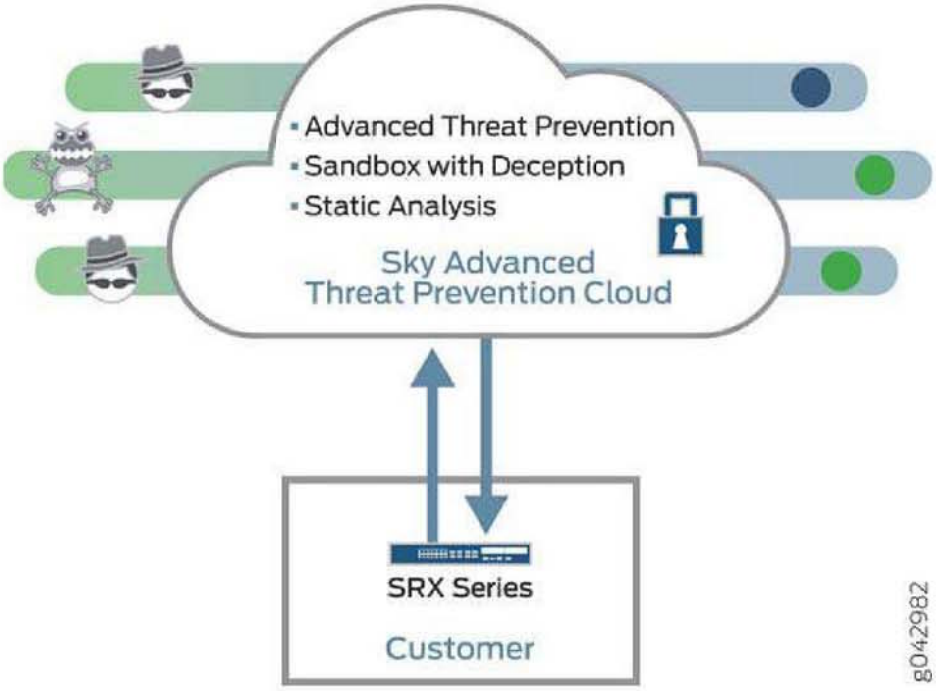
EXHIBIT 3

cloud-based threat detection software with a next-generation firewall system. See Figure 1 on page 4.

Figure 1: Sky ATP Overview



Sky ATP protects your network by performing the following tasks:

- The SRX Series device extracts potentially malicious objects and files and sends them to the cloud for analysis.
- Known malicious files are quickly identified and dropped before they can infect a host.
- Multiple techniques identify new malware, adding it to the known list of malware.
- Correlation between newly identified malware and known Command and Control (C&C) sites aids analysis.
- The SRX Series device blocks known malicious file downloads and outbound C&C traffic.

Sky ATP supports the following modes:

- Layer 3 mode
- Tap mode
- Transparent mode using MAC address. For more information, see Transparent mode on SRX Series devices.
- Secure wire mode (high-level transparent mode using the interface to directly passing traffic, not by MAC address.) For more information, see Understanding Secure Wire.

Sky ATP Features

Sky ATP is a cloud-based solution. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your sensitive data is secured even though it is in a cloud shared environment. Security analysts can update their defense when new attack techniques are discovered and distribute the threat intelligence with very little delay.

In addition, Sky ATP offers the following features:

- Integrated with the SRX Series device to simplify deployment and enhance the anti-threat capabilities of the firewall.
- Delivers protection against "zero-day" threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.
- High availability to provide uninterrupted service.
- Scalable to handle increasing loads that require more computing resources, increased network bandwidth to receive more customer submissions, and a large storage for malware.
- Provides deep inspection, actionable reporting, and inline malware blocking.
- APIs for C&C feeds, whitelist and blacklist operations, and file submission. See the Threat Intelligence Open API Setup Guide for more information.

Figure 2 on page 5 lists the Sky ATP components.

Figure 2: Sky ATP Components

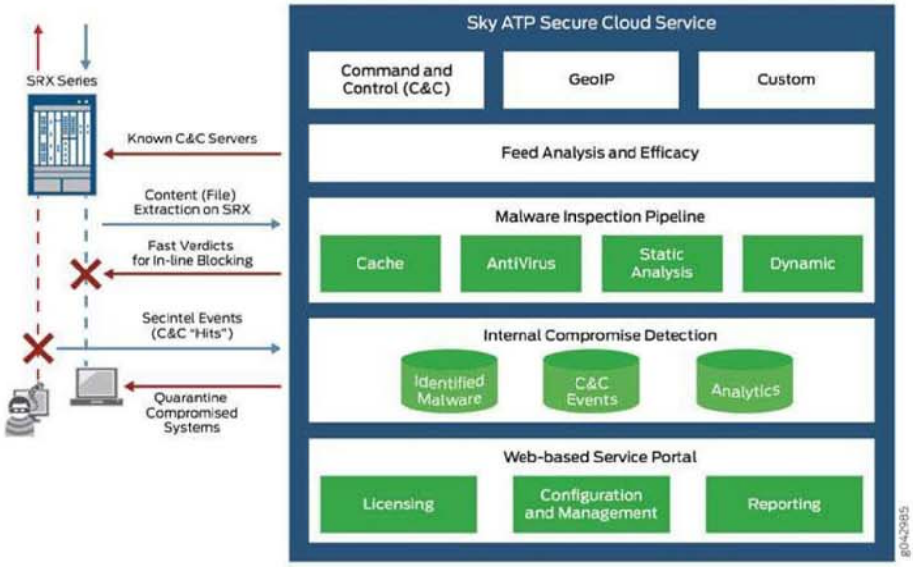
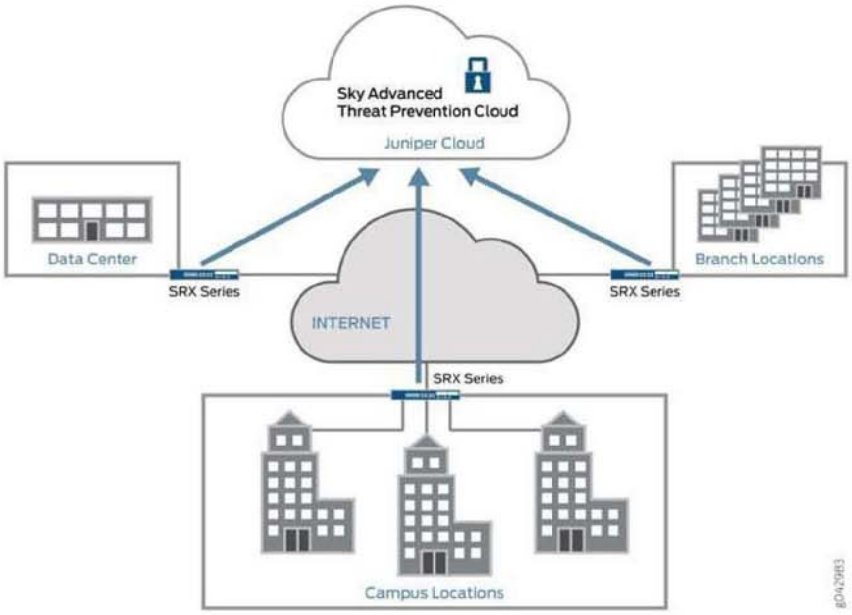


Figure 4: Sky ATP Use Cases



- Campus edge firewall—Sky ATP analyzes files downloaded from the Internet and protects end-user devices.
- Data center edge—Like the campus edge firewall, Sky ATP prevents infected files and application malware from running on your computers.
- Branch router—Sky ATP provides protection from split-tunneling deployments. A disadvantage of split-tunneling is that users can bypass security set in place by your company's infrastructure.

Related Documentation

- *Sky Advanced Threat Prevention License Types*

How is Malware Analyzed and Detected?

Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See Figure 5 on page 9.