Managed Security Services Distributor (MSSD)

Exclusive Networks Global Services

MSS: MANAGED SECURITY SERVICES

Service Overview

INTRODUCING MSSD

MSSD means Managed Security Services Distributor – an extension of the unprecedented value and 100% channel focus our partners expect from Exclusive Networks.

FOCUS ON YOUR BUSINESS

As cybersecurity challenges continue to grow in scale, scope and complexity, it is too important to leave it to chance, instead, leave it to the experts! MSSP's enable you to remain focused upon your business, safe in the knowledge that you have 24x7x365 security infrastructure in place. Reduce the burden upon in-house IT teams by outsourcing resource intensive security management, meaning that you do not have to recruit and retain highly skilled individuals, who are in very high demand, at a high cost to your business.

Choose the contract term that best suits your requirements, and benefit from multi-vendor and multi-solution support for your security infrastructure, and get back to focusing on your business!

YOUR CHALLENGES, SOLVED

Want to be sure you are able to tackle the current threat landscape with the right expertise while adhering to all compliance regulations for data?

- MSS fills the skills gap by providing expert oversight of core security infrastructure. Spend less on overtime and training budgets with 24/7 monitoring and alerting

Want to ensure you can dedictae IT resources to your core disciplines?

- MSS allows organisations some much-needed breathing space to pursue priorities without worrying about the increasing complexity of cybersecurity challenges

Need to reduce CAPEX liability within the business?

- MSS allow you to move to a fixed monthly payment OPEX model with SOC-as-a-service

SERVICES OFFERED

MSS driven by a 24/7 Global SOC Infrastructure

SOC:

- Permanently staffed
- SOC portal for live status and reporting tickets
- Enquiries answered by accredited and experienced engineers
- SOC 2 Type 2, ISO 27001 and ISO 9001 certified purpose-build webscale security automation and orchestration platform
- High levels of resilience and redundancy

MSS - MONITORING & ALERTING:

- Threat Event Enrichment, Analysis and Correlation
- Incident Monitoring, Alerting and RCA
- Remote Breach Support
- Security Dashboard
- Compliance Reporting
- AI-based threat hunting
- Post-breach investigation
- Service management reporting
- Security improvement advisories

MSS - PREVENTION & COUNTERMEASURES:

- Availability Monitoring and Backup
- Operational and Capacity Management
- Updates and Upgrades
- Policy Compliance and Best Practice Validation
- Device and Policy Configuration Change Management
- Automated Rules of Engagement
- Policy Topology Reporting
- Behaviour Baselining (*)

MSS: MANAGED SECURITY SERVICES

Solution Brief

EXCLUSIVE NETWORKS

LEAVE SECURITY TO THE EXPERTS

World class security-as-a-service, driven by a 24/7 global SOC infrastructure, with highly experienced and accredited engineers in place to respond to all queries. The webscale security automation and orchestration platform is SOC2 Type 2, ISO 27001 and ISO 9001 certified providing high levels of resilience and redundancy. Put the focus back onto your business safe in the knowledge that your security management is in place 24x7 across your network.

WE MANAGE

FORTINET

- NGFW (Fortigate)
- Secure SD-WAN
- FortiSwitch
- FortiAP

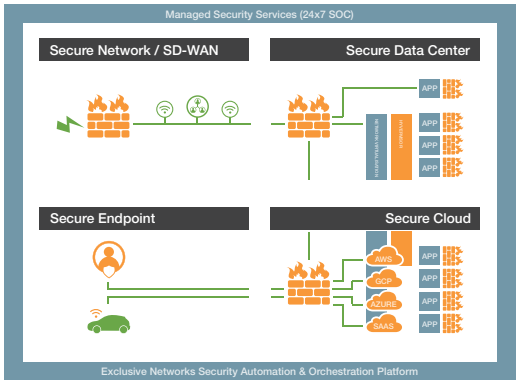
paloalto NETWORKS

STRATA
- NGFW

CORTEX
- Cortex-XDR Pro
- Cortex-XDR Prevent

PRISMA
- Prisma Access
- Prisma Cloud

CISCO
- Firepower
- Meraki MX Devices



SECURITY AUTOMATION & ORCHESTRATION PLATFORM

Risk:
Inventory of all assets and weighing the criticality to business continuity and compliancy.

IoG:
Every event is enriched, correlated and filtered by Indicators of Good. The residue is assumed to contain bad.

Machine vs. Machine:
Our countermeasure playbooks fight known bad and are improved with every SOC analyst action.

Policy:
Every policy degenerates in time; our Policy Engine and Security Delivery Manager enhance policy and automate countermeasures. The policy is composed of 14 years of best practices.

ZERO TRUST

SECURITY FRAMEWORK

- Identify and classify all data and associated risk
- Map all traffic and transaction flows
- Identify roles and assign people to a single role per dataset/application
- Design a logical segmentation of datasets/ applications
- Monitor the network; inspect and log the traffic; and update rules based on your behavior analytics
- Write rules on your segmentation or policy gateway based on expected behavior of the data (users and applications)

WE GOT THIS!
MSSD
BY EXCLUSIVE NETWORKS