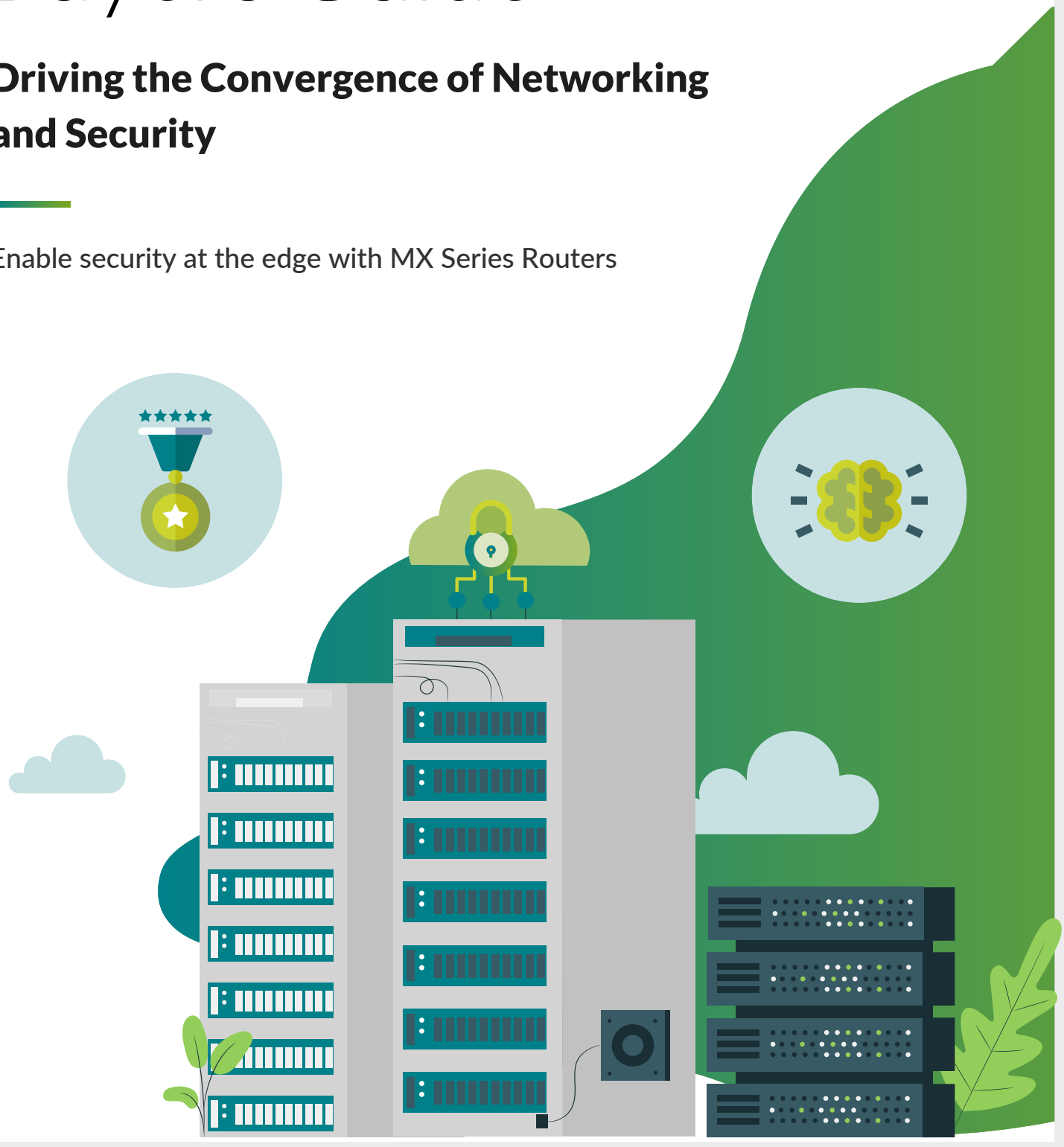
JUNIPER NETWORKS

MX Series Security Buyers Guide

Driving the Convergence of Networking and Security

Enable security at the edge with MX Series Routers



Network Technology & Security Integration.
Where are we now?

The security industry is growing by the day. Innovation is eroding the distance between the roles and responsibilities of physical and cybersecurity teams.

Computing devices are largely vulnerable to physical attacks, no matter how well they are managed. Attacks against both physical and cyber targets originate from far across the digital domain. As a result, network technology and security convergence is important.

The market is in its early infancy in embracing a fully converged network and security environment with centralized policy control. However, as digital environments evolve and change, and new architectures come in to play, particularly with the maturity of 5G, we expect better and more innovative infrastructure models to come into play which addresses the network and security convergence story.

Meeting security requirements while keeping up with the fast growth of network traffic, connected devices, and applications is critical for services providers and large enterprises alike.

Workplaces need to change their approach to protect their valuable data. Today, most organizations still need to develop a coordinated, converged approach to incorporate security measures. This means adopting a new mindset, from the defense to offense.

To be successful in an increasingly sophisticated digital era, it's important to ensure hardware, firmware, software and networking security is addressed at every level, without slowing down performance, or creating too much complexity.

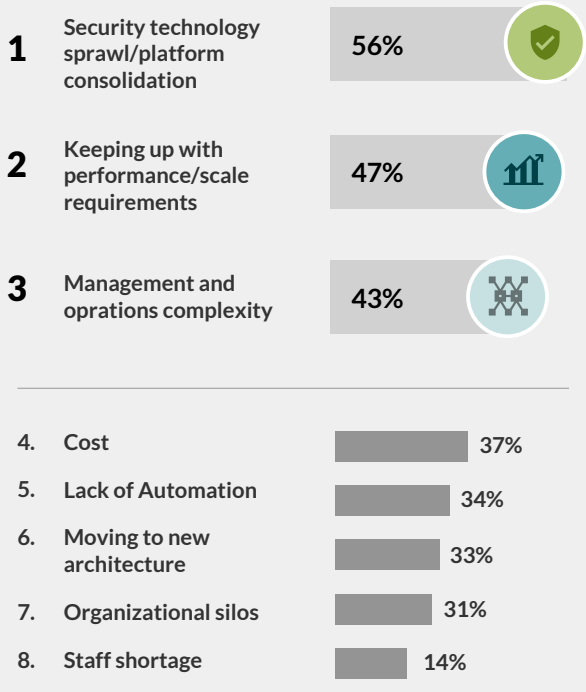
A new study by Omdia research[1] reveals that:

1. Technology management is the key.

The increase in performance, changes in network architecture and new technology adoption that come with it present major security implications.
The top three security challenges that service providers need to tackle to run a successful business and mitigate the associated risks are:

- Security technology sprawl/platform consolidation (56%)
- Keeping up with performance/scale requirements (47%)
- Complexity of Management and Operations (43%)

Figure 1 - What are your top 3 security challenges?



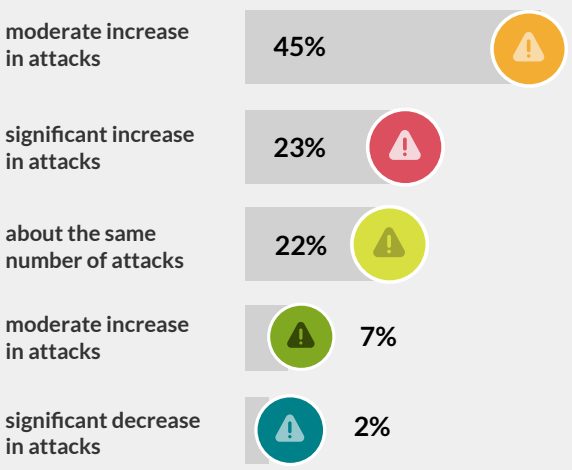
[1] Omdia research whitepaper: https://www.juniper.net/assets/us/en/local/pdf/whitepapers/3200095-en.pdf

While, at first glance, the challenges listed may not lead one immediately to think of security systems, the connected nature of today's solutions makes many, if not all, of them critical.

2. Cyber attacks are increasing. There is a need to focus on proactive prevention rather than just detection.

Interconnectivity makes for an extremely vulnerable world. When asked about the threats faced in the last 12 months, 45% of repondents admitted to have seen a moderate increase in cyber attacks, and 23% of respondents stated that the numer of attacks increased significantly. This means more than half of the companies are at the risk of cyber attacks.

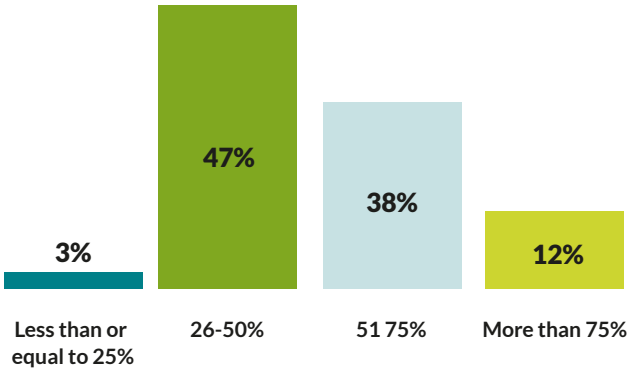
Figure 2 - Which of the following statements best describes the change in threats you've faced in the last 12 months?



As a result, organizations are turning their attention and resources to securing their businesses, examining the changes to take to secure essential services for their customers, and protect employees and citizens at large from data breach.

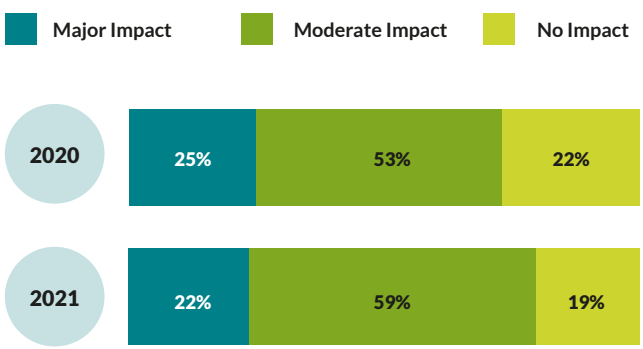
3. Security budget for 2021 is expected to increase due to COVID-19 pandemic effects on economy and technology.

Figure 3 - By what percent do you expect to increase your overall security capacity in the next year?



The COVID-19 pandemic is putting unprecedented strain on not only our way of living, but our networks, as well. In fact, it's during this time that we appreciate just how critical the network is in our lives. Many of our telecom respondents have reported network traffic numbers doubling and some IT teams are struggling to keep up amidst the pressures of maintaining operations while their entire workforce is remote. Some of this is temporary, but we will see some lasting effects that will have implications on the budget allocation priorities and the way networks are built and managed.

Figure 4 - What impact do you expect the COVID-19 pandemic to have on your security spending?



4. Network solutions that directly participate in mitigating security threads are an imperative for new investments.

Preventing data breaches and other network security threats is all about hardened network protection. Without proper security protocols, business data is at risk.

When asked about networking solutions and security threats, the majority of respondents recognized the importance of new network elements to directly particpate in mitigating security threats.

28% of respondents stated that it is “imperative for new networking solutions to have security integrations in place”, 21% of respondents rated the security integration as “very important”, and 6% as “somehow important”. Only a very minor part of respondents (6%) didn’t recognize the importance of this feature.

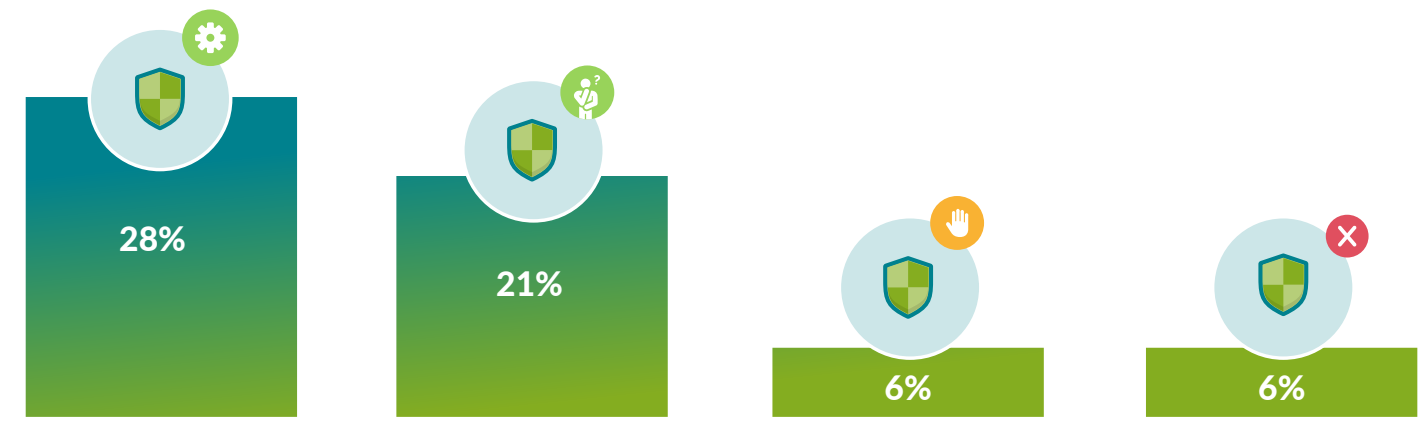
This means more than half of the companies recognized the key the role of new network solutions in protecting from malicious hackers and keeping company’s sensitive information safe and secure.

Did you know that..

97%

Ninety-seven percent (97%) of survey respondents admitted that they are specifically experiencing ongoing challenges when attempting to secure their organization’s network effectively.

Figure 5 - How important is it that network elements are able to directly participate in mitigating security threats?



5. Quick response, higher level of security and visibility. The key benefits of integrating networking and security.

As more employees work from home and cyber attacks become more sophisticated, security professionals are faced with new and emerging challenges that put organizations at even greater risk than before.

Companies need threat-aware networks that bring speed and agility, coupled with a Connected Security strategy that allows all network elements to work together for increased visibility and action where it matters most.

Old security implementations and methods will no longer suffice for those companies battling a new norm.

Figure 6 - What are the top 3 benefits of deploying networking solutions with integrated security?

About this research [1]

OMDIA

Methodology

Omdia Research interviewed over 360 respondents from different service providers across the globe to determine views on convergence of networking and security.

The concept of network and security convergence is currently in vogue among service providers in response to changing IT requirements. The new requirements to secure and accelerate cloud-based applications, deploy IoT and meet edge security threats are real.

The respondents were either decision-makers or key influences on the purchase decision for network security within their company.

They were from:

Global Companies with over 100 employees

Seven percent (7%) had an annual revenue up to $200 million, 9% had between $200 million and $500 million revenue, 20% had an annual revenue between $501 million and $1 billion, 27% earned between $ 1 to 5 billion and 37% more than $ 5 billion.

Four percent (4%) had over 5,000 employees, 11% had between 1,000 and 5,000 employees, 24% had between 500 and 1,000 employees, 37% had between 250 and 500 employees, and 23% had between 100 and 250 employees.

[1] Omdia research whitepaper: https://www.juniper.net/assets/us/en/local/pdf/whitepapers/3200095-en.pdf

Integrating Networking and Security.
Making it Work.

As service providers adopt new architectures, they must ensure that their security posture is sufficiently agile to change with new requirements, and that security does not act as a bottleneck to network performance.

Security infrastructure must be able to scale up to handle increased capacity requirements and scale out to accommodate edge computing and increased IoT deployments.

Service providers must take the following approaches to securing their assets as they adopt distributed cloud, IoT and 5G technology:

Modernize and maximize your existing platform with advanced security capabilities.

Be aware of the danger.
Mitigate advanced threats.
Extend security to new distributed networks.

Strengthen your infrastructure security posture without compromising on performance.

Increase network performance and scale.
High speed and reliable.
Security without performance degradation.

Add security capabilities to your existing MX Series platforms.

Automate threat detection and migration with machine learning algorithms and security intelligence.

Get greater returns on your investment.

Monetize-as-a-service.
Povide security as a value-add to your customers in addition to connectivity.

Threat-aware solutions to strengthen your infrastructure security posture without compromising on performance.

With 5G rollouts, IoT, and multicloud your existing network infrastructure may meet the performance and scale requirements of these new technologies, but is it threat-aware?

5G, IoT and Multicloud adoption have made the network more and more important than ever before. As companies continue investing in increasing their network performance, what about their security infrastructure? Will it be able to keep up?

With cyber attacks increasing in volume, frequency, and sophistication, security can no longer be an afterthought. Your network needs to be threat-aware, and that comes from extending security to every point of connection across the network.

Modernizing security infrastructure using the same approach as always can be costly, complex to manage and not scalable in the long term. To help you solve these challenges, we have expanded our MX solution to become an integrated routing security platform that you can leverage to modernize, mitigate and monetize.

Our integrated MX Security solutions help maximize your existing MX Series platforms with advanced security capabilities, so your network is better equipped to defend against cyber threats.

Security offerings that you can add on to MX series platforms:

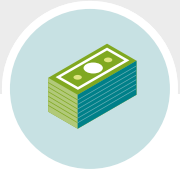
- **MX-SPC3 Security Services Card**
- **Juniper-Corero Joint DDoS Protection Solution**
- **Juniper Networks Security Intelligence (SecIntel)**

MODERNIZE

Maximize the scale and performance of your defense systems and deliver automated threat detection and mitigation.

MITIGATE

Mitigate advanced threats with machine learning algorithms and security intelligence.



MONETIZE

Monetize-as-a-service, providing security as a value-add to your customers in addition to connectivity.

MX-SPC3 Security Service Card

Be ready for 5G with **high performance CGNAT,** stateful firewall and beyond.

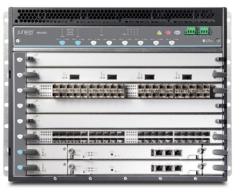
The MX-SPC3 services card allows you to modernize your current infrastructure and maximize return from your existing investment by leveraging the existing MX240, MX480 and MX960 routers without compromising performance, scale, or agility. The MX-SPC3 services card offers industry-leading carrier-grade Network Address Translation (CGNAT), stateful firewall services, Intrusion Detection Services (IDS), traffic load balancing, URL filtering and DNS sinkhole.

Features

- Junos OS Release 19.3R2 and later.
- Supported on MX240, MX480, and MX960 routers providing additional processing power to run the Next Gen Services providing the best of both routing and security features.
- Upgraded performance and scale for 5G, IoT and multicloud.
- The MX-SPC3 services card is compatible end-to-end with the MX Series Switch Fabrics, Routing Engines and MPC line cards for MX240, MX480, and MX960 routers.

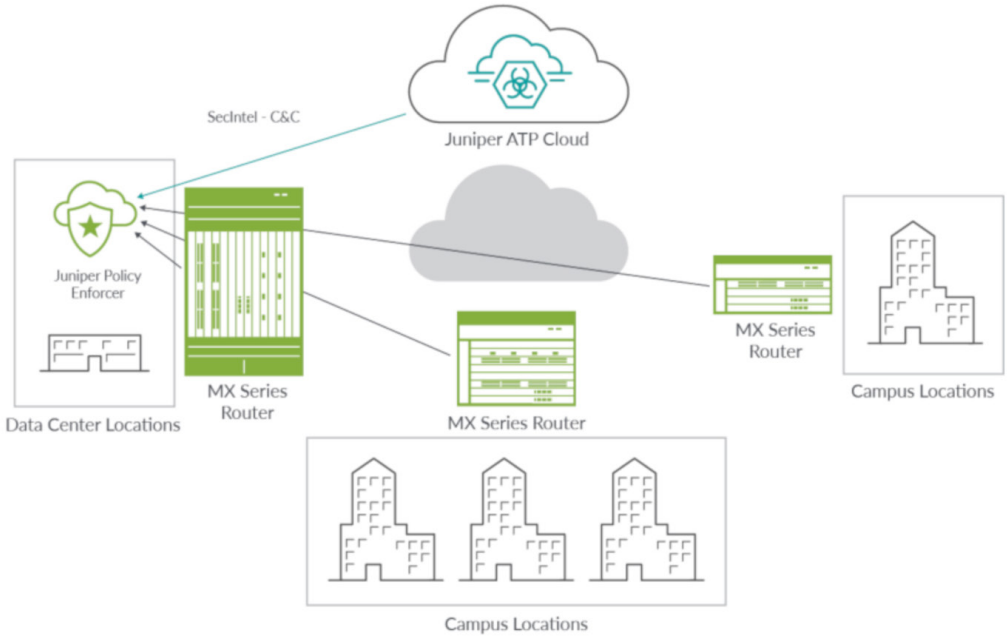
MX960

MX480



MX240

SecIntel on MX



Juniper Networks Security Intelligence (SecIntel)

Automate and protect your network at scale with **real-time threat intelligence.**

To defend against advanced threats, you need accurate up-to-date security intelligence at your fingertips. You can stop threats before they do damage by adding Juniper SecIntel to your existing MX Series routers.

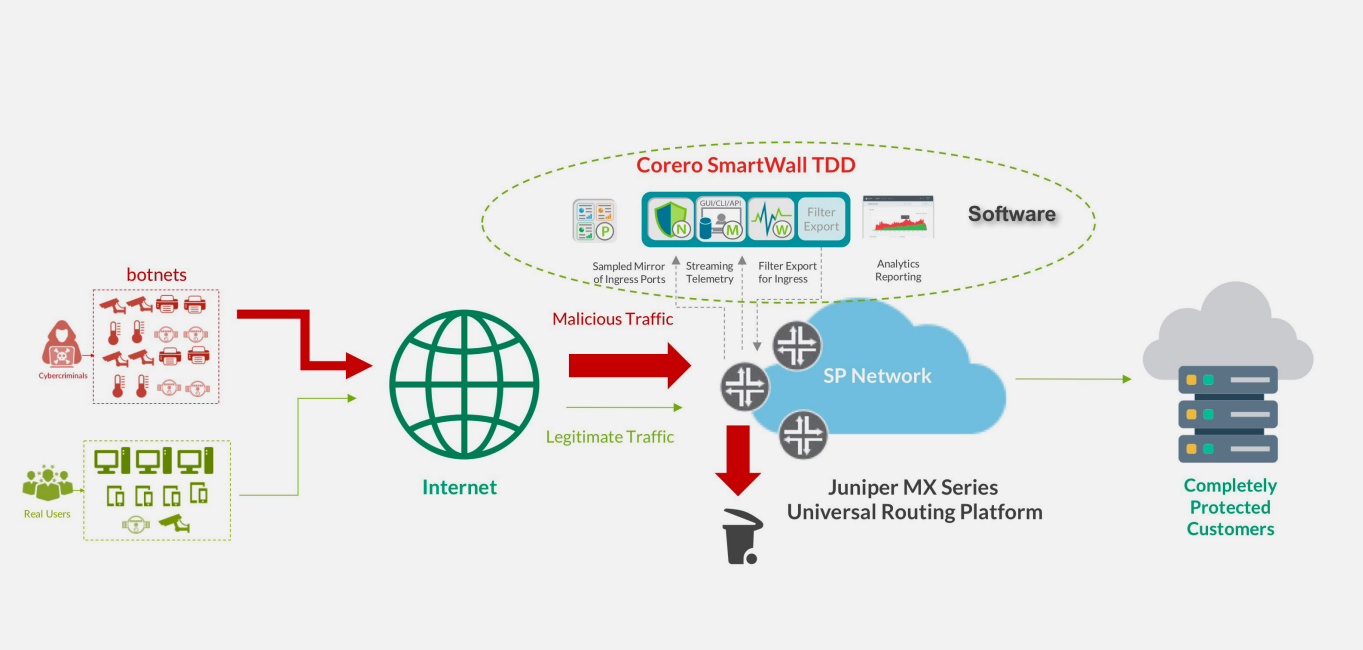
MX Series routers use the SecIntel threat feeds, providing an additional layer of network security by identifying and blocking Command & Control (C&C) traffic provided by **Juniper Advanced Threat Prevention (ATP)** cloud, along with custom whitelists and blacklists.

This feature evolves the role of the router from a simple connectivity layer into a threat-aware network device.

Features

- Supported on MX Series routers (MX240, MX480, and MX960) in Junos OS Release 19.3R2 and later.
- Threat-aware MX Series routers block threats before they even get to the firewall reducing the load on the firewall, which is typically more computationally expensive, and potentially offers protection to data flows that would otherwise go unprotected.
- Policy Enforcer enrolls into SecIntel within ATP Cloud to regularly fetch Global C&C feed, IP whitelist and blacklist.
- Feeds are delivered to the MX Series Routing Engine (RE) and consumed by the MX Series Packet Forwarding Engine(PFE), based on threat level and defined action (allow/block & log/sample/none).
- Block traffic from known malicious IPs at the network edge with MX Series routers.

Juniper + Corero SmartWall Threat Defense Director



Juniper and Corero Joint DDoS Protection Solution

Safeguard your **users, applications and infrastructure** against DDoS attacks.

Is your network equipped to keep pace with the increased sophistication, magnitude, and frequency of DDoS attacks?

You can stay ahead of these threats by adding **the Juniper and Corero DDoS Protection Solution** to your existing MX Series routers.

Features

- Boost your network protection with the equipment you already have
- Delivers real-time detection and line-rate mitigation by leveraging always-on packet-level monitoring, automated machine analysis and infrastructure-based enforcement across the network edge.
- Easy to add the Corero SmartWall Threat Defense Director (TDD) software to your existing MX Series platforms with a few quick configuration steps. Now, the networks will be protected and good to go - simple and affordable.

MX Security SKUs

SecIntel

SKU	Description
S-MX240-CSECINTEL1	SW, MX240, C, SECINTEL, W/CS, 1 YR
S-MX240-CSECINTEL3	SW, MX240, C, SECINTEL, W/CS, 3 YR
S-MX240-CSECINTEL5	SW, MX240, C, SECINTEL, W/CS, 5 YR
S-MX480-CSECINTEL1	SW, MX480, C, SECINTEL, W/CS, 1 YR
S-MX480-CSECINTEL3	SW, MX480, C, SECINTEL, W/CS, 3 YR
S-MX480-CSECINTEL5	SW, MX480, C, SECINTEL, W/CS, 5 YR
S-MX960-CSECINTEL1	SW, MX960, C, SECINTEL, W/CS, 1 YR
S-MX960-CSECINTEL3	SW, MX960, C, SECINTEL, W/CS, 3 YR
S-MX960-CSECINTEL5	SW, MX960, C, SECINTEL, W/CS, 5 YR

MX-SPC3

SKU	Description
MX-SPC3	HW, 3rd generation security services processing card for MX240/480/960. It includes the Traffic Load Balancer feature, and is the Base HW support for: CGNAT, Stateful Firewall, VPN, Intrusion Detection, DNS sinkhole, and URL Filtering
S-MXSPC3-A1-1	Software license, allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), with SW support, 1 YEAR
S-MXSPC3-A1-3	Software license, allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), with SW support, 3 YEAR
S-MXSPC3-A1-5	Software license, allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), with SW support, 5 YEAR
S-MXSPC3-A1-P	Software license, allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), without SW support, Perpetual
S-MXSPC3-A2-1	Software license, allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 1 YEAR
S-MXSPC3-A2-3	Software license, allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 3 YEAR
S-MXSPC3-A2-5	Software license, allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 5 YEAR
S-MXSPC3-A2-P	Software license, allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), without SW support, Perpetual
S-MXSPC3-A3-1	Software license, allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 1 YEAR

MX Security SKUs

MX-SPC3

SKU	Description
S-MXSPC3-A3-3	Software license, allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 3 YEAR
S-MXSPC3-A3-5	Software license, allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 5 YEAR
S-MXSPC3-A3-P	Software license, allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), without SW support, Perpetual
S-MXSPC3-P1-1	Software license, allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 1 YEAR
S-MXSPC3-P1-3	Software license, allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 3 YEAR
S-MXSPC3-P1-5	Software license, allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 5 YEAR
S-MXSPC3-P1-P	Software license, allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), without SW support, Perpetual
S-MXSPC3-P2-1	Software license, allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 1 Year
S-MXSPC3-P2-3	Software license, allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 3 Year
S-MXSPC3-P2-5	Software license, allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 5 Year
S-MXSPC3-P2-P	Software license, allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), without SW support, Perpetual
S-MXSPC3-P3-1	Software license, allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 1 YEAR
S-MXSPC3-P3-3	Software license, allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 3 YEAR
S-MXSPC3-P3-5	Software license, allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with SW support, 5 YEAR

MX Security SKUs

MX-SPC3

SKU	Description
S-MXSPC3-P3-P	Software license, allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), without SW support, Perpetual
S-PAR-MXSPC3-A1-1	SW, PAR Support, MX-SPC3, Allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), with PAR Customer Support, 1 YEAR
S-PAR-MXSPC3-A1-3	SW, PAR Support, MX-SPC3, Allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), with PAR Customer Support, 3 YEAR
S-PAR-MXSPC3-A1-5	SW, PAR Support, MX-SPC3, Allows end user to enable Carrier Grade NAT on a single MX-SPC3 in the MX-series routers (MX240, MX480, MX960), with PAR Customer Support, 5 YEAR
S-PAR-MXSPC3-A2-1	SW, PAR Support, MX-SPC3, Allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 1 YEAR
S-PAR-MXSPC3-A2-3	SW, PAR Support, MX-SPC3, Allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 3 YEAR
S-PAR-MXSPC3-A2-5	SW, PAR Support, MX-SPC3, Allows end user to enable Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 5 YEAR
S-PAR-MXSPC3-A3-1	SW, PAR Support, MX-SPC3, Allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 1 YEAR
S-PAR-MXSPC3-A3-3	SW, PAR Support, MX-SPC3, Allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 3 YEAR
S-PAR-MXSPC3-A3-5	SW, PAR Support, MX-SPC3, Allows end user to enable IDS on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 5 YEAR
S-PAR-MXSPC3-P1-1	SW, PAR Support, MX-SPC3, Allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 1 YEAR
S-PAR-MXSPC3-P1-3	SW, PAR Support, MX-SPC3, Allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 3 YEAR
S-PAR-MXSPC3-P1-5	SW, PAR Support, MX-SPC3, Allows end user to enable Carrier Grade NAT, URL Filtering, DNS Sinkhole, IDS, and Stateful Firewall on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 5 YEAR
S-PAR-MXSPC3-P2-1	SW, PAR Support, MX-SPC3, Allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 1 Year
S-PAR-MXSPC3-P2-3	SW, PAR Support, MX-SPC3, Allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 3 Year

MX Security SKUs

MX-SPC3

SKU	Description
S-PAR-MXSPC3-P2-5	SW, PAR Support, MX-SPC3, Allows end user to enable Stateful Firewall, URL Filtering, DNS Sinkhole, IDS, and Carrier Grade NAT on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 5 Year
S-PAR-MXSPC3-P3-1	SW, PAR Support, MXSPC3, Allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 1 YEAR
S-PAR-MXSPC3-P3-3	SW, PAR Support, MXSPC3, Allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 3 YEAR
S-PAR-MXSPC3-P3-5	SW, PAR Support, MXSPC3, Allows end user to enable IDS, URL Filtering, and DNS Sinkhole on a single MX-SPC3 in the MX-series router (MX240, MX480, MX960), with PAR Customer Support, 5 YEAR
SVC-COR-MX-SPC3	Juniper Care Core Support for MX-SPC3
SVC-CP-MX-SPC3	Juniper Care Core Plus Support for MX-SPC3
SVC-NDS-MX-SPC3	Juniper Care Next Day Ship Support for MX-SPC3
SVC-ND-MX-SPC3	Juniper Care Next Day Support for MX-SPC3
SVC-NDCE-MX-SPC3	Juniper Care Next Day Onsite Support for MX-SPC3
SVC-SD-MX-SPC3	Juniper Care Same Day Support for MX-SPC3
SVC-SDCE-MX-SPC3	Juniper Care Same Day Onsite Support for MX-SPC3
PAR-SUP-MX-SPC3	PSS Basic Support for MX-SPC3
PAR-RTF-MX-SPC3	PSS RTF Support for MX-SPC3
PAR-AR5-MX-SPC3	PSS AR5 Support for MX-SPC3
PAR-NDS-MX-SPC3	PSS Next Day Ship Support for MX-SPC3
PAR-ND-MX-SPC3	PSS Next Day Support for MX-SPC3
PAR-NDCE-MX-SPC3	PSS Next Day Onsite Support for MX-SPC3
PAR-SD-MX-SPC3	PSS Same Day Support for MX-SPC3
PAR-SDCE-MX-SPC3	PSS Same Day Onsite Support for MX-SPC3
SVC-COR-MXSPC3-A1P	Juniper Care Core Support for S-MXSPC3-A1-P
PAR-SUP-MXSPC3-A1P	PSS Basic Support for S-MXSPC3-A1-P
SVC-COR-MXSPC3-P1P	Juniper Care Core Support for S-MXSPC3-P1-P
PAR-SUP-MXSPC3-P1P	PSS Basic Support for S-MXSPC3-P1-P
SVC-COR-MXSPC3-A2P	Juniper Care Core Support for S-MXSPC3-A2-P
PAR-SUP-MXSPC3-A2P	PSS Basic Support for S-MXSPC3-A2-P
SVC-COR-MXSPC3-P2P	Juniper Care Core Support for S-MXSPC3-P2-P
PAR-SUP-MXSPC3-P2P	PSS Basic Support for S-MXSPC3-P2-P
SVC-COR-MXSPC3-A3P	Juniper Care Core Support for S-MXSPC3-A3-P
PAR-SUP-MXSPC3-A3P	PSS Basic Support for S-MXSPC3-A3-P
SVC-COR-MXSPC3-P3P	Juniper Care Core Support for S-MXSPC3-P3-P
PAR-SUP-MXSPC3-P3P	PSS Basic Support for S-MXSPC3-P3-P

Corero Smartwall TDD Software Licensing

SKU	Description
J-COR-DD100G-1-UPG	Upg from 100G to 200G, Corero SmartWall Threat Defense Director Virtual Edition 1 Yr SW subscription. Max 5 Detection Engine lics, for up to 200Gbps agg monitoring & mitigation. Includes J-Care, Soft Maint and Updates. Each DE w/10G proc capacity
J-COR-DD100G-3-UPG	Upg from 100G to 200G, Corero SmartWall Threat Defense Director Virtual Edition 3 Yr SW subscription. Max 5 Detection Engine lics, for up to 200Gbps agg monitoring & mitigation. Includes J-Care, Soft Maint and Updates. Each DE w/10G proc capacity
J-COR-DD100G-5-UPG	Upg from 100G to 200G, Corero SmartWall Threat Defense Director Virtual Edition 5 Yr SW subscription. Max 5 Detection Engine lics, for up to 200Gbps agg monitoring & mitigation. Includes J-Care, Soft Maint and Updates. Each DE w/10G proc capacity
J-COR-DD200G-1-UPG	Upg from 200G to 500G, Corero SmartWall Threat Defense Director Virtual Edition 1 Yr SW subscription. Max 5 Detection Engine lics, for up to 500Gbps agg monitoring & mitigation. Includes J-Care, Soft Maint and Updates. Each DE w/10G proc capacity
J-COR-DD200G-3-UPG	Upg from 200G to 500G, Corero SmartWall Threat Defense Director Virtual Edition 3 Yr SW subscription. Max 5 Detection Engine lics, for up to 500Gbps agg monitoring & mitigation. Includes J-Care, Soft Maint and Updates. Each DE w/10G proc capacity
J-COR-DD200G-5-UPG	Upg from 200G to 500G, Corero SmartWall Threat Defense Director Virtual Edition 5 Yr SW subscription. Max 5 Detection Engine lics, for up to 500Gbps agg monitoring & mitigation. Includes J-Care, Soft Maint and Updates. Each DE w/10G proc capacity
J-COR-DD500G-1-UPG	Upgrade J-COR-DOSDD-500G-1 from 500Gbps of DDoS detection to 1Tbps of DDoS detection. The expiration of the upgraded 1Tbps DDoS detection is the same as the expiration of the original J-COR-DOSDD-500G-1.
J-COR-DD500G-3-UPG	Upgrade J-COR-DOSDD-500G-3 from 500Gbps of DDoS detection to 1Tbps of DDoS detection. The expiration of the upgraded 1Tbps DDoS detection is the same as the expiration of the original J-COR-DOSDD-500G-3.
J-COR-DD500G-5-UPG	Upg from 500G to 1T, Corero SmartWall Threat Defense Director Virtual Edition 5 Yr SW subscription. Max 5 Detection Engine lics, for up to1Tbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-100G-1	Corero SmartWall Threat Defense Director Virtual Edition 1 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 100Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-100G-3	Corero SmartWall Threat Defense Director Virtual Edition 3 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 100Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-100G-5	Corero SmartWall Threat Defense Director Virt Edi 5 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 100Gbps agg monitoring and mitigation. Includes J-Care, Soft Maintenance and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-10T-1	Corero SmartWall Threat Defense Director Virtual Edition 1 Yr software subsc. Includes 1 Detection Engine lic, max 20, for up to 10Tbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity

Corero Smartwall TDD Software Licensing

SKU	Description
J-COR-DOS-DD-10T-3	Corero SmartWall Threat Defense Director Virtual Edition 3 Yr software subsc. Includes 1 Detection Engine lic,max 20, for up to 10Tbps aggmonitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity.
J-COR-DOS-DD-10T-5	Corero SmartWall Threat Defense Director Virtual Edition 5 Yr software subsc. Includes 1 Detection Engine lic,max 20, for up to 10Tbps aggmonitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-1T-1	Corero SmartWall Threat Defense Director Virtual Edition 1 Yr software subsc. Includes 1 Detection Engine lic, max 5, for up to 1Tbps aggmonitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-1T-3	Corero SmartWall Threat Defense Director Virtual Edition 3 Yr software subsc. Includes 1 Detection Engine lic, max 5, for up to 1Tbps aggmonitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-1T-5	Corero SmartWall Threat Defense Director Virtual Edition 5 Yr software subsc. Includes 1 Detection Engine lic, max 5, for up to 1Tbps aggmonitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-200G-1	Corero SmartWall Threat Defense Director Virtual Edition 1 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 200Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-200G-3	Corero SmartWall Threat Defense Director Virtual Edition 3 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 200Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-200G-5	Corero SmartWall Threat Defense Director Virtual Edition 5 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 200Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-40T-1	Corero SmartWall Threat Defense Director Virtual Edition 1 Yr software subsc. Includes 1 Detection Engine lic, max 40, for up to 40Tbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-40T-3	Corero SmartWall Threat Defense Director Virtual Edition 3 Yr software subsc. Includes 1 Detection Engine lic, max 40, for up to 40Tbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DD-40T-5	Corero SmartWall Threat Defense Director Virtual Edition 5 Yr software subsc. Includes 1 Detection Engine lic, max 40, for up to 40Tbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-500G-1	Corero SmartWall Threat Defense Director Virtual Edition 1 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 500Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOSDD-500G-3	Corero SmartWall Threat Defense Director Virtual Edition 3 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 500Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity

Corero Smartwall TDD Software Licensing

SKU	Description
J-COR-DOSDD-500G-5	Corero SmartWall Threat Defense Director Virtual Edition 5 Yr SW subscription. Includes 1 Detection Engine lic, max 5, for up to 500Gbps agg monitoring and mitigation. Includes J-Care, Soft Maint and Updates. Each DE with 10G proc capacity
J-COR-DOS-DE-10P-1	Corero SmartWall Threat Defense Director Detection Engine ,10 pack, Virtual Edition 1 Year software subscription with 10 Gbps of processing capacity per Detection Engine. Includes Juniper Care Support, Software Maintenance and Updates.
J-COR-DOS-DE-10P-3	Corero SmartWall Threat Defense Director Detection Engine ,10 pack, Virtual Edition 3 Year software subscription with 10 Gbps of processing capacity per Detection Engine. Includes Juniper Care Support, Software Maintenance and Updates.
J-COR-DOS-DE-10P-5	Corero SmartWall Threat Defense Director Detection Engine ,10 pack, Virtual Edition 5 Year software subscription with 10 Gbps of processing capacity per Detection Engine. Includes Juniper Care Support, Software Maintenance and Updates.
J-COR-DOS-DE-1P-1	Corero SmartWall Threat Defense Director Detection Engine, 1 pack, Virtual Edition 1 Year software subscription with 10 Gbps of processing capacity. Includes Juniper Care Support, Software Maintenance and Updates.
J-COR-DOS-DE-1P-3	Corero SmartWall Threat Defense Director Detection Engine, 1 pack, Virtual Edition 3 Year software subscription with 10 Gbps of processing capacity. Includes Juniper Care Support, Software Maintenance and Updates.
J-COR-DOS-DE-1P-5	Corero SmartWall Threat Defense Director Detection Engine, 1 pack, Virtual Edition 5 Year software subscription with 10 Gbps of processing capacity. Includes Juniper Care Support, Software Maintenance and Updates.

Please Note:

This guide contains general information about legal matters.
The legal information is not advice, and should not be treated as such.
Any legal information in this guide is provided “as is” without any representations or warranties, express or implied. Juniper Networks makes no representations or warranties in relation to the information in this guide.
You must not rely on the information in this guide as an alternative to legal advice from your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this guide.
Information correct at time of publication (2021).

Contact:

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schipol-Rijk, Amsterdam,
The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888-JUNIPER
(888-586-4737) or
+1.408.745.2000

Fax: +1.408.745.2100

Copyright: