Scalable, Flexible, Automated Security for IoT Deployment

Protect Data, Assets, and Critical Infrastructure with Real-Time Visibility, Detection, and Threat Remediation

Challenge

The volume and variety of IoT devices makes security a significant challenge. Most IoT endpoints have limited footprints for running security functions, security personnel are scarce, and zero-day vulnerabilities are exploding. Traditional perimeter-based security solutions are not enough.

Solution

Juniper's Software-Defined Secure Network lets you employ your entire existing network as a unified cybersecurity platform that leverages analytics, machine learning, and automation to improve your security posture defending against the explosive growth of IoT risks.

Benefits

- End-to-end visibility into IoT devices, networks, and applications
- Smart detection of known and unknown threats with behavior analytics and machine learning
- Real-time remediation and control through automated policy enforcement
- Meets regulatory compliance requirements such as NERC CIP, HIPPA, and GDPR
- Scalable, flexible, automated protection anywhere and everywhere

In 2018, the Internet of Things (IoT) will experience an important inflection point when many enterprises will move their IoT deployments from early experimentation to business scale.[1]

This is a critical milestone, marking the IoT's entry into the mainstream. Gartner, Inc. forecasts that by 2020, 20.4 billion connected things will be in use worldwide.[2] Likewise, IHS Markit predicts the number of connected IoT devices will surge to 125 billion by 2030.[3]

As the scale of IoT endpoints grows unabated, the attack surface grows right along with it, providing cyber criminals with ample opportunities to innovate their exploits. It is no wonder security is the number one concern for businesses considering IoT adoption.

The Challenge

In the early days of the IoT, security was merely an afterthought. Today's users are paying the price for that negligence. AT&T has reported a 3198% increase in the number of attackers scanning IoT devices for vulnerabilities over the past three years.[4] In 2016, approximately 100,000 IoT devices were infected by the Mirai malware, turning them into botnets that launched a slew of 1.2 Tbps distributed denial of service (DDoS) attacks against Domain Name System (DNS) service provider Dyn. These attacks resulted in an outage that lasted more than two hours and affected major Web service providers such as Twitter, Spotify, and Github.

It's been estimated that for companies with annual revenues of $2 billion or more, the potential cost of one IoT breach is more than $20 million.[5] In addition to financial loss, IoT breaches can also potentially result in physical damages and even threaten people's safety. In 2015, Chrysler recalled 1.4 million vehicles after hackers demonstrated they could remotely hijack a Jeep's digital systems. That same year, a Russian IoT malware targeted Ukraine's electrical grid, cutting off power to 230,000 people.[6]

[1] https://go.forrester.com/blogs/predictions-2018-iot-will-move-from-experimentation-to-business-scale/
[2] https://www.gartner.com/newsroom/id/3598917
[3] https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
[4] https://www.business.att.com/cybersecurity/archives/v4/emerging-vulnerabilities/
[5] https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security
[6] https://www.forbes.com/sites/thomasbrewster/2015/07/24/chrysler-recall-exploit/

Figure 1: The Internet of Things

Unique Security Challenges of IoT

Compared to traditional connected devices such as laptops, mobile phones, and tablets, IoT-connected devices have their own unique security challenges. For instance:

- Many IoT devices are small, low power, and inexpensive, with limited compute and memory for accommodating security functions. This is why the network itself is so critical to mitigating IoT threats.
- Security operations teams are challenged to keep pace with the exponential growth of IoT devices. Therefore, security automation is a must have for IoT deployment at scale.
- The variety of IoT devices (types, operating systems, manufacturers, etc.) means there are many unknown zero-day vulnerabilities that hackers can exploit. Organizations must leverage security analytics and machine learning to detect unknown threats and defend against these IoT attacks.
- Traditional perimeter-based security assumes everything outside the firewall is untrustworthy but everything inside is fine. This approach doesn't consider IoT scenarios where inside devices get compromised. A new perspective is required.

The Juniper Networks IoT Security Solution

The Juniper IoT security solution includes the following components.

- **Juniper Networks® SRX Series Services Gateways and vSRX/cSRX Virtual and Container Firewalls:** Juniper Networks physical SRX Series and virtual vSRX Services Gateways provide next-generation firewall (NGFW)-level protection with integrated application awareness, intrusion prevention, and role-based user controls, as well as best-in-class unified threat management (UTM) to protect business assets. The SRX Series and vSRX firewalls can be centrally managed via the Juniper Networks Junos Space® Security Director management application.

  The cSRX Container Firewall runs with no guest OS overhead, has a considerably smaller footprint, and is easier to migrate or download. It uses less memory, and its spin-up time is measured in sub seconds—all leading to higher density at a lower cost, which is perfect for various IoT use cases.

  To learn more about the SRX Series next-generation firewalls, please visit www.juniper.net/us/en/products-services/security/srx-series/.

- **Junos Space Security Director:** Juniper's scalable and intuitive Security Director management application lets enterprise users make precise decisions and achieve end-to-end visibility into applications, users, and threats through their physical and virtual SRX Series firewalls. Offering a holistic view, rich security feature set, and easy-to-use actionable intelligence such as threat intelligence received from Juniper Sky™ Advanced Threat Prevention and Juniper Sky ATP Appliance (see below), Security Director lets you create security policies that allow you to take remedial action and block high-risk applications and threats. By offering single pane-of-glass management, an easy-to-use intelligent security rule creation wizard, and an auto-rule placement feature, Security Director allows you to create less complex security policies faster.

  Policy Enforcer, a component of Security Director, is a central intelligence module that communicates with multivendor network elements and security products to consolidate threat intelligence from different sources throughout the network, provide analytics, and enforce security policies globally—from the edge to the cloud.

  To learn more about Security Director, please visit www.juniper.net/us/en/products-services/security/security-director.

- **Juniper Sky Advanced Threat Prevention:** A cloud-based service integrated with Junos Space Security Director and SRX Series firewalls, Juniper Sky ATP delivers deep inspection capabilities, inline blocking, and actionable alerts, constantly adapting to an ever-changing threat landscape by leveraging real-time information from the cloud. Juniper Sky ATP's identification technology uses a variety of sophisticated techniques to quickly detect and prevent cyber attacks. These include:
  - Powerful machine learning algorithms
  - Dynamic analysis with techniques to trick malware into activating and self-identifying
  - Rapid cache lookups to speed up previous malware identification
  - Antivirus signature-based engine to identify known files
  - Static analysis that analyzes software code to identify possible dangerous fragments

To learn more about Juniper Sky ATP, please visit www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/.

- **Juniper Advanced Threat Prevention Appliance:** The Juniper ATP Appliance provides comprehensive on-premises protection against a sophisticated, ever-changing threat landscape.

  With traditional signature-based security tools, zero-day attacks often go undetected. Leveraging advanced machine learning and behavioral analysis, the Juniper ATP Appliance identifies existing and unknown advanced threats in near real time through continuous, multistage detection and analysis of Web, e-mail, and lateral-spread traffic.

  The Juniper ATP Appliance ingests feeds from multiple security devices, applies analytics to identify advanced malicious traits, and aggregates the events into a single comprehensive timeline showing all threats on the network. Security teams can quickly determine how the attack unfolded and easily prioritize critical alerts.

  To learn more about the Juniper ATP Appliance, please visit www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/.

- **Juniper Secure Analytics:** Juniper Networks JSA Series Secure Analytics Appliances combine, analyze, and manage an unparalleled set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—empowering companies to automate the analysis of large data sets and efficiently manage business operations from a single console. A key component of the SDSN platform, JSA Series Secure Analytics is also integrated with the Security Director central management software, providing real-time intelligence for quick threat remediation and direct policy enforcement across the network.

  To learn more about the JSA Series Secure Analytics portfolio, please visit www.juniper.net/us/en/products-services/cecurity/secureanalytics/.

Features and Benefits

Juniper's IoT security solution allows you to turn your network into a single, widespread enforcement domain, leveraging analytics, machine learning, and automation for real-time visibility, detection, and threat remediation.

- **End-to-End Visibility into IoT Devices, Networks, and Applications:** If you can't see it, you can't defend against it. This is why visibility is so critical.
- **IoT Device Visibility:** When an IoT endpoint connects to the network, the Juniper access switches leverage existing standards-based AAA (RADIUS/DHCP/AD/LDAP), as well as integration with network access control (NAC) and security technology partners such as ForeScout, Aruba ClearPass, and Impulse Point, to provide device profiling and onboarding. This gives customers considerable implementation flexibility, allowing them to choose wired and/or wireless, agent-based and/or agentless, and whether they want 802.1X support. You get complete visibility into IoT devices and network traffic, allowing you to apply security policy and implement IoT network segmentation.
- **IoT Network Visibility:** As a leading Security Information and Event Management (SIEM) solution, JSA Series Secure Analytics continuously collects, aggregates, stores, and analyzes event data from Juniper and third-party network devices, providing a complete picture of how the network infrastructure is behaving in real time to identify unusual behavior. As the number of network objects grows, along with the amount of metrics they generate, the traditional pull model used by SNMP and the CLI—which requires additional processing to perform regular polling—limits scalability. The Junos Telemetry Interface (JTI), a feature of the Juniper Networks Junos operating system, overcomes these limits by adopting a push model to deliver data asynchronously, eliminating the need for polling. A request for data is sent once by a management station to stream periodic updates. As a result, JTI is highly scalable and supports monitoring thousands of network objects.
- **IoT Application Visibility:** Juniper Networks AppSecure, a core feature of the SRX Series NGFWs, provides a powerful mechanism for instantly recognizing even new applications by using techniques that identify all applications traversing the network, regardless of port, protocol, or encryption method. Offering deep application visibility and control, AppSecure provides the context that links application use to a user, regardless of location and device. Designed to understand application behaviors and identify vulnerabilities, AppSecure blocks application-borne security threats before they can do any damage. Additionally, Junos Space Security Director provides an easy and intuitive way to identify which applications use the most bandwidth, have the most sessions, or are most at risk.
- **Smart Detection of Known and Unknown Threats with Behavior Analytics and Machine Learning:** The sheer volume of IoT devices and data exchanges can make threat detection extremely challenging.

  The SRX Series devices include an intrusion prevention system (IPS) feature that provides complete protection against a broad range of known security exploits in applications, databases, and operating systems. SRX Series Services Gateways constantly look for new exploits against newly discovered vulnerabilities, ensuring that network protection is up-to-date against the latest attack methods.

For unknown threats such as zero-day attacks, Juniper's advanced threat prevention offerings—the cloud-based Juniper Sky ATP and the Juniper ATP Appliance for on-premises deployments—provide advanced threat detection through machine learning and behavioral analytics. Customers gain the ability to baseline normal IoT device behavior in order to detect behavioral anomalies, defend against attacks, and prevent broad IoT threat outages by turning "unknown" threats into known attacks.

- **Real-Time Remediation and Control Through Automated Policy Enforcement:** If we examine security incidents from the past, we find that most systems did actually detect the attack and send alerts. However, it frequently took hours or, in some cases, days to react manually; by then, the damage was already done. With IoT at scale, security automation is necessary for operations teams to keep pace with growth. And different scenarios require different treatments; for example, if a surveillance camera gets infected, you can simply disconnect it from the network, while an attack on, say, an automotive manufacturing line requires an unplanned shutdown that costs the company $22,000 per minute, or $1.3 million per hour[7].

[7] www.businessinsider.com/what-1-minute-of-unplanned-downtime-costs-major-industries-2016-9

Juniper's SDSN solution lets you define comprehensive and flexible policies to accommodate different IoT scenarios and make automated policy enforcement decisions consistent across any vendor, any cloud, anywhere, simplifying overall security operations. For example, when an IoT device gets infected by malware and attempts to initiate communication with a Command and Control (C&C) server, Juniper Sky ATP or the Juniper ATP Appliance detects this abnormal behavior and reports it to Security Director Policy Enforcer immediately. Policy Enforcer automatically applies a predefined response to quarantine the infected device, preventing the malware from spreading and remediating the threat—all in real time.

The remediation workflow unfolds as follows, and as shown in Figure 2:

- An infected IoT device attached to the network attempts to download a restricted file or launches an attack on critical infrastructure.
- The unauthorized download attempt is logged by JSA Series Secure Analytics and the ATP Appliance, then reported to Junos Space Security Director Policy Enforcer.
- Policy Enforcer applies an access control list/network access control rule to the affected switch port or Wi-Fi access point to quarantine the host, quickly remediating the threat.

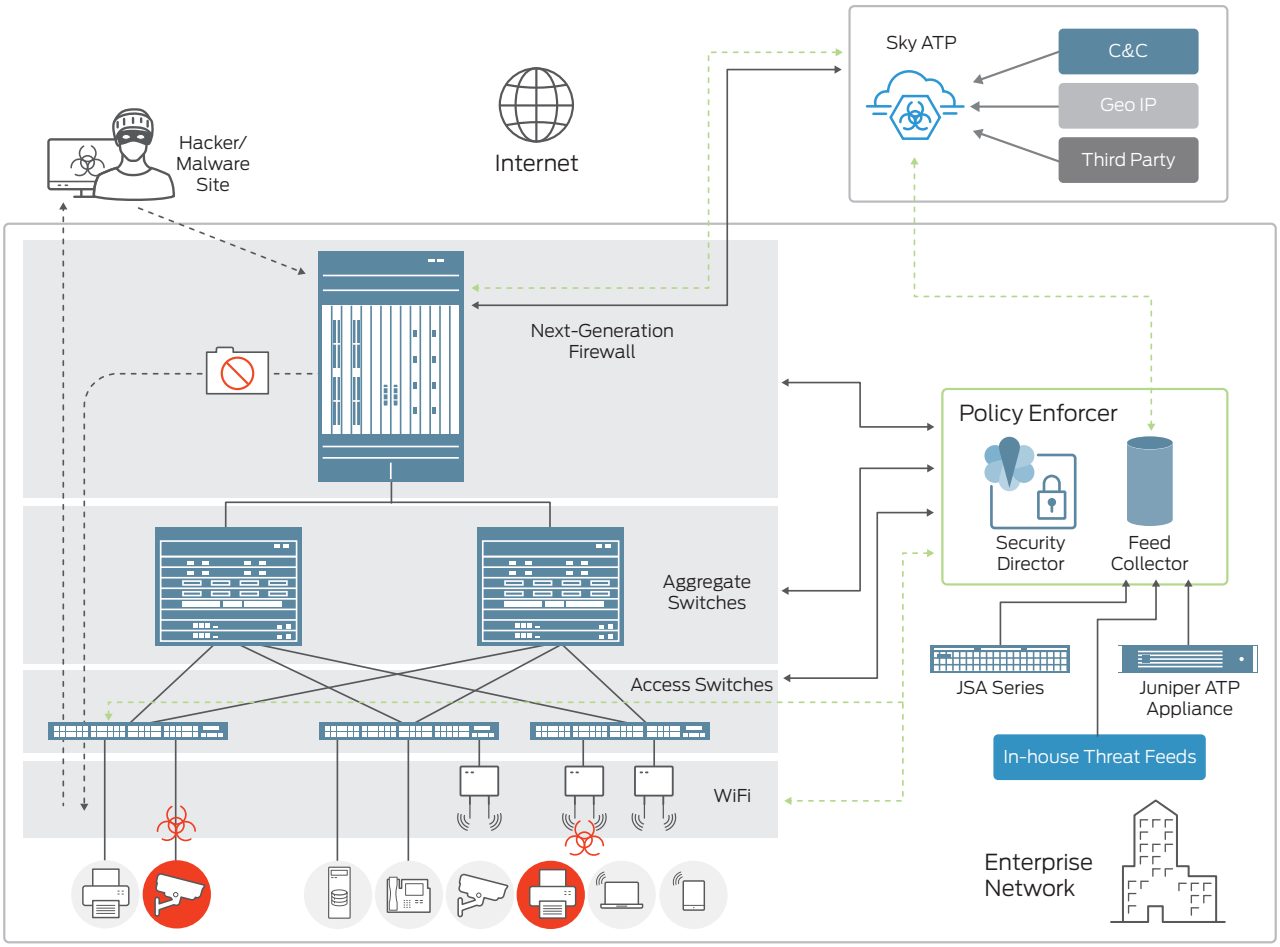

Figure 2 : Juniper IoT security solution architecture

- **Meeting Regulatory Compliance Requirements such as NERC CIP, HIPPA, and GDPR:** With more devices connected to the enterprise network, each generating more and more data, the need to comply with regulatory requirements grows ever more critical.

  In addition to traditional IP, as well as legacy protocols such as MODBUS for industrial Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), a number of new IoT-specific protocols such as Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) are also finding their way into the mainstream. In order to meet compliance requirements, organizations must be able to identify communications sources and control traffic based on the IoT protocols being used. Juniper's IPS, available on SRX Series Services Gateways, supports most IoT application signatures, as well as allowing end users to write custom application signatures to meet their specific needs. Security Director makes it easy to identify which applications are being used and provides the ability to modify application signatures.

  The JSA Series devices make regulatory compliance easy and automatic through powerful collection, correlation, and reporting tools. It conducts regular network scans and maintains detailed audit trails to facilitate compliance with federal or industry regulations. The JSA Series supports multiple regulations and security best practices, and includes more than 500 out-of-the-box compliance-driven report templates to meet specific regulatory reporting and auditing needs.

- **Scalable, Flexible, Automated Protection Anywhere and Everywhere:** While many IoT scenarios face similar security vulnerabilities as traditional IT environments, the sheer number of IoT devices dramatically increases scalability requirements. IoT sensors can create literally millions of short sessions to exchange information with IoT applications. In addition, a large number of IoT devices will be located in remote places; some may even be constantly moving. The traditional concept of "perimeter" no longer applies in the context of IoT. Threats will be coming from anywhere, and security protection needs to be applied everywhere.

  The SRX4000 and SRX5000 lines of Services Gateways, already deployed in critical infrastructure such as those protecting large power grids in North America, deliver the high connections-per-second and session capacity required to support these sessions in large-scale IoT deployments. The flexible physical, virtual, and containerized SRX Series form factors, large and small, means you can place them wherever you want, from the IoT edge such as a mobile-edge computing (MEC) server or IoT gateway, to the inside of a car, to any cloud, whether public, private, hybrid, or multicloud. Policy Enforcer lets you consistently apply automated security policies across not only Juniper but also third-party equipment, giving you true holistic protection.

Summary—Security for IoT at Scale Requires a Paradigm Shift

As you adopt IoT technologies for your organization with deployment at scale as a next step, security must be addressed holistically. IoT breaches mean big financial loss, reputational damage, and a threat to people's safety.

When you scale deployment, the sheer volume and variety of IoT devices and their data exchange makes security a significant challenge. Most IoT endpoints have limited resources to run security functions, making the network's role in mitigating risk ever more critical. For most organizations, security personnel are a scarce resource; with at-scale IoT deployments, it will be an enormous operational challenge for businesses to keep their systems safe. Cyber criminals will also continue to develop new exploits, especially explosive, unknown zero-day threats, making traditional perimeter-based security solutions insufficient.

IoT at scale requires a security paradigm shift. Unlike point products focused on single actions, Juniper's IoT security solution, the Software-Defined Secure Network, empowers you to make your entire network a unified cybersecurity platform that leverages analytics, machine learning, and automation to improve your security posture defending against expanding IoT risks. Juniper's SDSN is scalable, flexible, and automated, protecting your IoT data, assets, and critical infrastructure anywhere and everywhere.

Next Steps

For more information on Juniper security solutions, please visit us at www.juniper.net/us/en/products-services/security or contact your Juniper Networks representative.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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

3510636-002-EN Apr 2018