Securing the Cloud - Solution Brief

Threat Protection

Thousands of new strands of zero-day malware are created every day and traditional signature-based protections cannot keep pace. Sandboxing diagnostics take time and can fail to identify sophisticated malware that knows when it is being evaluated. Organisations need threat protection that can identify any threat quickly and efficiently to meet the demands of our cloud-first world.

Cloud applications and bring-your-own-device (BYOD) give organisations enhanced dynamism and efficiency, unfortunately they can also serve as proliferation points for malware when they are not properly secured. End user devices lacking adequate endpoint protection may upload infected files to corporate SaaS applications, which can then spread malware to other devices and connected applications.

A solution fully deployed in the cloud has the capability to deliver threat protection wherever an endpoint is located, and by leveraging machine learning and deep analysis of 500 billion events processed daily to identify both known and zero-day malware it meets the needs of any modern enterprise. By incorporating this next generation technology directly into a cloud access security broker (CASB), any kind of malware can be detected across an organisation's entire cloud footprint as well as on any device that accesses corporate IT resources. Unlike threat tools that are geared towards generating alerts, the CASB solution can be configured to detect and remediate threats automatically based on policies meaning there is no need to wait for IT to intervene.

Traffic is mediated between cloud applications and devices in order to enforce granular security policies on data in transit, by incorporating AI based threat detection capabilities malware can be identified and blocked in real time as infected files are uploaded to any cloud application or downloaded to any device. As enforcing policies and scanning for malware through traditional, agent-based tools can be a challenge on personal devices, this cloud-based ATP is a perfect fit for organisations that enable BYOD.

Key Features

Best of Breed Detection

- Behaviour-based detections use AI to identify zero-day malware.
- Autonomous block/allow decision requires no intervention from IT.
- Scan with the engine of your choosing; complement your existing AV tools.

Real-time protection

- Halt threats at download and upload from any cloud app or device, managed or unmanaged.
- Detect and remove threats already at rest within the cloud.
- Low-latency solution requires no sandbox, identifies malware in milliseconds using file characteristics.

Painless deployment

- Hosted on AWS for fast, scalable deployment.
- Minimal setup required – add ATP detection to policy database.
- Invisible to end users with no agents required on unmanaged devices and no signature updates.

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

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 focussed on managing and growing their business.

© 2022 NG-IT Limited. All rights reserved. No portions of this document may be reproduced without prior written consent of NG-IT Limited. Brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.
Specifications within are subject to change without notice.