CYBERCRIME CONTINUES TO THRIVE

$6 TRILLION
IN ESTIMATED CYBERCRIME DAMAGES BY 2021[1]

3.5 MILLION
CYBER SECURITY JOB OPENINGS BY 2021[1]

HOW WILL SECURITY TEAMS MANAGE RISK AND ENFORCE POLICY?

31 BILLION IoT DEVICES
INSTALLED WORLDWIDE BY 2020[2]

3 NEW ATTACK GROUPS IDENTIFIED
ON AVERAGE EVERY YEAR[3]

95% OF CLOUD SECURITY FAILURES
WILL RESULT FROM POOR MANAGEMENT[4]

NO INHERENT ENDPOINT SECURITY
FOR IoT DEVICES

LIMITED VISIBILITY AND DATA CORRELATION
FOR INCIDENT RESPONSE

LACK OF AUTOMATION TO ENFORCE POLICY
BASED ON RISK LEVEL

ENTERPRISE

- 30% of the breaches include malware[5]
- 94% of malware is polymorphic[6]

DATA CENTER

- Phishing and pretexting represent 93% of breaches[3]
- 4% of targets in any given phishing campaign will click it[5]

MULTICLOUD

- 13% overall increase in reported vulnerabilities[3]
- 6% of breaches are patchable vulnerabilities[5]

BEST SECURITY TOOLS
SECURITY TEAMS MANAGE AN AVERAGE OF 10-12 VENDORS[7]

I'll get to that P3 later, I have a P1 over here!

I'm manually removing infected devices from this branch 20 times or more a day.

How am I supposed to secure a scaling network? I can't keep up. There has to be a better way to protect my assets while still responsibly managing risk.

87% OF COMPROMISES HAPPEN WITHIN MINUTES OR LESS[5]

ONLY 3% ARE DISCOVERED AS QUICKLY[5]

JUNIPER NETWORKS | Engineering Simplicity

(1) Cybersecurity Ventures and Herjavec Group
(2) Statista, Internet of Things (IoT) Connected Devices from 2015 to 2015
(3) Symantec 2018 Internet Security Threat Report
(4) Gartner, Is the Cloud Secure?
(5) Verizon 2018 Data Breach Investigations Report
(6) 2017 Webroot Threat Report
(7) Juniper Networks 2018 Focus Group Research

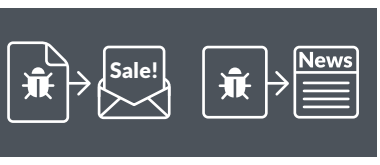
STOP INNOVATIVE CYBER CRIMINALS

LEVERAGE YOUR ENTIRE NETWORK TO FIND AND STOP THREATS FASTER.

CYBER CRIMINALS

COLLECTION OF RESOURCES
- Leaked exploits
- Off-the-shelf toolkits
- Stolen credentials
- Personal identifiable information

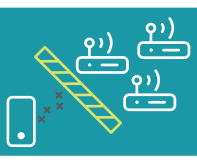
WEAPONIZE
Cyber criminals use data and resources to develop a weapon.



DELIVERY
Cyber criminals transmit the weapon to the target.

EXPLOITATION
Malware executes against vulnerabilities.

QUARANTINE THREAT
Threat is removed from the network.

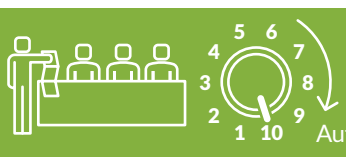


SECURITY TEAM

INVESTMENT IN SECURITY

Next-generation firewall, antivirus, Intrusion Prevention System

POLICY DEVELOPMENT
Security team develops policy based on risk insights.

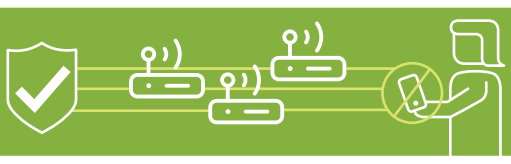


Automation level set between 1 and 10.

INFECTION
The unknown threat enters the network.

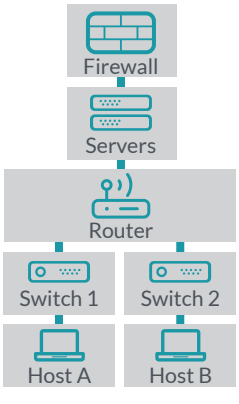
DATA CORRELATION
Threat intel and policy are correlated through Juniper security.

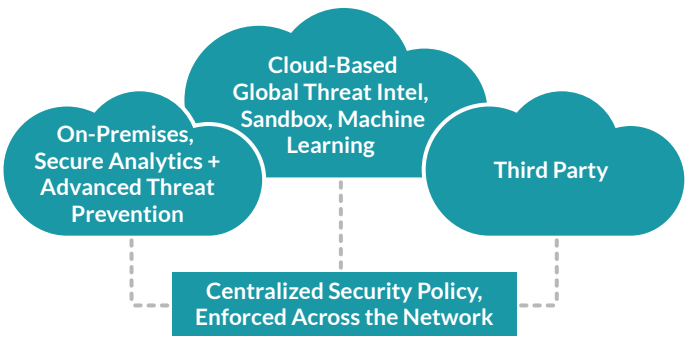
POLICY ENFORCEMENT
Security policy automatically enforced across all network devices.



ENFORCE SECURITY POLICY ACROSS ALL NETWORK DEVICES, AUTOMATICALLY

THERE'S NO RIP AND REPLACE





Juniper Networks' open architecture and API suite allows for simple integration. For example:

- ForeScout for access security
- CipherCloud for cloud application security
- Carbon Black for endpoint security
- JSA, QRadar, Splunk, and more for SIEM
- RADIUS services
- And more…

BUSINESS BENEFITS:

- Correlate all network threat intelligence
- Automate repetitive tasks; focus staff on strategy
- Expand policy enforcement to every network device
- Protect investment by leveraging current infrastructure

JUNIPER BENEFITS:

- Save time with unified cybersecurity management experience
- Stop malicious traffic; keep normal traffic flowing
- Turn skilled security staff from tactical to strategic

To learn how this works in your environment, contact <insert partner name>.

JUNIPER NETWORKS | Engineering Simplicity

ZettaNet Pty Ltd
www.zetta.net.au
sales@zetta.net.au

zettanet