Advanced Cyber Security Solutions

Cybercrime Pays

Next in our series of posts about protecting your business from cyber threats and data breaches, we will look at a range of solutions designed to safeguard your network from infiltration and detect any malicious software that is present. Cybercrime is a multi-billion dollar annual market. This means attackers are very well funded, and will continue to produce better, more disruptive malware and viruses. FBI research has found a single ransomware campaign can generate $60 million annually. Capable of generating massive profits for the cyber criminals, ransomware and other forms of cybercrime are with us for years to come.

In this blog, we will discuss how some advanced security solutions can help enhance your levels of protection and reduce your risk of infection.

Umbrella Roaming

Umbrella Roaming is a Cloud delivered service that protects all your employees' devices, even when they are not connected to your network. It works by blocking user requests to malicious domains at the Internet DNS layer, which means a connection is never made.

Umbrella Roaming constantly analyses real-time, diverse data sets to learn Internet activity patterns. It then uses machine learning and complex algorithms to spot trends, patterns and threats before an attack even happens. Because Umbrella Roaming is a Cloud delivered service, it is completely device and platform agnostic, and can eliminate potential blind spots when users are not in the office.

Currently, if users are working remotely without a VPN connection the perimeter security such as a firewall is being bypassed. Umbrella Roaming ensures every device gets the same level of corporate protection regardless of where your employees are based, working from home, in the office or at a motorway services.

ISE Potential Threats

Do you have complete visibility of all the devices connecting to your network? Do you know if all those devices are security compliant and only running approved applications? Identity Services Engine (ISE) is an application that enables you to better manage and secure your corporate network. ISE includes a posture service allowing you to check and verify the state of all devices connecting to your network before granting them access.

Working across both wired and wireless, corporate and guest networks you can control the devices connecting, and make sure they met your specified criteria for access. For example,

what operating system is a device running? Is it patched sufficiently? Does it have enterprise anti-virus installed and is it up to date? If not, you can quarantine the device, and give the user limited or no access until they have addressed the problem. This can significantly increase your level of control over devices that have the potential to threaten or infect your network.

Before, During & After an Attack

Advanced Malware Protection (AMP) for Endpoints provides protection against the most advanced cyberattacks, will prevent breaches and block malware at the point of entry. It will also rapidly detect, contain, and remediate advanced threats if they evade front-line defences, such as firewalls, and get inside your network. As we have said in previous blogs, no prevention method will catch every threat. However, AMP will help you be prepared when advanced malware does get inside. AMP enables you to see executable, file activity across all of your endpoints, so you can spot threats quickly and fix them.

One area where AMP differs from other solutions is it continues to monitor and record activity after a file is on the endpoint. It continues to watch, analyse and record file activity, regardless of the file's disposition. When malicious behaviour is detected, AMP shows you the recorded history of the malware's behaviour over time: where it came from, where it's been, and what it's doing. The malicious file is then quarantined automatically, any damage done is fixed and further harm prevented across all endpoints on your network.

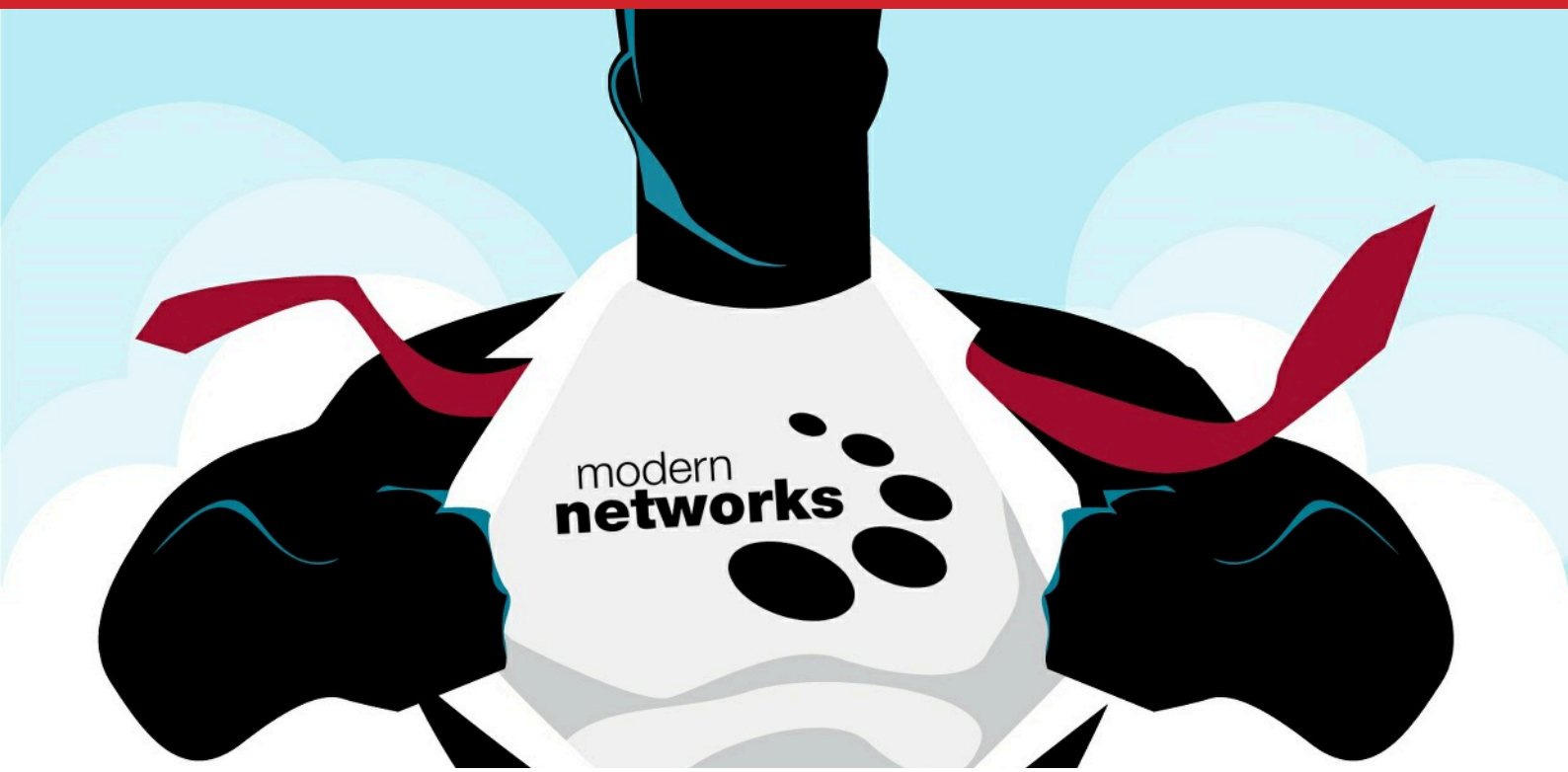
Threats You Cannot See

On average, malware goes undetected for around 200 days. That's 200 days cybercriminals are inside your corporate network doing harm. To even the playing field, Stealthwatch uses flow data to give you incredible visibility across your entire network including the data centre and Cloud. First, it establishes a baseline for normal network behaviour. Next, it uses advanced analytics to identify unusual patterns and alert you of possible threats.

Stealthwatch can help you spot a compromised device talking to an external command and control server, detect abnormal traffic and identify data exfiltration, if unusual file transfers are taking place. Without an application like Stealthwatch, the first time you learn there's been a data breach is when your customers' data goes on sale or is splashed across social media.

Choose Wisely

These are just a handful of advanced cyber security solutions available to you. They vary in complexity and costs. Naturally, we would recommend you evaluate your current levels of protection; check they are adequate for your needs and compliant with your industry standards. However, before you rush out and spend a shed load of cash because the Board have been reading the newspapers; take a moment to consider your security needs and options. First, you need to agree what are your security priorities. Next, shortlist vendors and applications that



meet your requirements now and for the near future. Get some independent advice and look at what existing customers have to say about applications. Look at total cost of ownership (TCO) and any hidden fees. You will also want to think about support and service levels. Take the applications out for a test drive, and give your IT people a chance to look under the bonnet.

About Us

Modern Networks provides IT and telecoms as a managed service to over 1600 commercial properties across the UK and hundreds of enterprise clients. We provide everything from computing, enterprise anti-virus, web content filtering, storage, backup and recovery to local area networks, VoIP telephony, broadband and mobile solutions. All our services are fully managed, continually monitored and expertly supported.

Contact Us

We trust that you've found this third blog in our series on cybersecurity and data protection useful? Please feel free to contact us should you have further questions.

Images courtesy of Freepik.com, freevector.com, pixabay.com and stockvault.net