ESET Converts Gloucester Rugby to Faster Anti-malware

ESET Endpoint Security resolves sluggish server response times and slow loading applications, while saving the club money.

GLOUCESTER RUGBY

CUSTOMER

Based at Kingsholm Stadium, Gloucester Rugby competes in the English Premiership, the Anglo-Welsh and the European Rugby Cup. With over 130 years of history, the West Country Rugby Union club has a strong and loyal following and a long list of notable players over the years.

Selling up to 16,100 tickets for each home game, Gloucester's thirteen ticket machines work extremely hard over short periods of time. Both the front office ticket desks and the back office administration computers are protected against malware threats, but when the antivirus software started to impact on performance Gloucester Rugby's IT Manager, Gareth Balmer, consulted Converge for a better solution.

CHALLENGE

"Server response time, particularly for the ticket machines, is extremely important as delays frustrate fans and potentially costs the club money," explains Gareth. "In addition, our own users had begun complaining about the time it took for applications to load and it was clear to us that we needed an alternative to our current antivirus provider."

Converge has been providing third line support to Gloucester Rugby since 2007. It recommended the switch to ESET Endpoint Security as it has a much smaller footprint and requires considerably less system resources to operate effectively. The move to ESET also meant a considerable cost saving, allowing the club to reuse the available budget elsewhere.

SOLUTION

ESET Endpoint Security integrates antivirus, antispyware and antispam with a bi-directional firewall to stop hacker attacks. Converge and ESET helped with the initial installation of ESET Remote Administrator that then allowed for all machines to be installed with the new software remotely. On a day to day basis Gloucester Rugby manage ESET Endpoint Security, though by their own admission there is very little involvement required.

"As soon as ESET was installed there was instantly a noticeable difference in the speed of response from the servers and we've stopped getting complaints from users," confirms Gareth. "In addition, ESET is fully customisable, making it much easier to operate at a user level."

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.

ENJOY SAFER TECHNOLOGY™