TRUSTMARQUE
Part of Capita plc

NETWORK AND PERIMETER SECURITY

Today's network and perimeter

As the progress of digital solutions and cloud continues to develop, so do the threats from cyber criminals. They can exploit gaps and vulnerabilities that can appear as networks and perimeters grow to meet your organisation's requirements.

Email Security

91% of targeted attacks start with an email and these threats are constantly evolving. The challenge is in detecting and stopping both known and zero day threats across malware, credential phishing, impersonation and email fraud.

Firewall

Your perimeter is exposed to a vast range of attacks, including distributed denial of service, vulnerability exploits, data leakage and advanced persistent threats (APTs).

Web Security

Your employees increasing use of web and cloud services means that they are likely to be one of your fastest growing threat vectors. Ensuring your users, regardless of location, can only access them appropriately and securely is of paramount importance. Furthermore, the growth of SaaS poses a new challenge around how you control and manage shadow IT and shadow data.

Stretching the boundaries

Your network is changing rapidly so it's paramount that your perimeter defences are up to the challenge. The rise of cloud, IOT and a mobile workforce may have moved some risks outside your perimeter, however a robust perimeter around your digital assets is still vital to a good security strategy.

A comprehensive approach to firewall, email and web security is essential.

TRUSTMARQUE
Part of Capita plc

Modern tools to meet modern challenges

Next Generation Firewall

Next Generation Firewalls are more than just a firewall. Acting as a critical tool in protecting your organisation from cybercrime, they can look at application level traffic, sandboxing and IPS. With a vast array of vendors producing firewalls, from budget to Gartner leading, we can help you understand which one is right for your requirements and budget.

Email

Safeguard your Office 365, G-Suite and on-premise email users against phishing, spear attacks, ransomware and spam by adding layers of added protection. Talk to us to find out how we help you to deliver Domain-based Message Authentication, Reporting and Conformance (DMARC). There is no such thing as a silver bullet against email attacks, but with DMARC implemented well to combat email fraud… it comes close.

Web Security

Ensure your users only access appropriate content from work devices. By limiting risk, this allows protected access through web isolation which blocks malicious websites, prevents social engineering and stops phishing attacks.

Cloud Access Security Brokers (CASB) and Data Loss Prevention (DLP)

CASB and DLP software will identify shadow IT and let you evaluate your risk across tens of thousands of applications by monitoring and protecting your sensitive data in your cloud applications.

Why Trustmarque?

Trustmarque helps you understand your organisation's true risk and exposure. Our experts will recommend the best solution for your organisation by understanding your unique requirements. We have a fine-tuned portfolio of services and partners that gives you access to the most relevant and advanced solutions. In addition, we have invested highly in staff training and are proud of our expertise as well as our relationships and certifications with the industry's leading vendors. We are uniquely placed to leverage both the strength of our strategic ecosystem partners and Microsoft.

Founded in 2004, acquired by Capita in 2013 and now a part of Trustmarque, our team is a multiple award-winning practise that has been in operation for 17 years. We have over 55 in-house engineers and a customer facing Security Managed Service manned 24x7x365 providing industry leading support coverage for our strategic security vendors.