

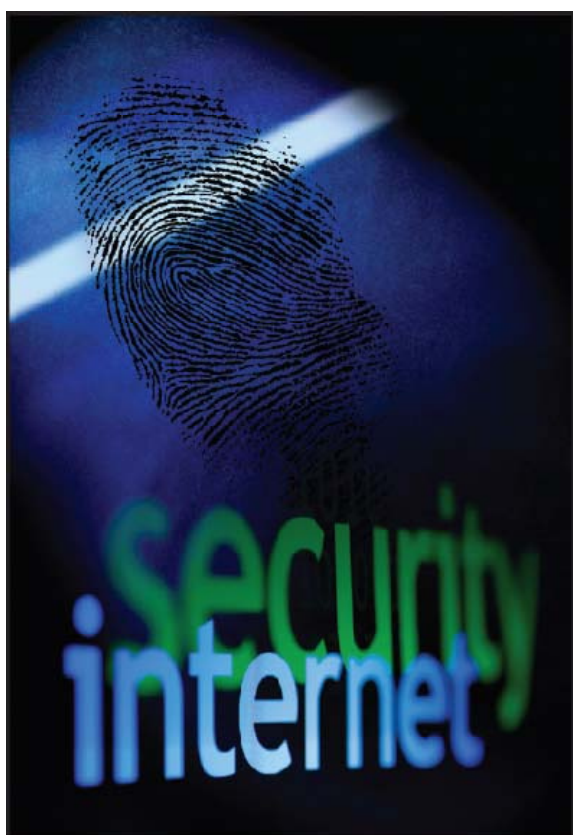
Dorset Police Hi-Tech Crime Unit Relies on ESET NOD32

The Dorset Police Hi-Tech Crime Unit is instrumental in the investigation of computer related crime in the area and is responsible for gathering evidence for prosecution by examining and analysing data from machines connected to criminal activities. Back in 2005, the unit was looking for an anti-virus product to protect its own network, but had a slightly different set of requirements to most organisations, as DC Tristan Oliver explains.

“The trouble is when you’re working in hi-tech crime you have two opposing sets of needs. On one hand you require that your machines do not become infected, either from ‘normal’ sources or from something that may be lurking in the data of the machine being investigated. At the same time, if you’re studying data from a suspect’s computer and there is a virus, you may actually want to run it just to prove its exact intentions. Our forensic work can make it very challenging circumstances for anti-virus products.”

The Hi-Tech Crime Unit required an anti-virus product that was low on system resources, operated in the background without being intrusive and yet would provide the flexibility to allow settings to be easily altered as required. In addition, the Hi-Tech Crime Unit required that its secure network, which was not connected to the internet, could easily be updated with the latest virus signatures and engine updates.

“We looked at several different products, but chose ESET NOD32 as it met all of our requirements and had an enviable reputation as the vendor with the most VB100 awards,” continues Tristan Oliver. “Other products we looked at had nowhere near the same small footprint as NOD32 and frequently tied up resources that we would prefer to be available for other processes. In addition,



Case Study: Public Services

Product



Overview

Company

- Dorset Police Hi-Tech Crime Unit

Pains

- Required flexibility in actions to be taken when malware is detected
- Needed to be able to easily update offline computers
- Run many forensic processes, so a small footprint was essential

Solution

- ESET NOD32 Antivirus

Results

- Comprehensive protection in an untrustworthy environment
- Can choose to run malicious software if required
- Ability to update offline computer from a central management console, enabling machines to remain up to date with minimal administrative overhead

Quick Facts

- Industry: Police
- Customer Profile: Responsible for gathering evidence for prosecution by examining and analysing data from machines connected to criminal activities



updating NOD32 on our offline secure network is very easy, allowing us to keep these machines up-to-date with a minimal administrative overhead.”

ESET NOD32 is a single, highly optimised engine that works as a unified anti-threat system to protect against a broad spectrum of malware including viruses, worms, spyware and other malicious attacks. NOD32 continually wins awards for the fastest performance of any antivirus application, on average 2 to 5 times faster than the competition (source: Virus Bulletin). Virus Bulletin introduced its first VB100 award in 1998. In order to display the VB100 logo, an antivirus product must meet two criteria. (1) Demonstrate it detects all “In-the-Wild” viruses during both on-demand and on-access scanning. (2) Generate no false positives when scanning a set of clean files. “

Analysing copies of other people’s data poses a high risk to the machines used in our forensic analysis,” says Tristan Oliver. “But ESET helps us to mitigate that risk and stop accidental infections, whilst providing the flexibility to deliberately compromise machines when required. With NOD32 we have the option to do nothing at all when it discovers a virus and that is very helpful in our investigation procedures. We also like the fact that you can easily look-up a virus on ESET’s website to find out further information and more about its payload.”

ESET NOD32 can be configured to suit an organisation’s individual needs. Typically, companies require minimal user intervention and NOD32 is automatically set to delete or quarantine all suspicious files, reporting incidents to the administrator through the centralised management console.

For organisations such as the Hi-Tech Crime Unit that have varying requirements, the software can be programmed to give the user full control over the action to take on individual security incidences. The centralised management console also allows the administrator to set other parameters such as scheduling updates, which, in online networks, operate in the background. In the case of the Hi-Tech Crime Unit’s secure network, updates are downloaded onto clean media such as a CD or memory stick and then copied over to the offline network to be centrally distributed.

“Most of the data we look at I would say definitely doesn’t come from a trusted source. Recreating data from a machine linked to crime would normally be asking for trouble, but we know that we can rely on ESET NOD32 to identify the threats, whilst allowing us to decide what action to take,” concludes Tristan Oliver.

“We’ve been using NOD32 since 2005 and ESET is still the vendor with the most VB100 awards and the one that has the smallest footprint, two of the key reasons we chose the product in the first place.”

QUOTE:

“Recreating data from a machine linked to crime would normally be asking for trouble, but we know that we can rely on ESET NOD32 to identify the threats, whilst allowing us to decide what action to take.”

– DC Tristan Oliver,
Dorset Police Hi-Tech Crime Unit

ESET NOD32 Antivirus
ESET NOD32 Antivirus Business Edition
ESET Smart Security
ESET Smart Security Business Edition

Detection of viruses, worms, trojans, rootkits, etc.	✓	✓	✓	✓
Detection of spyware, adware, riskware, dialers, etc.	✓	✓	✓	✓
Residential protection web and mail content filtering	✓	✓	✓	✓
Antispam unwanted mail filtering			✓	✓
Personal firewall network communication filtering			✓	✓
ESET Remote Administrator remote and central administration		✓		✓
Mirror enables updates from local servers		✓		✓

IT Doctor

Tel: 01706 838276

Web: www.itdoctor.co.uk

Email: info@itdoctor.co.uk

Fax: 0870 4321 155

