DDOS PROTECTION AND MITIGATION

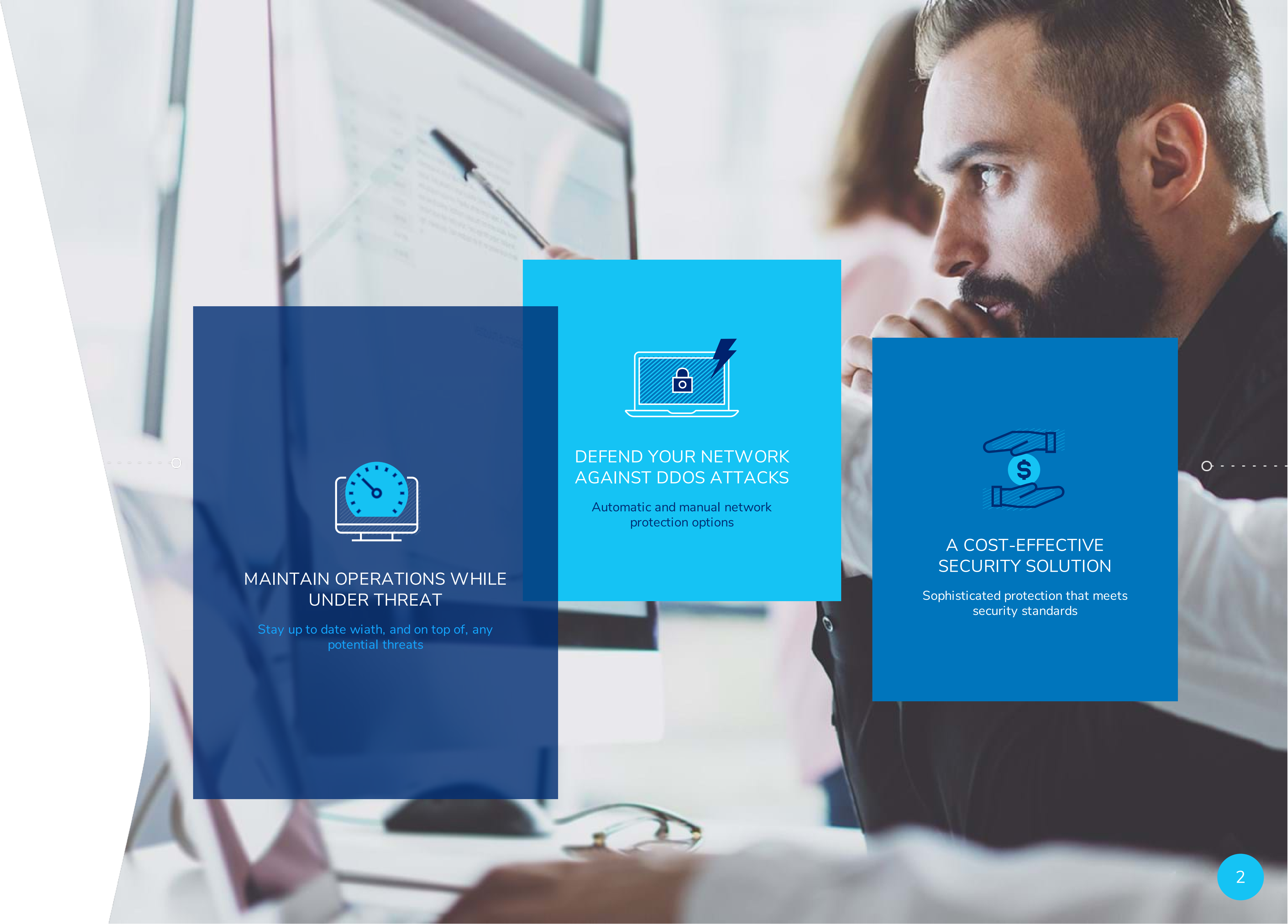
EFFECTIVE DENIAL-OF-SERVICE PROTECTION

While some organisations face a greater risk of distributed denial of service (DDoS) attacks than others, anyone with an online presence can fall victim to this sophisticated form of cybercrime.

Following a DDoS attack, organisations could face significant financial, data and productivity losses, and damage to their reputation. The costs of finding, repairing and recovering from an attack can also be excessive.

You may not be able to prevent DDoS attacks, but you can equip yourself with the right defences to deal with them if they happen.

DDoS Protection and Mitigation protects your organisation from the consequences of even the most advanced, robust attacks. It detects when you've been compromised, and notifies you so you can act immediately.



MAINTAIN OPERATIONS WHILE UNDER THREAT

Stay up to date wiath, and on top of, any potential threats

DEFEND YOUR NETWORK AGAINST DDOS ATTACKS

Automatic and manual network protection options

A COST-EFFECTIVE SECURITY SOLUTION

Sophisticated protection that meets security standards

BUSINESS BENEFITS

MAINTAIN OPERATIONS WHILE UNDER THREAT

Stay up to date with, and on top of, any potential threats

Protect your business against complex security breaches

As technology evolves, DDoS attacks are becoming more sophisticated, complex and intense, making it harder to block traffic and catch the perpetrators.

DDoS attacks are the most prevalent denial-of-service (DoS) attacks, and therefore the biggest risk to your organisation. Constantly evolving attack methods means there's no one technique, system or tool that can handle all potential threats. Attacks from multiple sources outside the network aren't easy to detect – it's possible that you can be targeted, or even attacked, without knowing it.

Mitigate the risk of a full shutdown

DDoS Protection and Mitigation helps you manage the risks of network downtime associated with attacks. A DDoS attack attempts to slow down or even shut down the targeted server, site or network by inundating it with illegitimate traffic. By being able to redirect traffic when the network is under threat, you can safely continue operations and won't be at risk of shutting down completely. During an attack, some services may be slower or temporarily unavailable, but you will still mitigate the critical risks with DDoS Protection and Mitigation.

If you do experience an attack, you'll be able to download a report with information that will assist you to identify and address security weaknesses

Safeguard against associated risks

Falling prey to a DDoS attack comes at an immense cost. If you're unable to detect and mitigate an attack, you could face significant losses, in the form of:

- Direct theft (money, data or intellectual property)
- Lost business and productivity
- Poor customer experience and customer churn
- Reputation damage from bad publicity
- Potential lawsuits or service level agreement penalties

There's also the high cost of resources needed to find and repair the problem. Thanks to DDoS Protection and Mitigation, you can successfully safeguard your business against these serious, and often unexpected, risks. When it comes to DDoS attacks, prevention truly is better than cure.

DEFEND YOUR NETWORK AGAINST DDOS ATTACKS

Automatic and manual network protection options

Detect, mitigate and recover from internationally sourced DDoS attacks

DDoS Protection and Mitigation is a security service that makes your organisation resilient to even the most advanced and tenacious volumetric attacks, the most common DDoS attack, which attempt to slow down (or shut down) your sites, networks or servers by flooding them with huge volumes of traffic.

The service instantly analyses the type and scale of the attack, and quickly redirects network traffic through our scrubbing centre, putting you in a strong position to combat these large-scale attacks.

Options for managing traffic under threat

We offer three fully hosted, cloud-based packages to help you manage the risk of loss and damage caused by these attacks, and protect your corporate information, intellectual property and client data. They give you different options for handling network traffic in the event of an attack so you're able to maintain normal operations:

- **Cloud Blackhole Mitigation** sends host server requests to a black hole.
- **Cloud Scrubbing Mitigation** scrubs all traffic so only clean traffic gets through.
- **Hybrid Cloud Mitigation** automatically detects application, TCP-state and volumetric attacks, and combines a cloud-based scrubbing service with an onsite CPE solution.

All packages offer:

- Automatic detection of internationally sourced volumetric DDoS attacks
- Protection of traffic via our scrubbing centre
- Real-time alerts, reports and traffic dashboards on our self-service portal

Start the attack mitigation process automatically or manually

You can choose to start the attack mitigation process automatically or manually. Automatic mitigation starts as soon as an attack is detected, while manual mitigation notifies you of a detected attack. You can then log into our self-service portal to view the details of the attack and start the mitigation process.

OTHER FEATURES

A COST-EFFECTIVE SECURITY SOLUTION

Sophisticated protection that meets security standards

Hassle-free management

Because DDoS Protection and Mitigation is a fully managed service, you won't have to invest in and maintain the hardware and software required to monitor and manage potential threats which greatly assist in cost savings. We manage the cloud devices that run the solution, based on your policies. You just need to manage the policies – and tell us when they change. You only have one point of contact and one service provider to deal with which takes away the admin headache of running advanced protection software across and entire organisation.

Service and support, wherever you are

Cybercriminals are never off the clock, and neither should your DDoS protection solution be.

Our 24/7 support means you can rest assured that help is a quick phone call away, while lights-out management gives you control of your service, wherever you are. Most of all, you can trust the protection of your systems to our expertise, so you don't lose focus on what you do best.

Fully compliant

When it comes to security services, it is essential that your systems and processes are up to date and meet the necessary requirements and standards. DDoS Protection and Mitigation meets Federal Information Processing Standard Publication (FIPS) 140-2 Level 3 standards. We use the latest technology and intelligence to provide effective mitigation against attacks that compromise the security of your systems and data. We use Arbor Peakflow SP Threat Management System technology together with an Arbor Availability Protection Service for maximum protection.

SECURITY

INDUSTRIES MOST AFFECTED BY CYBERCRIME

Sean Nourse

Chief Solutions Officer

SECURITY

WHAT A SECURITY BREACH IS REALLY COSTING YOUR ENTERPRISE

Sean Nourse

Chief Solutions Officer

Enterprise Level Security Risk Assessment

SECURITY

CHAT TO US

MORE FROM SECURITY