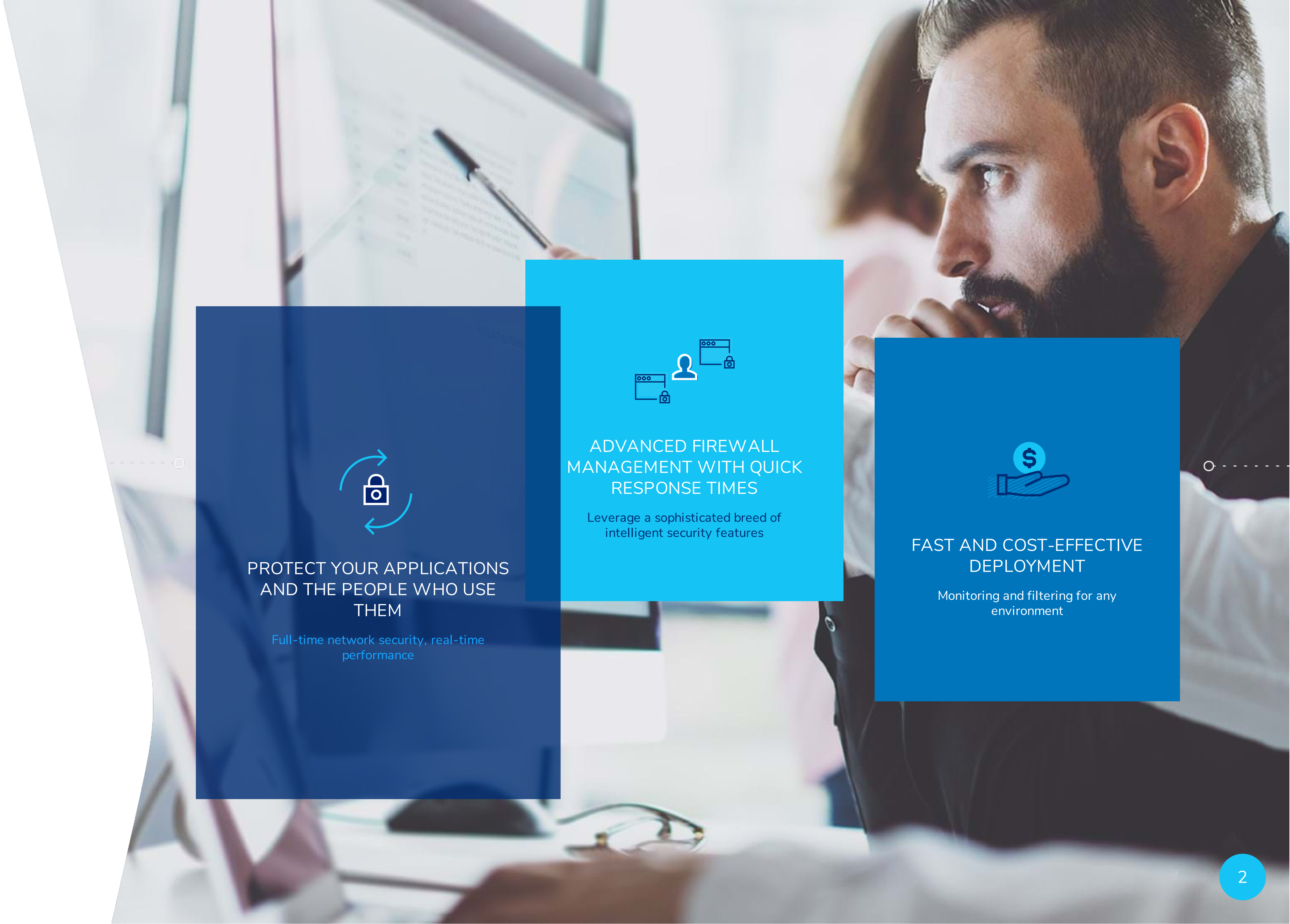
WEB APPLICATION FIREWALL

UNMATCHED PROTECTION FOR WEB-BASED APPLICATIONS

Your website and web-based applications can be exploited by hackers in order to gain entry to – and control of – information stored in the application’s backend databases.

Because these types of attacks are directed at the applications themselves, conventional firewalls or intrusion prevention systems can’t accurately detect and prevent them. You need a network security system that monitors traffic to and from the application and prevents unauthorised access to the application and its contents.

Web Application Firewall provides specialised, layered application threat protection to protect your web-based applications and Internet-facing data from attack and data loss.



PROTECT YOUR APPLICATIONS AND THE PEOPLE WHO USE THEM

Full-time network security, real-time performance

ADVANCED FIREWALL MANAGEMENT WITH QUICK RESPONSE TIMES

Leverage a sophisticated breed of intelligent security features

FAST AND COST-EFFECTIVE DEPLOYMENT

Monitoring and filtering for any environment

BUSINESS BENEFITS

PROTECT YOUR APPLICATIONS AND THE PEOPLE WHO USE THEM

Full-time network security, real-time performance

Protect your organisation against a range of attacks

Web Application Firewall protects your organisation and the people who use your web-based applications from sophisticated threats such as SQL injection and cross-site scripting (XSS) and cross-site request forgery (CSRF).

Hackers can retrieve, change or even delete data by using SQL injection attacks. All they need to do is send a command to your database through one of your own web-based applications. In the case of cross-site scripting, or XSS, the attacker can even insert malicious scripts into your database. These are executed by an individual user's browser to redirect the user to another location, show fraudulent content, or steal cookies and other sensitive information, such as credit card numbers and personal details. Hackers can also use XSS to impersonate the user in order to gain further access to your data. In a CSRF attack, the user's browser is forced to perform unauthorised requests from a trusted website.

With Web Application Firewall, your data is protected against these attacks in a fast, secure and reliable way.

Manage resources better in line with best practices and regulation

The Web Application Firewall platform helps you to counter attacks that could result in identity theft, financial fraud and corporate espionage – high-risk events with severe consequences. Web Application Firewall has an intelligent, application-aware data compression and optimisation engine that increases application performance and improves resource utilisation and application stability. This reduces server response times, which means your resources are used correctly, quickly and effectively to provide round-the-clock application protection.

The system also delivers the technology you need to enforce government regulations, industry best practices, and internal policies. The Vulnerability Scanner module provides a comprehensive solution for meeting certain security requirements of the Payment Card Industry Data Security Standards.

ADVANCED FIREWALL MANAGEMENT WITH QUICK RESPONSE TIMES

Leverage a sophisticated breed of intelligent security features

An auto-learning security system

Ensuring that a web-based application is free of security vulnerabilities can be difficult, given the ongoing discovery of new vulnerabilities, patching challenges, code revisions, the inherent difficulty of vulnerability identification and even access to the application code.

The Web Application Firewall system uses advanced techniques to analyse traffic flowing to and from the application in order to detect these kinds of attacks. The auto-learn profiling capability means it can build a comprehensive network security profile for each application, and use this as a model for protecting the application against any known or unknown attacks.

Anti-web defacement to restore original content, fast

When it comes to preventing reputational damage, quick response times are key should your business fall victim to a cyber-attack.

Attackers can change the appearance of a site or webpage and alter the content in a way that can severely damage your reputation and the longer you are unaware of the defacement, the worse the damage can be. Being able to restore that original lost content, however, can often be an overlooked component of web-based firewall strategies. Sometimes you are unable to return the content to its original state, which means extra time, money and resources spent to restore the information.

Our anti-web defacement component has unique capabilities for monitoring protected applications for defacement. It automatically detects these incidents and quickly reverts your site to a stored, approved version, helping you prevent any further damage or losses while you focus on addressing and rectifying other affected areas of the business.

FAST AND COST-EFFECTIVE DEPLOYMENT

Monitoring and filtering for any environment

Simple deployment and high availability

When it comes to securing your web-based applications, the faster you set up the necessary security systems, the better. Web Application Firewall can be deployed quickly, in any environment, drastically reducing the time required to protect your Internet-facing data and helping you manage the challenges associated with policy enforcement and regulatory compliance.

A failover option allows for a network-level failover in the event of unexpected outages, while integrated bypass interfaces provide additional fail-open capability, ensuring that traffic will still flow in the event of control failure.

Quick reporting to help identify threats

By viewing your real-time data statistics and detailed reports, you can analyse web application usage from multiple vectors. This gives you the opportunity to map requests to their geographic location, which means you can block access from specific countries to further enhance your security settings.

Although a Web Application Firewall is an intelligent system that auto-learns the security profile of each application, you can still contact us for 24/7 support and service to make sure your web-based applications are protected and any security threats managed at all times, no matter what.

SECURITY

A STEP-BY-STEP GUIDE TO PERFORMING A SECURITY RISK ASSESSMENT

Sean Nourse

Chief Solutions Officer

SECURITY

OUR SECURITY SOLUTIONS REDUCE YOUR ONLINE RISK

Sean Nourse

Chief Solutions Officer

PROTECT

CHAT TO US

MORE FROM SECURITY