Securing the Cloud - Solution Brief

Breach Detection & XDR

Cyberthreats are soaring and continuously targeting organisations with network, endpoint, and user-based attacks. Breach Detection & XDR prevents and detects threats on endpoints, networks, and user devices then triggers an automated investigation flow that reveals the attack scope and root cause and applies automated remediation.

Complete coverage of all attack vectors that involve endpoint, user and network requires complete protection. This type of defence usually entails the deployment and operation of multiple security products by a skilled team, which for most organisations is too complex and costly to operate.

A more effective and manageable solution is the implementation of an Autonomous Breach Protection platform that natively integrates the endpoint, network, and user prevention & detection of XDR with automated investigation and remediation, backed by 24/7 MDR services—placing end to end breach protection within reach of any organisation, regardless of its security team size and skill. XDR Prevention & Detection integrates the capabilities of Next-Generation Antivirus, Endpoint Detection and Response, Network Analytics, Deception and User Behavioural Analytics. Enhanced assessment of network activities is utilised to uncover and identify advanced threats that bypass less capable solutions.

Response Orchestration includes a full set of remediation actions to address infected hosts, malicious files, attacker-controlled network traffic and compromised user accounts. Remediation can be performed either directly on the endpoint or by utilising infrastructure components such as firewall or Active Directory. Response can be automated by gathering remediation actions into playbooks that are activated upon occurrence of respective alerts.

Access to a 24/7 SOC team of specialist threat researchers and security analysts that complement the solution can assist with in-depth investigation, proactive threat hunting, malware analysis and attack reports, ensuring that every security event is handled and resolved.

About NG-IT

NG IT Limited is a privately held IT Solutions partner providing next generation cloud infrastructure and cloud security. Our aim is to provide peace of mind for our customers so they remain focused on managing and growing their business.

Key Features

Comprehensive Solution
Single management platform and complete coverage from endpoint, user, and network-based attacks in one comprehensive solution.

Deception Capabilities
Decoy files, machines, user accounts, and network connections to detect, lure and occupy attackers.

Response Automation

- Automated root cause and impact analysis
- Actionable conclusions on attack origin and affected entities
- Elimination of malicious presence, activity, and infrastructure
- Intuitive flow layout of the attack and the automated response flow

Managed Detection & Response

- Alert monitoring
- Attack investigation
- Incident response guidance

Contact

t:	+44 (0)330 2233915
e:	webenq@ng-it.co.uk
w:	www.ng-it.co.uk

Registered Office
4 Oxford Court
Manchester
United Kingdom
M2 3WQ

Specifications within are subject to change without notice.