

PROTECT AGAINST BUSINESS
EMAIL COMPROMISE

SMARTER EMAIL SECURITY

Today's targeted attacks use social engineering that can trick even the most discriminating user into opening an email and clicking a malicious link. The growing adoption of cloud mailbox services like Office 365 mean that blended attacks can target an organisation from more than one side.

Blended attacks use web links to phishing sites, advanced malware that is difficult to detect and insider threats and outbound attacks that put intellectual property and customer assets at risk. More recently we have seen a rapid increase in ransomware attacks that maliciously encrypt key business data.

72% OF REPORTED UK CYBER
ATTACKS ORIGINATED FROM
EMAIL OR BEING DIRECTED
TO FRAUDULENT WEBSITES.

IT IS NO LONGER SUFFICIENT TO RELY ON BASIC
EMAIL SPAM FILTERS AND FIREWALLS; YOU NEED
CONTENT SECURITY THAT CAN MONITOR INNOCUOUS
LOOKING CONTENT LONG AFTER IT HAS BEEN
DELIVERED TO SPOT LATER THREATS.

THE EMAIL SECURITY THREAT LANDSCAPE

£750M

loss from
ransomware.

£4BN

the cost of compromised
business email.

67%

of malware delivered
via phishing.

A SMARTER EMAIL SECURITY CHECKLIST



GET FULL
VISIBILITY

Awareness at the perimeter isn't enough. Knowing where email is coming from and what it contains after entering the network is vital. Retrospective security gives you the ability to see and contain threats across your environment—even sophisticated attacks that morph over time.



PROTECT
AGAINST BEC

Business Email Compromise (BEC) threats use social engineering to trick recipients into an action. To outsmart BEC, use a combination of user education, validation and integration of executive user identities, and IT monitoring such as sender policy frameworks.



AUTOMATE YOUR
SOLUTION

When malware infiltrates your network, an automated retrospective remediation tool will find and contain it before serious damage occurs. Intelligent monitoring and analytics can discover polymorphic malware, trigger reputation analysis, and prioritise fixes automatically.



FOCUS ON
DATA LEAKS

Reduce the chance of critical data leaving the network, maliciously or accidentally, with content-aware, policy-based data loss prevention capabilities, outbound email scanning, content encryption, and intelligent rate limiting.



ENCRYPT ACROSS
THE ENTERPRISE

Secure your business communications, and meet regulatory compliance requirements, with multi-layered encryption. Advanced encryption key services protect financial, personal, and intellectual-property data with recipient registration, authentication, and per-message/per-recipient control.

CISCO EMAIL SECURITY

The Cisco Email Security solution offer high-availability layers of email protection against the dynamic, rapidly changing threats affecting organisations today.

SIMPLE SET UP AND AUTOMATION

Get protected within minutes with a solution that is easy to set up, cost-effective, on-guard and up-to-date.

MULTI-DEVICE SUPPORT

Cisco email security supports a range of end-points including desktop, mobile, laptop and tablet.

FLEXIBLE DEPLOYMENT OPTION

Deployment options include on-premises or in the cloud, with hybrid models and managed services.

WHY NATILIK?



We help our clients to take a holistic and 'threat-centric' approach to security, providing solutions that work seamlessly together to secure your entire network.



For IT, we reduce management overhead while reducing both time to detect and remediate breaches, and for the end-user we provide a secure environment in which to work.



London HQ and offices in Sydney and New York with 24/7 follow the sun support team which provide a consistent experience globally.

SEE WHERE WE CAN TAKE YOU

Alternatively take a free 45-day trial, find out more here www.natilik.com/email-security-trial