntel, a critical component of Juniper Connected Security, helps customers build a truly threat-aware network.

Next Steps

To learn more about Juniper's security solutions, please visit us at www.juniper.net/us/en/products-services/security and contact your Juniper account representative.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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: +31.207.125.700
Fax: +31.207.125.701

Driven by Experience™