NxtGen
Infinite Datacenter

Managed Security-as-a-Service

NxtGen Managed Security-as-a-Service (MSaaS)

Our customers have an urgent & critical need to secure their digital assets in the cloud and on their premises. They deserve the best people and technologies, NxtGen has the best resources in terms of people, technology and processes in India.

Our vision is to enable our customers with an Infinite Datacenter, taking out the complexity of running mission-critical infrastructure and letting our customers focus on applications. Managing security is critical ensuring peace of mind to our customers.

It is not enough that our cloud is secure, we have to ensure our customers are not compromised by the end-points & related other applications accessing their assets in our cloud.

The services portfolio covers threats from end-customers accessing customer applications, multi-cloud scenarios, customer end-points and other on-premise infrastructure. NxtGen is able to offer a 360 degree approach to securing its customers from Cyber-threats.

Log management

Service Name	Detailed Activities
Log management	1. Collect logs 24*7 from the in scope sources. 2. Retention of the log per the applicable legal, regulatory and compliance requirements.

Security Monitoring & Incident Response Services

Security event monitoring for network devices	1. Collect, monitor & analyze logs and incidents reported by the network devices based on agreed use cases. 2. Classify incidents, perform triage, escalation and investigation (RCA) as per an initially agreed process and parameters 3. Recommend and coordinate solutions / responses for high severity incidents 4. Publish operational and Management dashboards on Daily, weekly and Monthly frequency {Please note the above commercials are calculated assuming firewall is managing a pipe of 15 MBPS}
Network device management such as Firewall, Load Balancer etc.	1. Monitor device uptime and utilization / capacity 2. Carry out changes with proper prior approval / recommendation of client 3. Coordinate with Security device OEM (Original Equipment Manufacturer) and client for fault logging, fault rectification, and Return Materials Authorization(RMA) 4. Review of version updates and patch releases, and other updates on a monthly basis and advising the client on upgrading of the same. Support for upgrading the patches for devices under scope. 5. Provide reports for CPU utilization, errors, memory utilization, bandwidth utilization, connections and other health parameters of devices on Daily / weekly / fortnightly / monthly basis as mutually agreed 6. Provide reports for any failures / incidents along with details of resolution, root cause, preventive and proactive measures taken to avoid recuzzrrence.

Service Name	Detailed Activities
Security event monitoring for servers (OS and DB)	1. Collect, monitor & analyze logs and incidents reported by the servers such as Windows, Unix, Linux etc. based on agreed use cases. 2. Classify incidents, perform triage, escalation and investigation (RCA) as per an initially agreed process and parameters. 3. Recommend and coordinate solutions / responses for high severity incidents 4. Publish operational and Management dashboards on Daily, weekly and monthly frequency.
Security event monitoring for applications	1. Collect, monitor & analyze logs and incidents reported by the applications such as enterprise application, home grown, COTS etc. 2. Classify incidents, perform triage, escalation and investigation (RCA) as per an initially agreed process and parameters. 3. Recommend and coordinate solutions / responses for high severity incidents 4. Publish operational and Management dashboards on Daily, weekly and Monthly frequency.

Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and remedial assessment	1. Vulnerability assessments of devices for known vulnerabilities. 2. Perform the reassessment within 90 days for remedial actions after confirmation from the client. 3. Provide vulnerability assessment report with recommendations for remediation. 4. Final report with detailed findings, a risk rating, and suggestions for mitigating risk.
Penetration Testing Security with remedial assessment – Devices	1. Security testing of internet facing devices (Network devices, servers etc.) for security vulnerability/ bugs, their exploitability. 2. Provide guideline to client team for closure of issue. 3. Perform the reassessment within 90 days. 4. Provide penetration testing report with recommendations for remediation. 5. Final report with detailed findings, a risk rating, and suggestions for mitigating risk.

Devices Configuration Reviews

Automated configuration checks for network and servers devices as per the industry baselines	1. A secure configuration review checks for devices. This includes operating systems, network and databases. 2. Comparison of the script output against established PwC baseline settings. 3. Provide a safe/unsafe status check with detailed descriptions of unsafe findings and discuss those findings with administrators. 4. Final report with detailed findings, a risk rating, and suggestions for mitigating risk.

Application Security Testing

Service Name	Detailed Activities
Penetration Testing Security with remedial assessment –Web Application	1. Security testing of internet facing applications for application bugs, their exploitability. 2. Provide guideline to client team for closure of issue. 3. Perform the reassessment within 90 days. 4. Provide penetration testing report with recommendations for remediation. { We have assumed that a web application is limited to 25 pages. In case in scope web application has more than 100 pages the pricing will be calculated based on 4 units }

NxtGen Technology Pte Ltd.
4 Battery Road, #25-01, Bank of China Building, Singapore (049908)

NxtGen Datacenter & Cloud Technologies Private Limited
#05A 101 & 04A 101, Cinnabar Hills, Embassy Golf Link Business Park, Challaghatta,
Bengaluru, Karnataka -560071