Adopting the NIST Cybersecurity Framework?

Minimize effort, mitigate risk, and maximize speed with security automation.

3 Reasons to Automate Security

Manual workflows for cybersecurity amplify risk from human error and time delay.

New cybersecurity architectures are needed, not more security hardware.

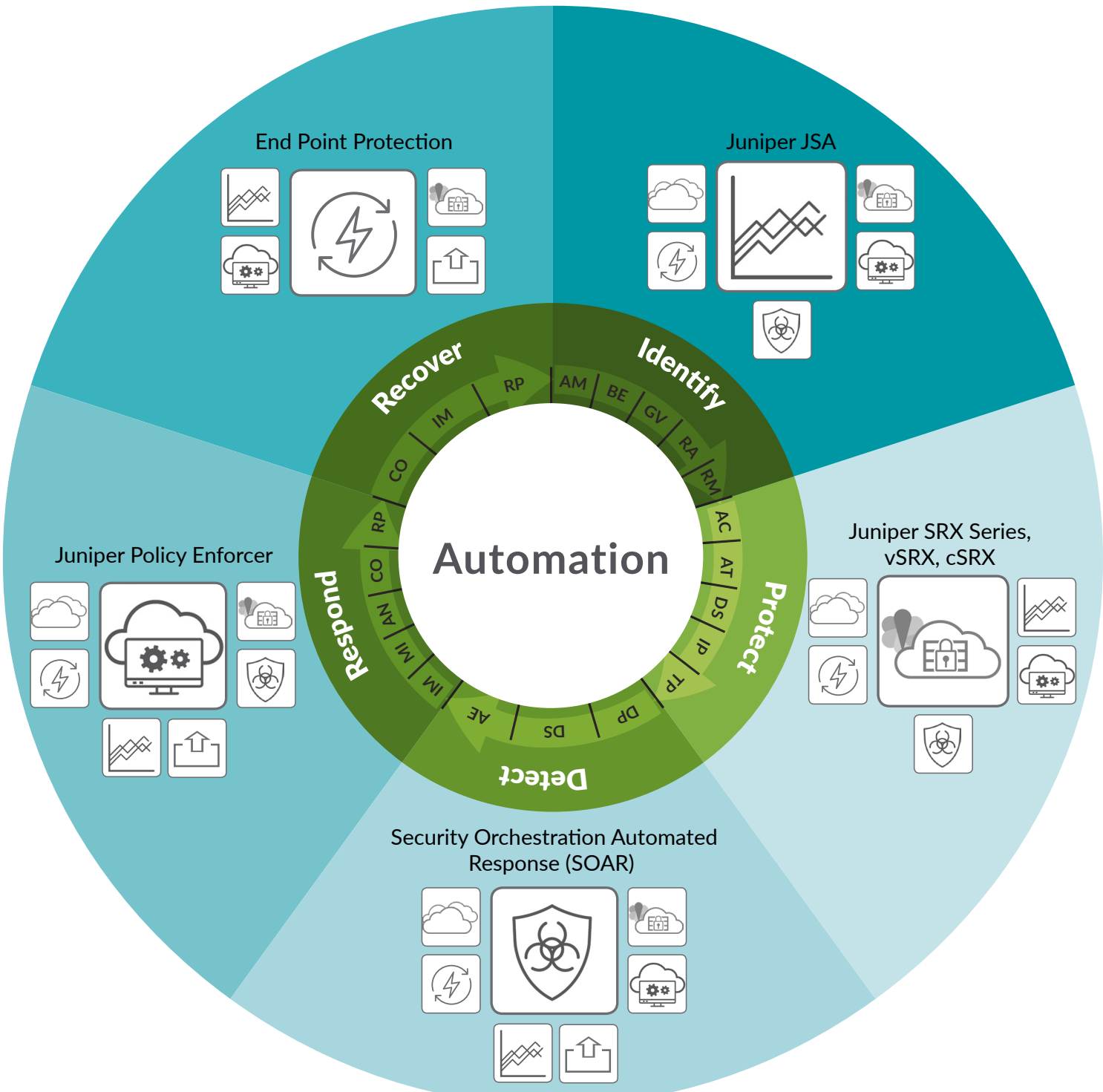
Every port in your network should participate—routers, switches, and firewalls—to help stop attacks faster in the kill chain.

Juniper Connected Security

- Shrink process time between categories and subcategories
- Inject assessments, correlations, anomalies, and behavioral analytics feeds into automation policies
- Accelerate detection, response, and remediation from days to minutes
- Consolidate manual tactical actions and reactions into automated strategies
- Leverage consistent policies across multicloud environments, physical and virtual

NIST Cybersecurity Framework Acceleration

Detect, respond, recover in seconds



Automation Elements

SECURE ANALYTICS | JUNOS — NGFW, ROUTER, SWITCH | SECURITY DIRECTOR POLICY ENFORCER | SECURITY ORCHESTRATION AUTOMATED RESPONSE | MULTICLOUD SECURITY | SECURITY FEEDS | TECHNOLOGY PARTNER END POINT PROTECTION

To learn more about Juniper Connected Security, visit www.juniper.net/security

3050047-002-EN June 2019

JUNIPER NETWORKS