

ESET displaces more competition

“Empirically speaking, ESET’s detection methodology is superior to the competition.”

— Eldon Sprickerhoff, co-founder, eSentire



Mark Van Der Sande is the Manager of Infrastructure at GoldenTree Asset Management (GTAM), an investment firm based in New York with offices in Brazil and London. He oversees hundreds of workstations and servers around the globe. From the time he arrived seven years ago, GTAM has used Symantec for its workstation antivirus needs.

Then something changed. “We started seeing a lot more ‘drive-by’ malware incidents reported by our Managed Security Services Provider (MSSP),” said Van Der Sande.

Typically, after receiving an alert from the MSSP that a workstation had connected to a site that contained

potentially malicious code, Van Der Sande’s team would then run a full scan on the machine in question.

The full scan, using Symantec Endpoint Protection, would find “absolutely nothing.”

“We called up our MSSP to confirm the traffic pattern, and they were pretty confident that something had bypassed our defenses.” Mark then decided to run a scan by using Malwarebytes. Sure enough, the offending software was soon located. Curiously, every time Malwarebytes was run and detected something, at that same moment, Symantec would also report finding it.

“We had spent money on licensing, time on creating good configs and a good deal of effort working with Symantec support to make sure we had dotted the i’s and crossed the t’s. We also created an automatic reporting system to give us real-time updates regarding the status of the antivirus environment, as we take virus and malware threats very seriously. Too many people have been burned by setting and forgetting their AV products,” said Van Der Sande.

Frustrated, Van Der Sande turned to one of the co-founders of eSentire, Eldon Sprickerhoff, for an antivirus recommendation. Basing his opinion of how well a variety of antivirus vendors detected new malware, Sprickerhoff recommended ESET.

Case Study: GoldenTree Asset Management



"We deal with a wide variety of malware every day and monitor how well the AV vendors react to new threats. It was my opinion that empirically speaking, ESET's detection methodology is superior to the competition," stated Sprickerhoff.

That recommendation led to an evaluation by Van Der Sande, who assessed McAfee, Symantec, Trend Micro, Kaspersky and ESET. His team installed the base version of each, with all available updates, on separate laptops, and visited some websites he was assured had known harmful code that has been available on the Internet for at least 36 hours. "Thirty-six hours should be more than enough time for an AV vendor to integrate appropriate protections within their updates," said Van Der Sande.

"We visited three known bad sites. The machines running McAfee, Trend and Symantec were compromised within 30 seconds. Kaspersky fared somewhat better, but still gave us the opportunity to become infected. ESET instantly dropped each before we even had a chance to get connected. I was amazed. Of course, there are steps you can take to minimize that risk, but your virus scan should be able to do what it is advertised to do."

Van Der Sande sent these results along with his finding, and began the ESET installation, starting with 250 workstations, 100 servers and 25 loaners.

Why GoldenTree switched to ESET – the business case

Goals

Mark had three goals in mind when making the switch to ESET.

1. Find malware other AV products weren't finding.
2. Secure the environment.
3. Witness virus protection doing what it is designed to do.

Implementation

"Implementation was great," he continued. "We used Rip and Replace (ESET's customized solution), because it's almost impossible to completely remove Symantec from a machine manually. ESET installed quickly and easily, and did not require us to reboot our servers."

Improvements

Since installing ESET, Mark and his team have experienced zero drive-by downloads and improved ROI in the form of fewer man-hours. He adds that the management console is a lot more intuitive, and support much more responsive.

What would you tell an IT Admin considering ESET?

"If you want to minimize your headaches, make the change."



Quick Facts

Company name:	Golden Tree Asset Management
Website:	www.goldentree.com
Location:	New York, NY
Industry:	Finance



ESET NOD32 Antivirus — Business Edition



The ultimate solution for your computer security

Comprehensive, proactive protection is crucial in a business environment. ESET NOD32 Antivirus helps business protect its most valuable data from malware and hacker attacks.

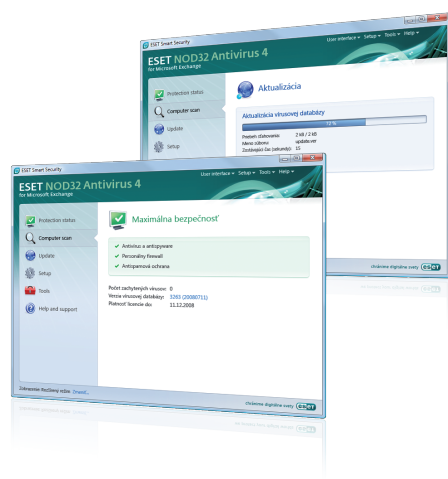
When it comes to complex network security implementations at universities, hospitals and businesses, ESET NOD32 Antivirus, coupled with ESET Remote Administrator, gives your IT staff back its valuable time. Long after-hours battles with installation, permissions and compliance reports disappear. NOD32 + Remote Administrator is easy to install, easy to manage and can protect mixed networks composed of PCs, servers, mail servers, Linux boxes and Macs.

With more than 100 million users trusting ESET worldwide, you know you're in good hands. And, because each of those protected PCs regularly checks in to ESET's ThreatSense® database, you can also rest easy that your protection is staying strong 24/7.

Unlike conventional AV that depends on signature updates alone to stay safe, ESET uses both ThreatSense signatures and our secret weapon — advanced heuristic scanning. This is where NOD32 really shines — because our scanning core has been “learning” about new threats for more than a decade, our proactive protection can identify a novel malware threat before competitors' patches and signatures go out. That's why ESET has never missed an “In-the-Wild” infection.

And on the user end, ESET NOD32 boasts fewer interruptions and less slowdown during startup and file scans. ESET has lower system impact because it runs lightly in the background. Chances are, your end users won't even know it's there. But they'll be free of viruses, trojans, worms and spyware.

Why switch? Simple installation. Powerful, intuitive management. ThreatSense protection and advanced heuristic scanning. And faster performance with fewer interruptions.



ESET NOD32 Antivirus + Remote Administrator

Proactive protection

Two layers of protection — powerful ThreatSense signatures generated by 100 million ESET PCs, plus advanced heuristics that can identify and “sandbox” new threats — mean that you'll be protected on Zero Day of an outbreak, not hours or days later.

Lightweight design

ESET NOD32 requires less memory and CPU power and performs faster in competitive benchmark testing. It's easier on your end users and easier on IT staff.

Simple management

Generate installation packages and push them out to your clients — whether your network has 10, 1,000 or 10,000 PCs. And with Active Directory management, keeping track of them dynamically is a breeze. You can even configure a mirror server so your clients can download signature updates locally, rather than connecting one-by-one.



© 2010 ESET, LLC. All rights reserved. ESET, the ESET Logo, ESET SMART SECURITY, ESET.COM, ESET.EU, NOD32, VIRUS RADAR, THREATSENSE, SYSINSPECTOR, THREAT RADAR, THREATSENSE, NET and CYBERSECURITY are trademarks, service marks and/or registered trademarks of ESET, LLC and/or ESET, spol. s.r.o. in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.



ESET, LLC

610 West Ash Street, Suite 1900
San Diego, CA 92101 U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 876-5845