



MK Dons CASE STUDY

ESET Defends the Net for MK Dons

League One football team the MK Dons switches malware defence to ESET for the entire Milton Keynes based complex including stadium, hotel and conference centre.

Customer

Part of the UK's bid for the 2018 World Cup, stadiummk is a conference centre, hotel and home to local football club, the Milton Keynes Dons. Currently in League One, the club has ambitious plans to reach the Premier League with a strategy of signing solid players and nurturing new talent.

Computers are used throughout the whole complex from stadium ticket sales to administrating MK Dons SET, a sports and educational trust that encourages a healthy lifestyle, whilst providing football opportunities for players as young as three years old. Last year the MK Dons' IT infrastructure increased significantly with the opening of the Doubletree by Hilton hotel, which is fully integrated into stadiummk.

Challenge

"We had two main criteria when considering our antivirus strategy, reliable protection and cost," explains MK Dons' IT Manager, Steve Ward. "Looking at the price to renew our contract with McAfee it seemed comparatively expensive against other similar products on the market. We also wanted to consider additional protection for our laptop users in areas where the machines maybe used outside of the protection of the corporate firewall. Protecting an IT infrastructure against malware attack is always a challenge, there's no telling where the next strike will come from, or what shape it will take."

Solution

Endpoint Antivirus was installed on the machines requiring anti-malware protection only, and ESET Endpoint Security was deployed for the club's fifty or so mobile users. ESET Endpoint Security affords users additional protection over the antivirus product with the inclusion of a personal two way firewall and antispam protection. Using predefined rules, the firewall protects the computer against intrusion from potentially dangerous outside networks or computers, by analysing all incoming traffic and prevents unauthorised outgoing traffic.

"One of the first things that stood out was the cost," continues Steve Ward. "I also liked the Remote Administrator feature which makes it far easier to manage the entire antimalware system than the previous deployment tool and therefore making it inherently more secure. In addition, the ability to centrally manage policies increases ease of management further still. When it comes to accuracy, ESET is always on the ball," concludes Steve Ward.



A comprehensive solution for company endpoints with multiple layers of protection including Antivirus, Antispyware, Firewall and Web Control. Remote administration enables centralised management from a single console.

System Requirements:
Windows® 7, Vista, XP, 2000,
Windows Server 2000, 2003, 2008, 2008 R2
Processor Architecture:
Intel®/AMD® x86/x64

Antivirus and Antispyware

Eliminates all forms of threats, including viruses, rootkits, worms and spyware, keeping your network protected online and off. Optional cloud-powered scanning utilises our reputation database for increased scanning speed and minimal false positives.

Host-based Intrusion Prevention System (HIPS)

Provides tampering protection and protects the system registry, processes, applications and files from unauthorised modification. You can customise the behaviour of the system down to every last detail and detect even unknown threats based on suspicious behaviour.

Web Control

Allows to limit access to select website categories by a way of automatic in-the-cloud classification. Create detailed rules for user groups to comply with your company policies and block sites generating high traffic volume.

Trusted Network Detection

Lets you define trusted networks and protect all other connections with strict mode, making company laptops invisible in public Wi-Fi networks in hotels, airports and at conferences.

Two-way Firewall

Prevents unauthorised access to company network and protects company data from exposure. Remote administration provides a firewall rule merge wizard that makes aggregating firewall rules in the network a snap.

Client Antispam

Protects your company communications from spam and email-borne threats. Set white- and blacklists and self learning separately for each client or group. The antispam natively supports Microsoft Outlook and also filters POP3, IMAP, MAPI and HTTP protocols.

Device Control

Lets you block unauthorised media and devices based on pre-set rules and parameters. Set access permissions (read/write, read, block) for individual media, devices, users and groups.

Component-based Installation

Install any or all of these security components: firewall, antispam, web control, device control, Microsoft NAP support, and web access protection. You can also remotely enable/disable installed modules.

Low System Demands

Ensure proven detection while leaving more system resources for programs you use daily. Our software also runs smoothly on older hardware, saving your time and costs of having to upgrade your endpoints.

Multiple Log Formats

Save logs in common formats - CSV, plain text, or Windows event log for immediate analysis or harvesting. Take advantage of data being readable by 3rd party SIEM tools; RSA enVision is supported directly via a plug-in.