Encrypted Traffic Insights

70–80% of enterprise inbound network traffic is now encrypted

Eric Parizo, Senior Analyst at Ovum

More than 40% of attacks use encryption to evade detection

Ponemon Institute, 2016

• SECURITY VS PRIVACY

Customers should not have to choose one over the other

- Rise in encrypted traffic; privacy and security benefits of encryption allows us to do more business on the web, cloud, and mobile networks securely
- Bad actors are also using encryption
- Not everything can or should be decrypted
- Decryption and deep packet inspection are expensive

Juniper Business Use Only

Encrypted Traffic Insights

- **Looking for threats without breaking encryption**
- **Provides insight and visibility**
  - Based on the network behaviors analyzed, connections are classified as malicious of benign
  - Can identify the hallmarks of botnet and malware command and control traffic
- **No need for additional hardware**
  - Relevant data extracted by the SRX
  - Behavior analysis and machine learning provided by the ATP Cloud

Metadata

- Known malicious certificates
- Connection details from the TLS handshake

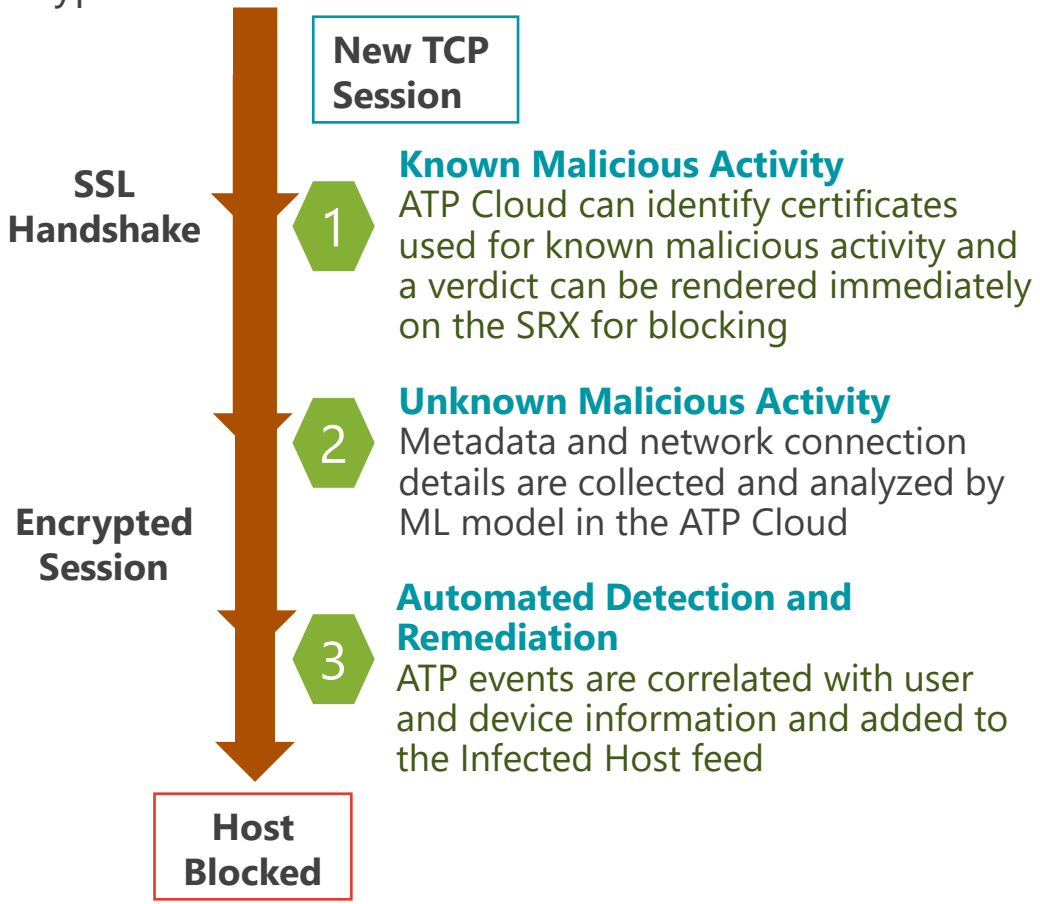
Connection Patterns

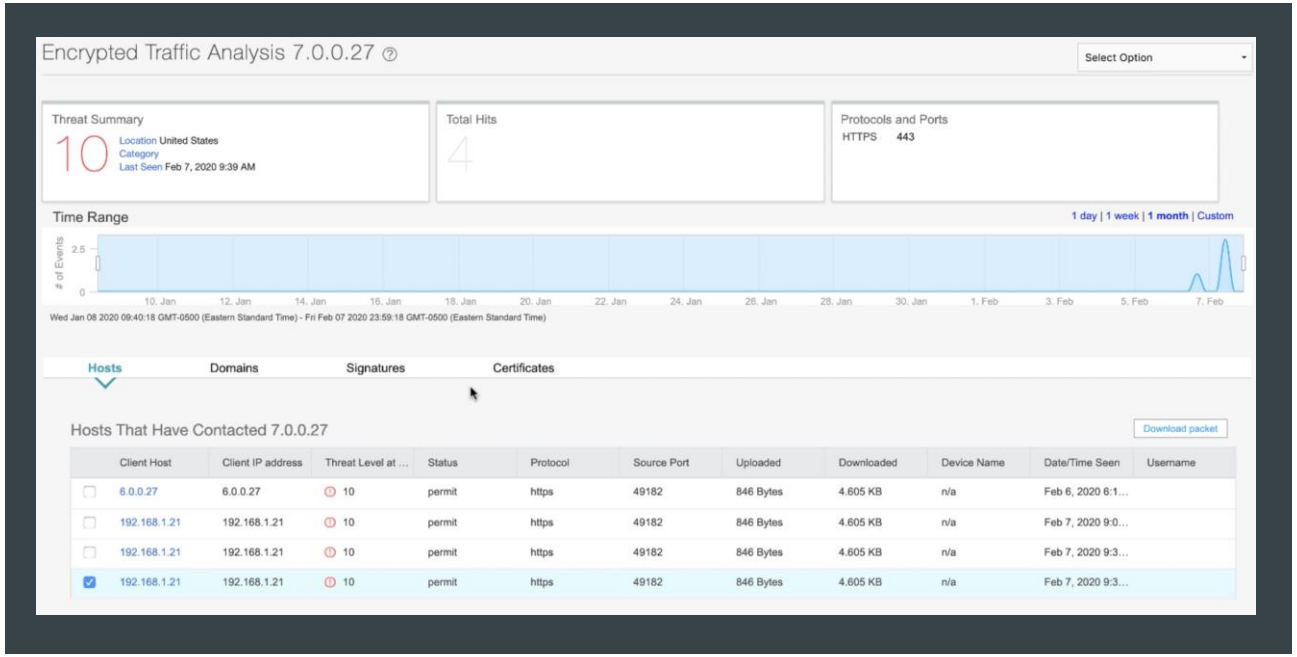
- Connections per second
- Beaconing behavior

Juniper Business Use Only

Juniper's Encrypted Traffic Insights

Multi-staged Analysis: Combining rapid response and network analysis to detect and remediate malicious activity hidden in encrypted sessions



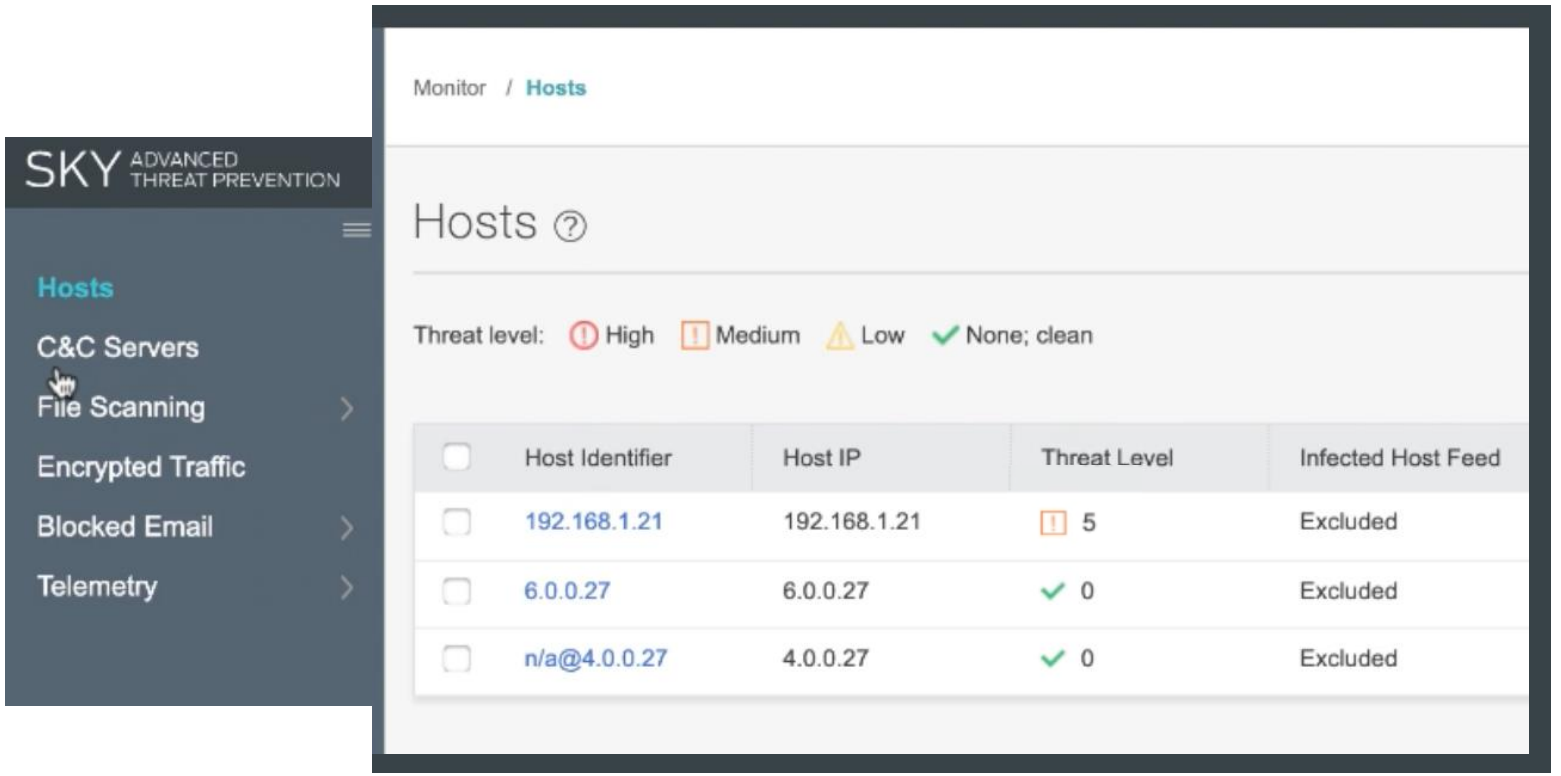


Juniper Business Use Only

Infected Host Risk Scoring

- Machine learning algorithms, change as threat trends change
- Observed detections from threat intelligence feeds
  - Malware or suspicious download
  - C2 communications
  - Requests to suspicious URLs/domains
  - ETI detections
  - Advanced Threat Profiling feeds*

*September release



Juniper Business Use Only

Encrypted Traffic Insights

Looking for threats without breaking encryption

Visibility

Gain insight into what has been completely unknown to admins

- Collecting contextual information about the SSL connection itself without breaking privacy and security

Confidence

Correlated with other malicious related activity detected by the ATP Cloud

- Give a high degree of confidence by using network behavioral analysis as another indicator of compromise

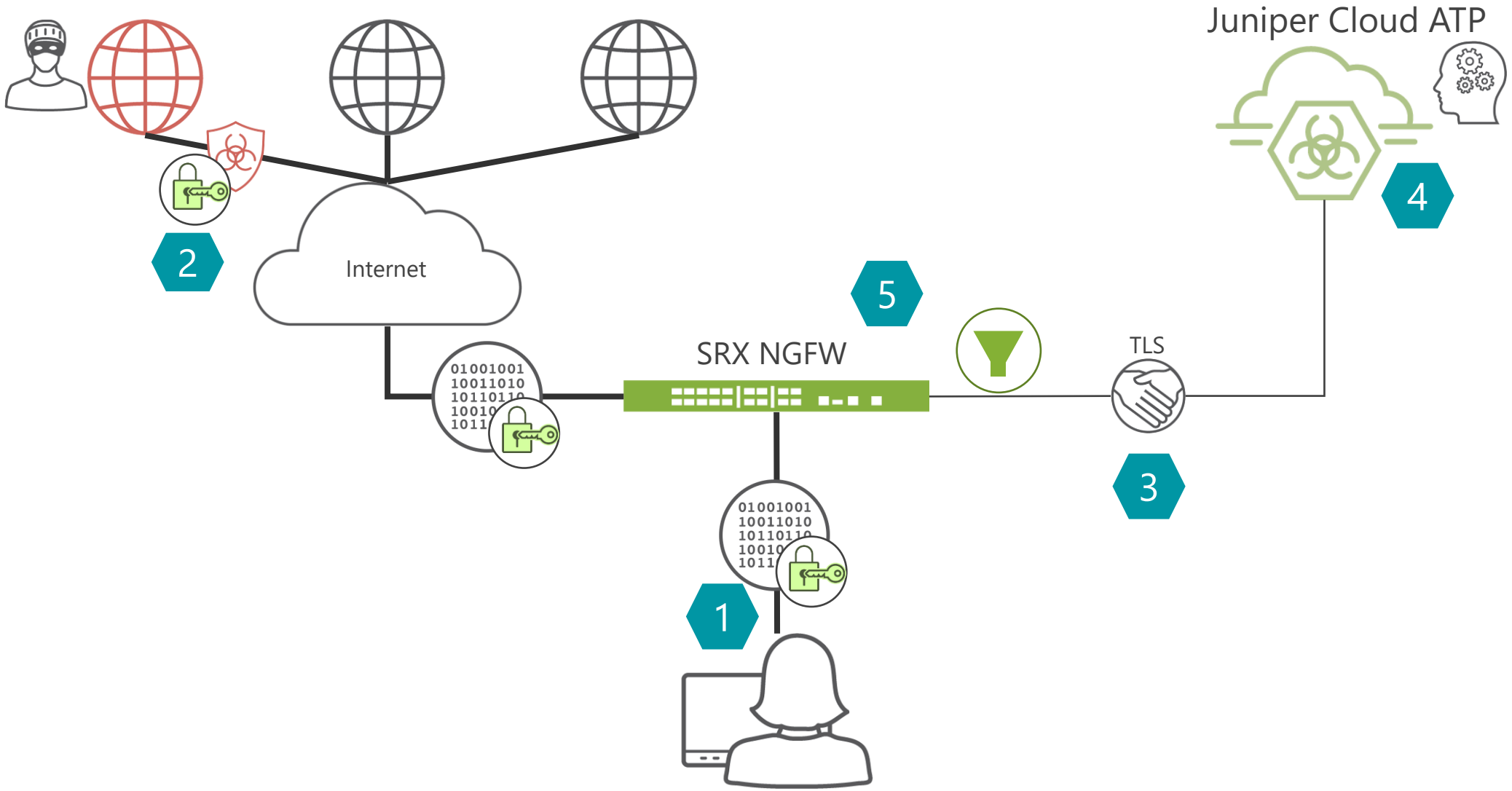
Quick Response

Automated remediation greatly shortens time to response

- High fidelity events correlated with user and device information helps admins access risk and prioritize
- Infected devices can be contained using Juniper and 3rd party integrations

Juniper Business Use Only

Juniper's Encrypted Traffic Insights



Juniper Business Use Only

Key Takeaways

Challenges

- Rapid pace at which threats emerge and propagate
- Expanded attack surface with cloud and IoT
- Traffic going dark and lack of visibility

Solutions

- Leverage Machine Learning for unknown threats
- Correlated threat data with contextual information
- Use automated workflows to shorten dwell time

Benefits

- Real-time protection against sophisticated attacks
- High fidelity events to help admins access and prioritize risk
- Leverage your entire infrastructure for threat mitigation

Juniper Business Use Only


Thank you
JUNIPER NETWORKS
Engineering
Simplicity