ESET Defends the Net for MK Dons

League One football team the MK Dons signs-up ACS to switch 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, stadium ***mk*** 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 the stadium***mk***.

The MK Dons FC relies on assistance from ACS for its hardware and software needs. Voted one of the best companies to work for by The Times, ACS specialises in providing support and services to public and private organisations, so when the club's antivirus contract came up for renewal MK Dons' IT Manager, Steve Ward, turned to them for advice.

CHALLENGE

"We had two main criteria when considering our antivirus strategy, reliable protection and cost," he explains. "Looking at the price to renew our contract with McAfee it seemed comparatively expensive against other similar products on the market, so we asked ACS for some recommendations. 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."

SOLUTION

ACS proposed that Endpoint Antivirus be installed on the machines requiring antimalware protection only, and that ESET Endpoint Security be deployed for the club's fifty or so mobile users. "One of the first things that stood out from ACS's proposal was the cost," continues Steve Ward. "Besides being considerably cheaper, ESET Endpoint Security would enable us to consolidate the additional protection required for the laptops, bringing further savings too. I also particularly 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."

"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. However, when it comes to accuracy, ESET is always on the ball," concludes Steve Ward. "Together with ACS we can be confident that we have the best defence whenever malware strikes."

ENDPOINT SECURITY
FOR WINDOWS

ESET Endpoint Security delivers comprehensive IT security for your business via multiple layers of protection, including our field-proven ESET NOD32® detection technology, complete data access protection and fully adjustable scanning and update options.

Keep your system running at its best thanks to low system demands, virtualization support and optional cloud-powered scanning.

And oversee it all effortlessly with our completely redesigned, user-friendly remote administrator tool.

Antivirus and Antispyware	Eliminates all types of threats, including viruses, rootkits, worms and spyware Optional cloud-powered scanning: Whitelisting of safe files based on file reputation database in the cloud for better detection and faster scanning. Only information about executable and archive files is sent to the cloud – such data are not personally attributable.
Virtualization Support	ESET Shared Local Cache stores metadata about already scanned files within the virtual environment so identical files are not scanned again, resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, so these don't have to be downloaded every time a virtual machine is reverted to default snapshot.
Host-Based Intrusion Prevention System (HIPS)	Enables you to define rules for system registry, processes, applications and files. Provides anti-tamper protection and detects threats based on system behavior.
Exploit Blocker	Strengthens security of applications such as web browsers, PDF readers, email clients or MS office components, which are commonly exploited. Monitors process behaviors and looks for suspicious activities typical of exploits. Strengthens protection against targeted attacks and previously unknown exploits, i.e. zero-day attacks.
Advanced Memory Scanner	Monitors the behavior of malicious processes and scans them once they decloak in the memory. This allows for effective infection prevention, even from heavily obfuscated malware.
Client Antispam	Effectively filters out spam and scans all incoming emails for malware. Native support for Microsoft Outlook (POP3, IMAP, MAPI).
Web Control	Limits website access by category, e.g. gaming, social networking, shopping and others. Enables you to create rules for user groups to comply with your company policies. Soft blocking – notifies the end user that the website is blocked giving him an option to access the website, with activity logged.
Anti-Phishing	Protects end users from attempts by fake websites to acquire sensitive information such as usernames, passwords or banking and credit card details.
Two-Way Firewall	Prevents unauthorized access to your company network. Provides anti-hacker protection and data exposure prevention. Lets you define trusted networks, making all other connections, such as to public Wi-Fi, in 'strict' mode by default. Troubleshooting wizard guides you through a set of questions, identifying problematic rules, or allowing you to create new ones.
Botnet Protection	Protects against infiltration by botnet malware – preventing spam and network attacks launched from the endpoint.
Device Control	Blocks unauthorized devices (CDs/DVDs and USBs) from your system. Enables you to create rules for user groups to comply with your company policies. Soft blocking – notifies the end user that his device is blocked and gives him the option to access the device, with activity logged.