Technical Validation

Juniper Networks Automated Threat Detection and Remediation

Sky Advanced Threat Prevention and SRX Series Firewalls

By Jack Poller, Senior Analyst

July 2019

This ESG Technical Validation was commissioned by Juniper Networks and is distributed under license from ESG.

Contents

Introduction 3
Background 3
Juniper Networks Sky Advanced Threat Prevention and SRX Series Firewalls 3
Sky Advanced Threat Prevention 3
SRX Series Services Gateway 4
ESG Technical Validation 5
Getting Started 5
Infection, Detection, and Response 7
Administrative Resolution and Remediation 11
The Bigger Truth 12

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Introduction

This ESG Technical Validation is an evaluation of Juniper Networks Sky Advanced Threat Prevention (ATP) and SRX series next-generation firewalls with a focus on the effectiveness and efficiency of automated threat detection and remediation. As part of the validation process, ESG compromises an endpoint with malware and detects the attack using Sky ATP, causing the firewall to block the endpoint's north-south traffic and the local switch to block the endpoint's east-west traffic, disconnecting the endpoint from the network.

Background

ESG's annual technology spending survey revealed that cybersecurity has emerged as IT's top mandate, with 40% of organizations indicating that strengthening cybersecurity will be a top business driver for their technology spending in the next 12 months.[1]

These organizations may find improving aspects of cybersecurity to be problematic. According to ESG research, more than three quarters (76%) of organizations say that threat detection and response is more difficult today than it was two years ago. Respondents believe that the primary challenges toward threat detection and response include increasing threat volume and sophistication (34%), increasing threat detection/response workload (17%), increasing attack surface (16%), and increasing number of disparate threat detection/response tools (11%), along with the ongoing global cybersecurity skills shortage (8%).[2]

The percentage of respondents who believe *strengthening cybersecurity* will drive the most technology spending within their organization over the next 12 months.

The percentage of respondents who consider *threat detection and response* to be more difficult today than it was two years ago.

In practice, organizations deploy multiple, disparate tools from multiple vendors in their effort to detect and respond to threats, requiring analysts to log into a variety of systems to manage alerts and take protective actions. This leads to manual intervention, decelerating the detection, investigation, response, and remediation process, while increasing mean-time-to-respond (MTTR) and extending threat actor dwell time.

What is needed is a solution that aggregates the functionality of multiple point tools—a solution that simplifies the use and management of these tools by automating threat detection and response workflows. Eighty-two percent of survey respondents said that improving their threat detection/response is a high priority, and 87% stated that they had a formal plan and funding to improve threat detection and response.[3]

Juniper Networks Sky Advanced Threat Prevention and SRX Series Firewalls

Sky Advanced Threat Prevention from Juniper Networks works synergistically with Juniper Networks SRX Series Services Gateways to provide high performance network security and advanced threat mitigation with routing, switching, and WAN interfaces for virtual, distributed, and core locations.

Sky Advanced Threat Prevention

Juniper Networks designed Sky Advanced Threat Prevention (ATP) as a SaaS solution using real-time information from the cloud for anti-malware protection for the purposes of defending organizations against cyber-attacks, including advanced persistent threats (APT) and ransomware. Sky ATP's integration with SRX Series next-generation firewalls provides deep

[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.
[2] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.
[3] Ibid.

packet inspection and inline blocking of threats. To detect and prevent cyber-attacks, Sky ATP uses machine learning, dynamic analysis, anti-sandbox evasion techniques, static analysis, and antivirus signatures. Organizations deploying Sky ATP benefit from:

- **Cloud-based analysis**—potentially harmful files are sent to the cloud for advanced analysis to determine whether they are benign or malicious.
- **Malware remediation**—detection of malware is communicated to SRX series firewalls to block attacks.
- **Reporting and analytics**—the Sky ATP web interface can help simplify management including configuration and updates and provides reporting and analytics tools for visibility into threats and compromised systems.
- **Systems quarantine**—SRX series firewalls use information from Sky ATP to quarantine compromised systems.
- **Integrated threat intelligence**—real-time communication with Juniper Networks SecIntel threat intelligence service can share threat information to SRX Series firewalls for immediate action. Using open APIs, Sky ATP distributes third-party threat intelligence feeds to all ATP-subscribed SRX firewalls for immediate action, reducing the attack surface.
- **Command-and-control prevention**—Sky ATP communicates with SRX Series firewalls to prevent lateral movement of malware and bock communication with command-and-control servers.
- **Email and web analysis and remediation**—machine learning algorithms analyze email and web files to detect malicious attachments and files and block those files at the firewall, preventing email from being used as an attack vector.
- **Integrated management**—Sky ATP and SRX Series firewalls can be integrated into Juniper Networks Junos Space Security Director, an integrated application that unifies the management of all Juniper Networks devices and services into a single console. Using the Security Director, administrators can manage all phases of the security policy lifecycle for stateful firewall, unified threat management, intrusion prevention, application firewall, VPN, and NAT.

SRX Series Services Gateway

Juniper Networks SRX Series Services Gateways are next-generation firewalls available as virtual or physical appliances designed to support cloud, branch office, small, medium, and large enterprises; large data centers; and service providers. SRX firewalls are designed for:

- **Security for organizations of all sizes**—SRX firewalls are available in many form factors from all-in-one, integrated physical and virtual security networking devices to highly scalable chassis-based data center solutions.
- **Comprehensive threat protection**—can defend against known and unknown threats with a comprehensive suite of layered security services.
- **Performance and scalability**—scales to support up to 1Tbps throughput with up to 285 Gbps IMIX firewall, 90 million concurrent sessions, and 230 Gbps IPS.
- **Reliability**—continuous uptime via in-service hardware and software upgrades, redundant components, and up to six-nines reliability for nonstop business continuity, security, and application availability.

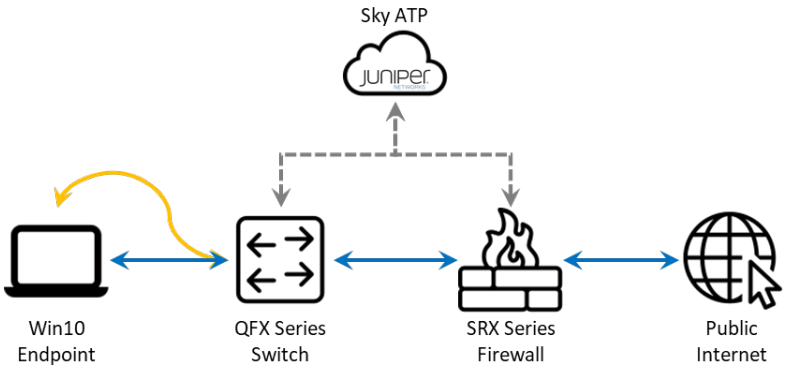
ESG Technical Validation

ESG's evaluation and testing of Sky Advanced Threat Prevention and SRX Series firewalls involved downloading a malicious file to an endpoint and validating that the file was sent by the SRX firewall to Sky ATP for evaluation. We focused on the automated detection, response, and remediation observed upon Sky ATP's detection of the infected endpoint.

Getting Started

To get started, we developed the test bed, as seen in Figure 1. This started with a Windows 10 endpoint running as a virtual machine. The endpoint was connected to a Juniper Networks virtual QFX Series switch on VLAN 4025 with the ability to switch to a separate connection on VLAN 3025. The QFX switch was connected to an SRX Series virtual firewall, and then to the public internet. The QFX switch and the SRX firewall were integrated with Sky ATP.

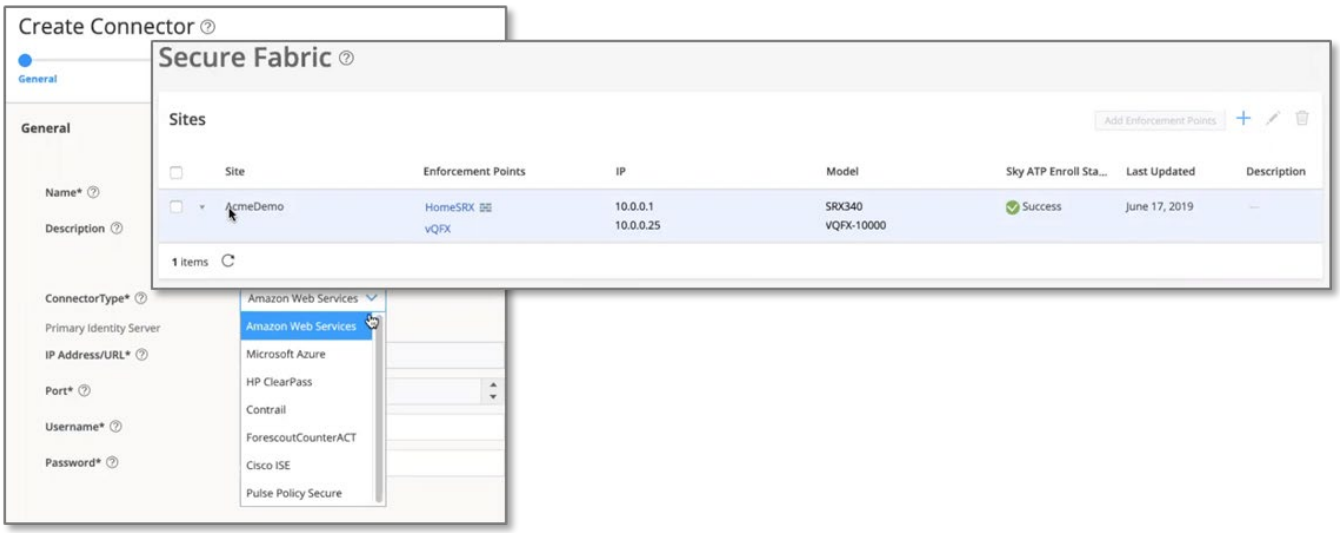
Figure 1. ESG Test Bed



Source: Enterprise Strategy Group

We used Juniper Networks Junos Space Security Director as a unified console to manage all the Juniper systems. As shown in Figure 2, we created a secure fabric enabling us to manage the firewall and switch as a single security domain. We also reviewed the ability to create connectors, which allows Sky ATP to connect to third-party services and switches, including AWS, Azure, ClearPass, Contrail, Forescout CounterACT, Cisco ISE, and Pulse Policy Secure.

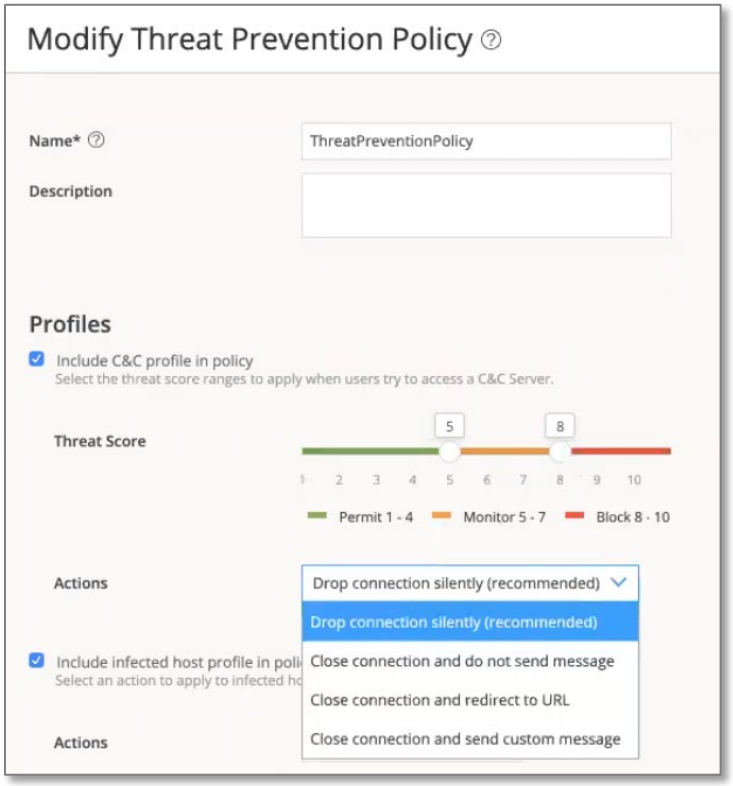
Figure 2. Sky ATP Secure Fabric and Connectors



Source: Enterprise Strategy Group

Next, we reviewed the Sky ATP Threat Prevention policy. As shown in Figure 3, Sky ATP enabled us to set predetermined actions based on threat scores. We chose to silently drop connections for any object with a threat score ≥ 8.

Figure 3. Sky ATP Threat Prevention Policy



Source: Enterprise Strategy Group

Why This Matters

Cybersecurity is complex and challenging, and the difficulty of detecting and preventing threats is exacerbated by the shortage of experienced or trained staff and the intricacy of coordinating multiple point tools from different vendors with different user experiences and interfaces. To address this complexity, organizations need a solution that simplifies cybersecurity infrastructure and processes.

ESG's validation revealed that Juniper Networks can simplify deployment—it was easy for us to create secure fabrics. Instead of setting policy individually on each device, we were able to define and set policies for groups of disparate systems. Defining security policies was just as easy using sliders to set thresholds and actions for differing levels of risk.

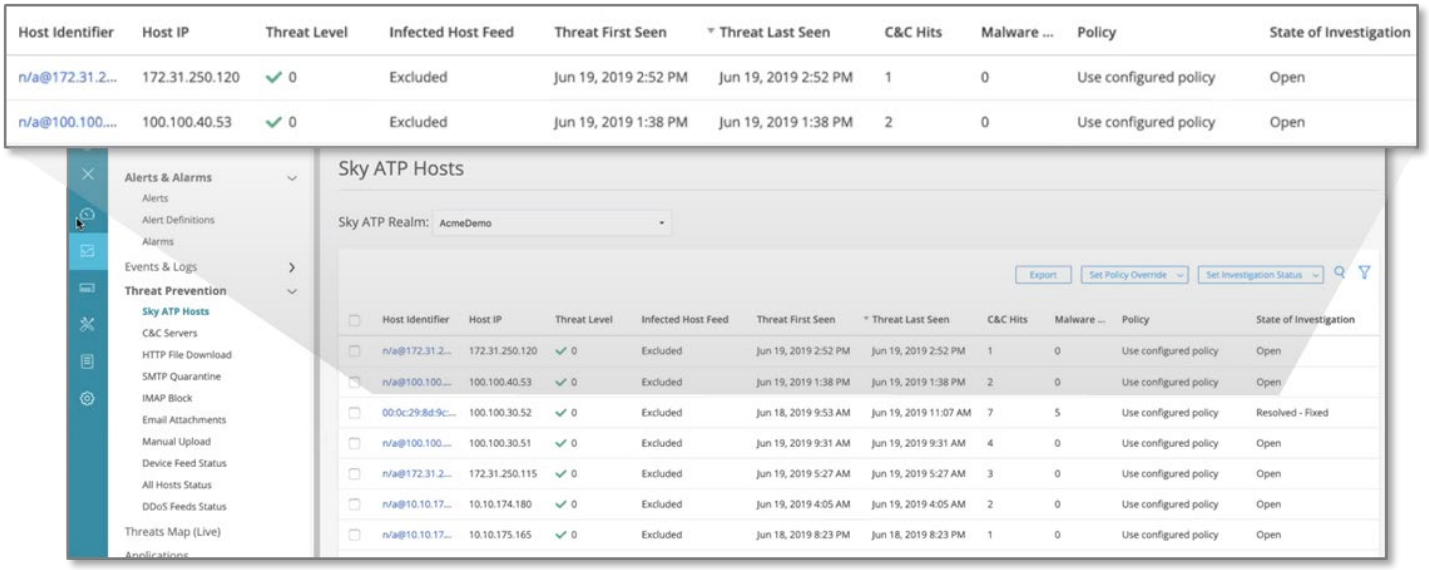
ESG also validated that we were able to define and set policy for arbitrary groups of virtual and physical Juniper Networks devices, simplifying security and network management in complex environments. Using Sky ATP and SRX firewalls, security analysts can spend less time configuring and managing tools, providing more time for critical activities such as responding to alerts and investigating threats and attacks.

Infection, Detection, and Response

ESG observed the process Juniper Networks uses to prevent threats when downloading files. We downloaded malware onto the endpoint and the SRX firewall sent the downloaded file to Sky ATP for analysis. When Sky ATP analyzed the file and determined that the file was malware and had infected the host, Sky ATP directed the SRX firewall and QFX switch to disconnect the endpoint from the network, preventing both north-south traffic (SRX firewall) and east-west traffic (QFX switch).

First, we reviewed the current state of the environment, as shown in Figure 4. Sky ATP included our test Windows 10 endpoint in the list of managed endpoints, and the endpoint, IP address 100.100.40.53, was ***excluded*** from the ***Infected Host Feed.*** Sky ATP uses this list to track compromised hosts.

Figure 4. Sky ATP Host Monitoring



Source: Enterprise Strategy Group

Next, we logged in to the virtual SRX firewall and virtual QFX switch and verified that the configuration enabled the endpoint to correctly communicate internally (east-west) and externally (north-south).

We logged in to the Windows 10 endpoint, and using a web browser, we navigated to a website hosting malware samples and downloaded three files containing malware.

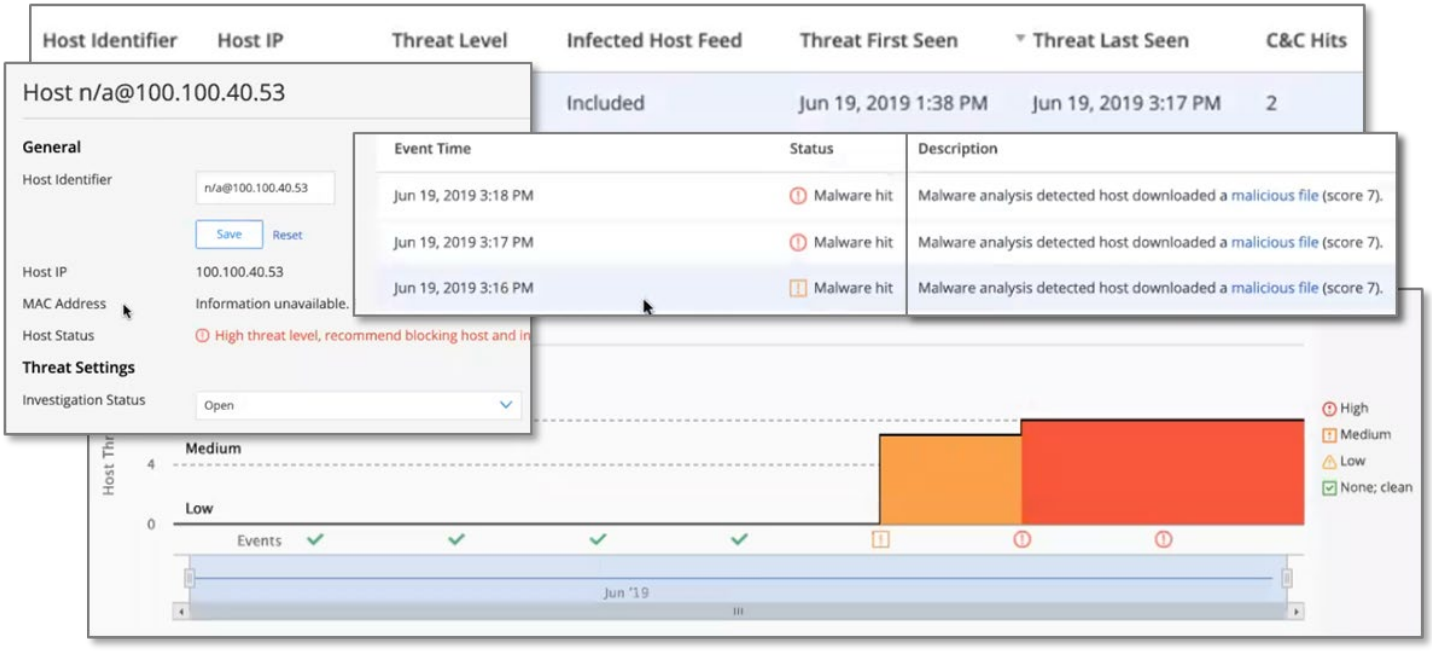
At the end of each file download, the SRX firewall sent a copy of the file to Sky ATP for analysis. Sky ATP applied a series of checks to each file including a comparison of the signatures against a malware database, static analysis using machine learning, dynamic sandbox analysis, and behavioral analysis. Using these checks, Sky ATP determined that each file contained malware. Based on the information gathered during the automated analysis phase, Sky ATP assigned a threat score to each file, and then computed a combined threat score for the endpoint.

Based on the combined threat score and the previously configured threat prevention policy (see Figure 3), Sky ATP set the host status to ***High threat level***, set the investigation status to ***open,*** and added the endpoint to the list of infected hosts—the ***Infected Host Feed***, as shown in Figure 5.

Following the typical workflow of a security analyst, we started our investigation by clicking on the host identifier link, which brought up additional information, including the list of malware infecting the host and a graph showing infections

over time. We found this information to be useful for starting our investigation, analyzing root causes, remediating endpoints, and resolving problems.

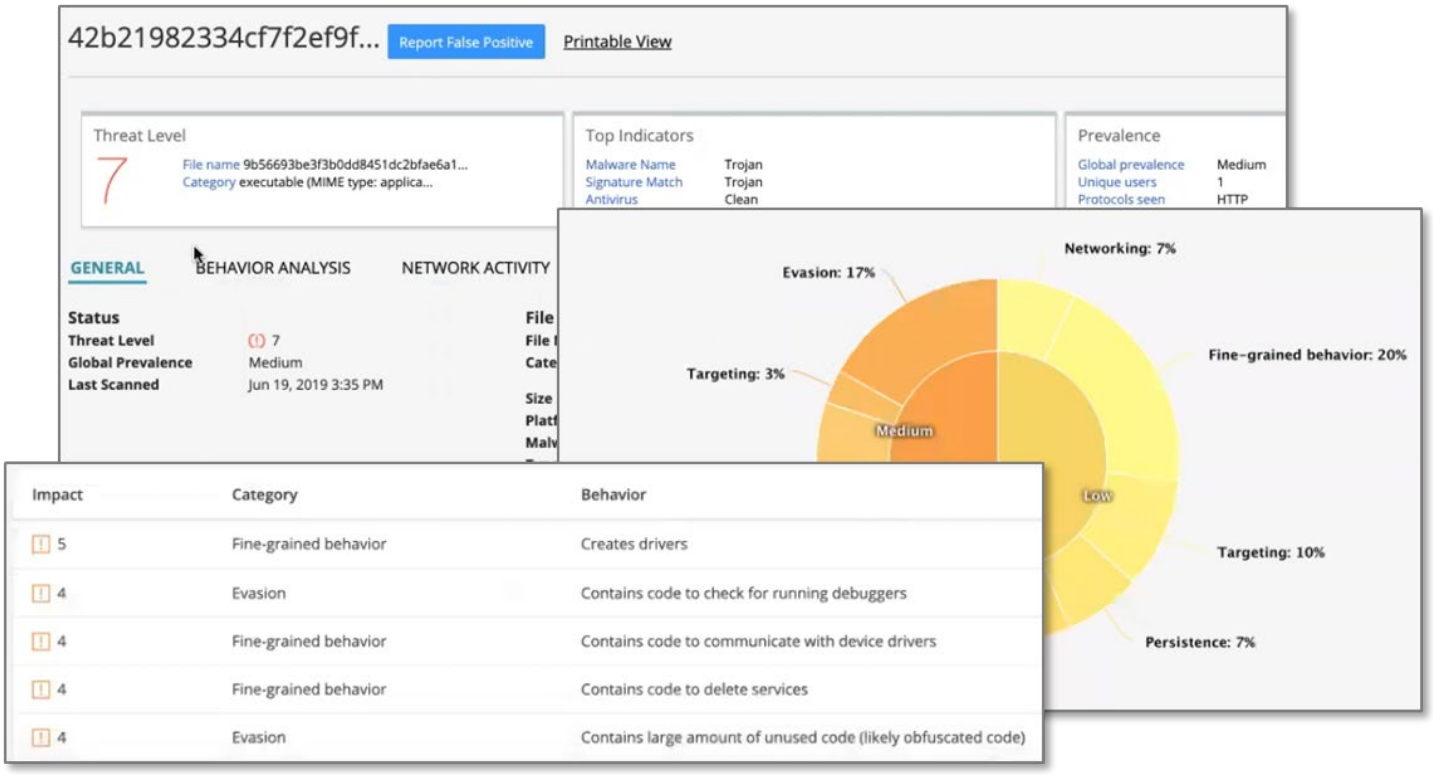
Figure 5. Infected Host Details



Source: Enterprise Strategy Group

Next, we clicked on the link for the downloaded malware and Sky ATP provided additional information on the infection, as shown in Figure 6. Summary information, including the threat level, top indicators, and prevalence of the threat, were provided at the top. A tabbed pane below the summary data provided general information. Clicking on the Behavior Analysis tab brought up a risk-based pie chart, categorizing the different behaviors based on risk. This malware was classified as a trojan, including medium risk evasion and targeting techniques along with low risk networking, evasion, targeting, and persistence techniques. Sky ATP also displayed a table with specifics on each of the identified behaviors. An additional tab provided a table detailing the malware's network activity.

Figure 6. Malware Details



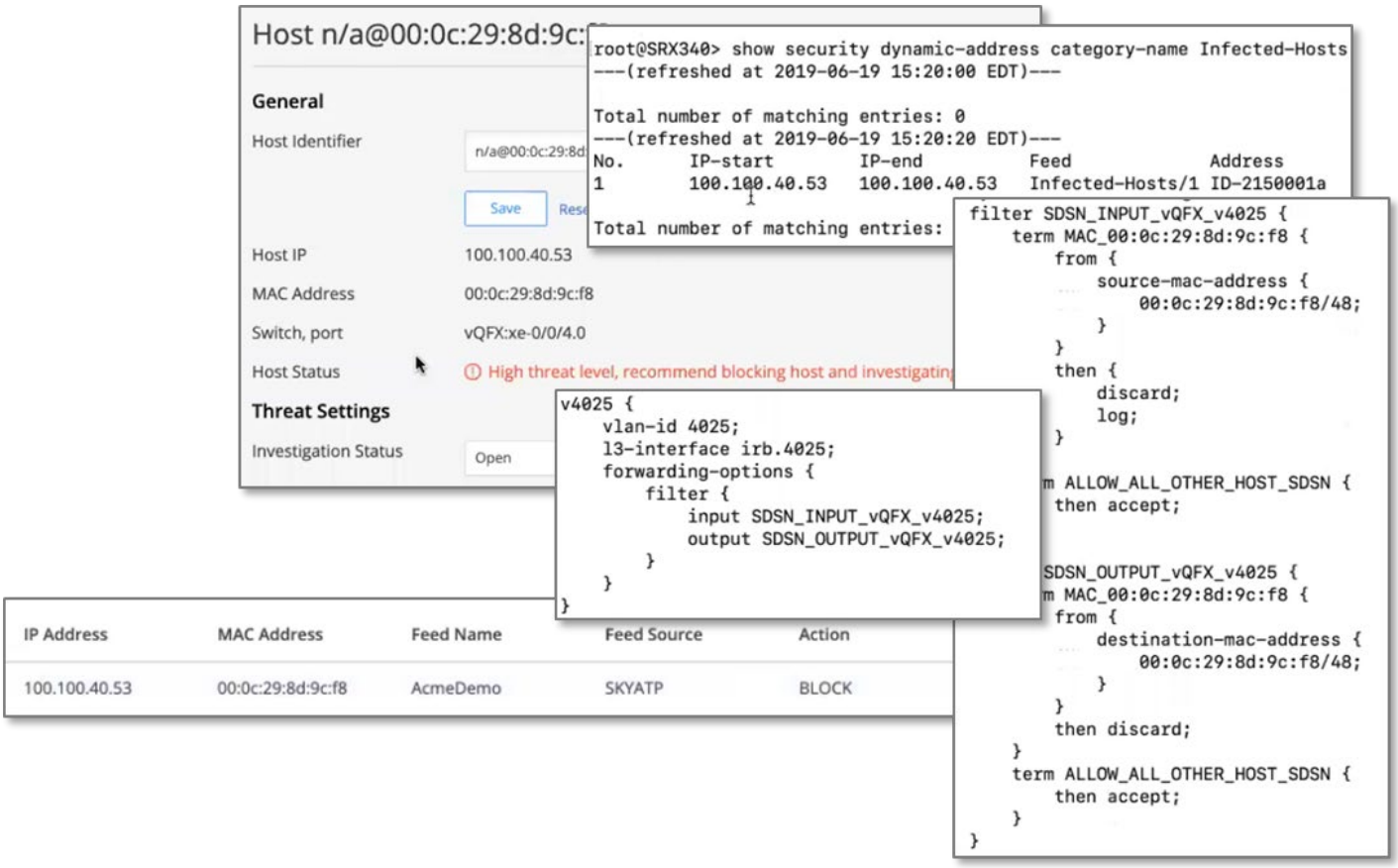
Source: Enterprise Strategy Group

Within five minutes of downloading the file, we determined that the endpoint had been isolated from the network—we could not ping internal or external IP addresses, thus demonstrating Sky ATP's automated threat remediation. Adding the endpoint to the infected host feed caused the SRX firewall to block the endpoint from north-south communication. In addition, the endpoint's DHCP lease was revoked and the endpoint lost its IP address.

Since the IP address was invalidated, Sky ATP updated its database to refer to the infected endpoint by its MAC address, as shown in Figure 7.

Using the built-in connector enabling Sky ATP to communicate with all Juniper Networks devices, Sky ATP told the QFX switch to partition the endpoint, preventing east-west traffic. The switch created a filter, blocking packets to or from the endpoint's MAC address (00:0c:29:8d:9c:f8). This filter was applied to the endpoint's VLAN (4025).

Figure 7. Automated Remediation



Source: Enterprise Strategy Group

Having found that their endpoint couldn't communicate to the network, and assuming that the network might be having problems, a frustrated user might attempt to use a different ethernet port. We simulated this situation by using the virtualization server to switch virtual networks, moving the endpoint from VLAN 4025 to VLAN 3025. As soon as we switched, the endpoint was granted a new IP address and was able to communicate both internally and externally.

After approximately five minutes, communication was once again blocked—both internally and externally. Sky ATP and the SRX firewall continuously monitored the network and identified the endpoint via its MAC address. Since the endpoint was already on the infected host feed, the SRX firewall applied a new north-south block. And Sky ATP directed the QFX switch to update its stateless firewall to apply the MAC address block on VLAN 3025.

Why This Matters

Facing perpetual cybersecurity skills shortages, organizations cannot afford to invest in multiple complicated products with extensive learning curves, requiring significant efforts and manual processes to detect and prevent threats.

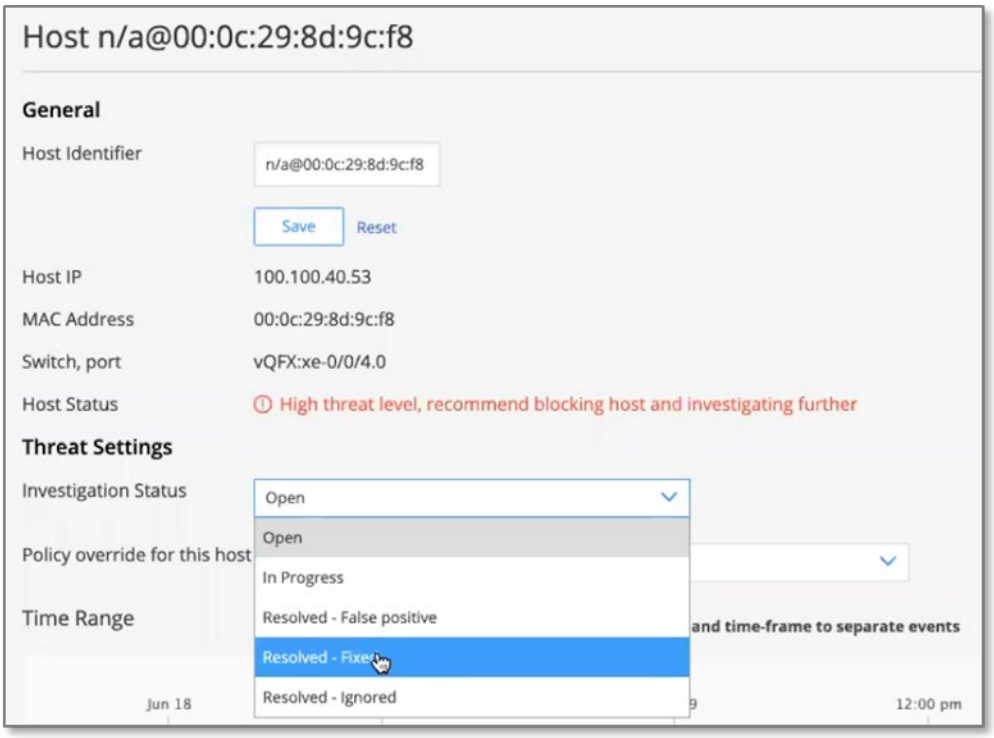
ESG validated that Juniper Networks SRX Series firewalls automatically forwarded downloaded files to Sky ATP for analysis and detection of malware. When Sky ATP determined that the endpoint was infected, the endpoint was added to the list of infected sites. Built-in automation and orchestration disconnected the endpoint from the network, preventing both internal and external communication.

Using Sky ATP and SRX Series firewalls helps organizations detect cyber-attacks as quickly as possible and stop the progression of the cyber kill chain, protecting critical assets and reducing malware dwell time.

Administrative Resolution and Remediation

ESG simulated the typical security analyst workflow of disinfecting the host by removing all malware files from the host. Next, we used the Sky ATP interface to change the investigation status, marking the issue as closed. From the host monitor section, we clicked on the host. Using the pulldown, we selected ***Resolved – Fixed*** for the investigation status. As shown in Figure 8, security analysts can set the investigation status to ***open***, ***in progress, resolved – false positive, resolve – fixed,*** or ***resolve – ignored***.

Figure 8. Updating the Investigation Status



Source: Enterprise Strategy Group

Setting the investigation status to any of the resolved options indicates that the system is no longer infected and can resume communicating on the network. Sky ATP removes the system from the infected host feed, and both the SRX firewall and QFX switch remove any firewall entries for the host. Shortly after setting the investigation status to Resolved - Fixed, we observed that the endpoint was able to communicate both internally and externally.

Why This Matters

As organizations grapple with a rising number of increasingly sophisticated cyber-attacks, security analysts must continually investigate potentially compromised systems in a timely manner. Lack of integration, automation, and orchestration forces analysts to expend significant time and effort on mundane, repetitive tasks.

ESG validated that once a security analyst marks an investigation as closed, Juniper Networks automation communicates with all appropriate firewalls and switches to remove network communication blocks, enabling the host to communicate internally and externally. Thus, the analyst no longer must manually figure out which set of switches and firewalls needs to be updated, log in to each device, update the rules, and save the new configurations. Juniper Networks automation not only lightens the security analyst workload, it also helps prevent human errors.

The Bigger Truth

The cybersecurity landscape is growing more complex and difficult to manage. Intellectual property, customer information, and financial data are increasingly at risk of compromise, which can lead to profound consequences, including financial penalties, impact to brand and company valuation, and legal action. Meanwhile, businesses must investigate and respond to a steeply increasing number of security incidents. The proliferation of new systems and applications is creating more security incident scenarios, while better detection tools are generating more alerts. With 53% of organizations reporting that they have a problematic shortage of cybersecurity skills in 2019, up from 51% in 2018,[4] organizations are seeking enhanced efficiency and efficacy, and are turning toward automated and automatable tools to alleviate the burden of manual or repetitive tasks.

Juniper Networks designed Sky ATP to automate cybersecurity, using real-time intelligence for anti-malware threat prevention. The SaaS solution integrates with SRX Series next-generation firewalls and the entire suite of Juniper products as well as third-party products through a variety of connectors. Using threat intelligence, antivirus signatures, static and dynamic analysis, and machine learning, as well as other techniques, Sky ATP can automatically detect and remediate threats.

The SRX Series next-generation firewalls automatically forwards downloaded files, email attachments, and other potentially malicious objects to Sky ATP for analysis. Upon threat detection, SRX firewalls work in conjunction with Sky ATP, QFX Series switches, and other network devices to disconnect infected systems from the network, automatically blocking north-south traffic, preventing malware from exfiltrating data to command and control servers, and automatically blocking east-west traffic, preventing lateral movement.

ESG validated that Sky ATP simplified deployment, configuration, and management. We were able to define secure fabrics—collections of network devices—enabling us to use simple operations to control large groups of systems, useful for large and complex environments. A clean and simple user interface accelerated and streamlined the effort to define security policies.

We validated that SRX Series firewalls automatically forwarded suspicious objects to Sky ATP for analysis and detection of malware. Infected hosts, as classified by Sky ATP, were automatically disconnect from the network by SRX firewalls, preventing north-south traffic. In addition, Sky ATP and SRX automation worked in conjunction with QFX switches to disconnect infected systems from east-west traffic. This automation helped to prevent lateral movement and communication with command and control servers.

Sky ATP can help with the infected host investigation effort, providing accurate information necessary to identify the infection, root cause, and corrective actions. When we fixed the issue and marked the investigation as resolved, Sky ATP and SRX firewalls automatically restored network connectivity, removing another tedious and complex manual process from the security analyst's workflow.

For organizations that want to move beyond complex, error-prone, manual workflows and leverage automation and orchestration throughout their environments to detect and prevent threats, it would be worthwhile to take a closer look at Juniper Networks Sky ATP and SRX Series next-generation firewalls.

[4] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.

PN2000747-001-EN

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188