

vigilancepro

International broker selects VigilancePro® to manage and audit USB device use and comply with FSA

BACKGROUND

RP Martin Holdings (<http://www.martin-brokers.com>) is a wholesale broking firm with 300 employees worldwide. The company is headquartered in the UK, with offices in the US, Europe and Asia.

To support the sale of bonds and financial derivatives in international capital markets, the company operates a large communications network, consisting of local area network (LAN) switching and wide area network (WAN) links to RP Martin's remote offices. In addition, connections to Bloomberg, Reuters and other third party providers are delivered to the trading floor, where brokers use desktops with up to four screens.

To maximise processing speeds and business continuity, RP Martin Holdings operates a virtual server infrastructure, with a disaster recovery site in Amsterdam and key servers replicated between the London and Amsterdam offices.

THE CHALLENGE

Scott Martin, IT Manager at RP Martin Holdings, heads up a team consisting of four IT support employees and a dedicated communications engineer. Martin cites the issue of ensuring zero downtime on the network as one of the key challenges for his team. As a result, IT applications at RP Martin Holdings are restricted to those that are required by the brokers and back office staff to enable them to do their jobs. However, while this

helps to secure files, documents and applications, Martin also wanted to combat the risk posed by the use of personal USB devices.

As well as the obvious risk of company data being downloaded to a personal device, that could subsequently be lost or stolen, USB devices have been known to infect corporate networks with viruses and worms, such as Conficker.

In 2006, this risk was prioritised when the Financial Services Authority (FSA) demanded that financial services firms restrict and audit the use of removable storage devices.

"We really needed to get a clear picture of all the devices that were being plugged in. We wanted to be able to control the use of devices that were capable of storing large amounts of data, such as USB sticks. We also wanted to prevent consumer devices, such as MP3 players, iPhones, microphones and digital cameras, from being connected to RP Martin's network without our knowledge," says Martin

In response to the FSA directives, Martin had implemented a leading endpoint security solution that could identify when users were attempting to connect USB devices to the network and block and audit these attempts.

However, over time, the IT team found that while they were able to block the unauthorised use of USB sticks and other removable storage devices, they were not able to gain the required visibility of USB device use on the network. "Lots of low

level detail was included, making it difficult to decipher the reports," explains Martin.

THE SOLUTION

In 2010, Scott Martin was introduced to user activity management software, Overtis VigilancePro. When installed on desktops, laptops and servers, VigilancePro is able to manage and monitor every USB device connection, keystroke and input/output executed on that machine.

After an initial pilot, RP Martin Holdings migrated to the VigilancePro 5.0 software to protect 230 workstations. "The flexibility of the rule sets and the ability to monitor all use of devices and any transfer of files to removable storage media were key reasons for selecting VigilancePro," reports Martin. "The fact that we were able to create a clear audit trail of all authorised USB device use and prevent any unauthorised use has helped us to immediately comply with the FSA directive on removable storage devices".



Scott Martin explains that the only authorised devices are RIM BlackBerry devices which have been issued by the company. If an employee needs to use a USB storage device for a specific task, he must contact the IT support desk to get this authorised. All device usage is logged by VigilancePro, to create a clear audit trail of devices that have been authorised, or blocked from connecting to the network.

EASE OF IMPLEMENTATION

Scott Martin reports that it took one working week to implement Overtis VigilancePro. "The installation of the software was swift. It then took a few days to configure our rule sets and test to ensure that they were correct," says Martin.

Because the software tracks every mouse movement and keystroke, it is extremely interactive and helps IT managers to adjust rules and policies in direct response to the way that employees use company devices and applications. As a result, security is maximised without interrupting legitimate workflows.

When asked about the key benefits of this new endpoint security solution, Scott Martin cites the ease of use of the VigilancePro console and the fact that the IT team are immediately sent an SMS or email message if someone tries to connect a device to RP Martin Holdings' network:

"The previous solution included too many low level details. When you looked at the report it didn't mean much and it didn't send alerts. The VigilancePro central management console is a lot easier to use and has clarified our view of what is happening on our network. VigilancePro

sends an alert to the IT management team as and when a device connects and this has greatly improved our visibility of any attempts to use unauthorised devices."

Where a member of staff has a genuine need to use a USB device other than the company BlackBerry, Scott Martin is able to allow this via the central console, while also auditing the activity to comply with the FSA directives. He explains that while much of the dialogue could have been facilitated within the software, his team prefers to have a direct conversation with colleagues who request special permission to use devices: "We have a pop-up screen on the workstations informing staff that if they need to connect a device they can contact our service desk for help. We could have used the on screen dialogue boxes within VigilancePro to capture individual requests for device authorisation. However, because of the nature of our business, many brokers prefer to speak to us on the phone, so we wanted to facilitate that. It's part of our company culture".

THE BENEFITS

Martin reports that the key benefits of installing VigilancePro include gaining clear visibility of all devices that are attempting to connect to the network and control over all devices that are permitted to connect, as well as the proactive alerts that are sent to the IT team whenever an employee attempts to connect a device.

He adds that this allows his IT team to control the data that is coming into and out of the RP Martin Holdings network, reassuring them that they are compliant with financial industry regulations governing information security:

"The cost of managing removable devices is next to nothing. The main benefit of

installing VigilancePro is that I have peace of mind that I've secured data from being downloaded to devices without our knowledge.

We've also mitigated the risk of viruses getting onto our network through an infected device and protected against surreptitious surveillance devices being used within our premises. When we have our annual audit, I've got clear data to prove that we're managing and monitoring all USB device use. Where exceptions to the rule have been requested, I've got an audit trail showing where I signed off any changes."

"We are now looking at how we can roll out the other features of VigilancePro to help us add a second layer of security that manages and audits the printing of documents," concludes Martin.

"The cost of managing removable devices is next to nothing. The main benefit of installing VigilancePro is that I have peace of mind that I've secured data from being downloaded to devices without our knowledge."
Scott Martin
RP Martin Holdings