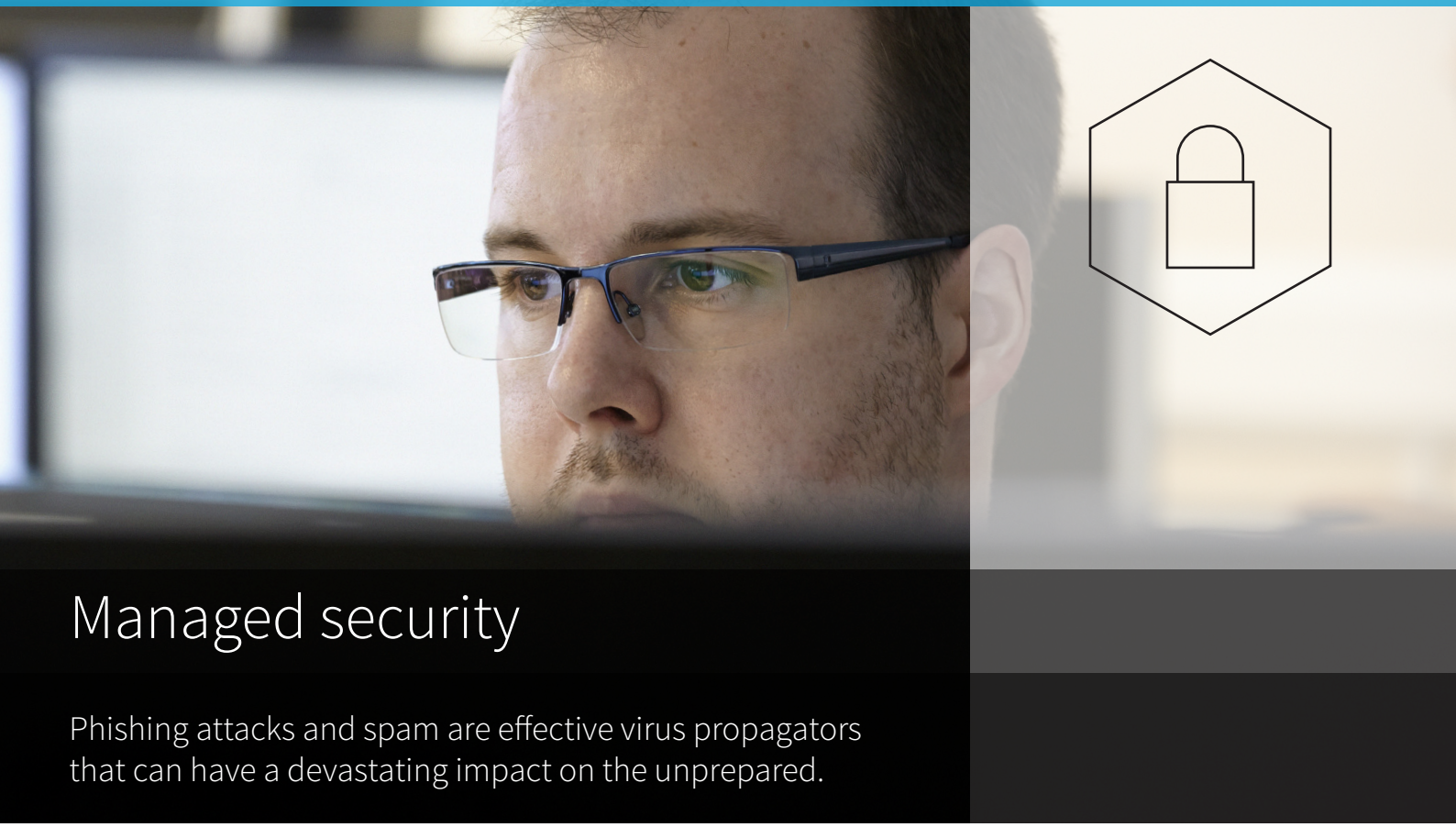

Managed security

Phishing attacks and spam are effective virus propagators that can have a devastating impact on the unprepared.

One careless click and your business could be compromised. Increased usage of email and web-browsing dramatically increases the risk of contamination.

Communication and training are critical components in an organisation's security strategy. Threat awareness and remedial action prevent unauthorised access to the company's internal systems and data. To avoid risk, this process must be:

• planned • effectively integrated • continually monitored • supported, and improved

We provide best-of-breed security technology with real-time threat analysis and detection. Our managed security portfolio offers resilience, scalability and flexibility to organisations for a simple low-cost monthly charge.

Direct access to our experienced security consultants gives you peace of mind.

Benefits of managed security

- Protect your brand and bottom line by quickly detecting and responding to attacks. Our security solutions give you the visibility and insights to make decisions faster and with confidence
- Email security solutions deliver protection from malware, phishing, spam and targeted attacks for cloud hosted or on-premise mailboxes
- Website security solutions utilise cutting-edge SSL certificates to trust and encrypt end-to-end data. Our products further provide anti-malware and anti-virus vulnerability protection

Threats

- Email spam
- Email worms
- Network viruses
- Spyware and malware
- Data theft
- Phishing attacks

Key features

An enterprise class solution	Utilise the most innovative software to protect your business from spam. Receive e-mail via in-stream filtering that scans in real-time and stores inbound emails. This avoids delay, and is invaluable if your server goes offline
Simple configuration	Flexible configuration options allow you to determine what constitutes spam. Personalised white lists, black lists and rules can be set up and changed via a web interface
Comprehensive reporting	Frequent detailed reports provide visibility of the volume of email and type of threats so you can see that your business is constantly protected
Scans outbound emails	Choose an optional add-on that checks out-bound emails against known phishing sites and protects your business from users inadvertently propagating a virus or replying to a malicious email, which could result in your company being black listed

Email protection

- Content filtering
- Hosted anti-virus filtering
- Hosted anti-spam filtering
- Malicious content filtering
- Policy management
- Linked to an active directory
- Black and white listings management (optional)
- Monthly status and threat reporting (optional)

Anti-virus: servers and workstations

- Anti-virus, anti-spyware and anti-malware: monitoring and management of all servers, PCs and laptops
- Policy management, designed to meet the needs of the organisation and use of applications
- Web content filtering for all devices
- Enforce web usage policies to all users regardless of location
- Customisable access levels
- Web usage policies cover all standard restrictions such as gambling etc. and can also be tailored to your company web usage policies

Managed router and firewall security

- Frequent status and threat reporting on usage of licenses across your install base
- Management of VPNs
- Managed firewall rules and access lists
- Traffic management
- Asset and warranty management
- Manage and renew SSL certificates
- Firewall and router configurations are backed up to Ni for disaster recovery purposes
- Frequent health and usage reporting, including traffic usage

80% of all email traffic is spam. Once on the desktop, it can put your entire business at the mercy of the employee doing the right thing.

Be prepared, protect your IT environment from attack.

Talk to us today for a quote.

Network Interlinks Ltd.
318 Worple Road
London
SW20 8QU

+44 (0)20 8739 0660

theteam@networkinterlinks.com

www.networkinterlinks.com