



Case Study Stonesoft

A construction company specialising in civil engineering, Careys' construction project portfolio covers everything from highway construction to building power stations. The company delivers around 35 construction and 15 demolition project sites at any one time. There are around 500 employees on the books, with 150 people at head office, plus numerous sub-contractors at its sites across the UK.

Stonesoft Helps Careys' to Manage Nationwide Construction Portfolio



A construction company specialising in civil engineering, Careys' construction project portfolio covers everything from highway construction to building power stations. The company delivers around 35 construction and 15 demolition project sites at any one time. There are around 500 employees on the books, with 150 people at head office, plus numerous sub-contractors at its sites across the UK.

All of which provides constant network security challenges. Eoin McMenamin, network technical manager at Careys, explains: "We have to have secure, reliable communications in place at all sites from day one. The primary challenge facing IT communications at any construction company is that the critical data that those on site rely on appears in the first few weeks and months of a job not at the end. That is when the initial plans and the requirements are transmitted to a site."

"If we have the correct information on site in good time then construction errors are minimised – in other words you do not pour 50 tons of concrete in the wrong place because you have not got the latest revision." To complicate matters there's also the need to factor in the lead time that Openreach need to get your connection. "So the challenge was really summed up in the phrase zero-day connectivity," said McMenamin.

This challenge led Careys' to talk to Stonesoft as a supplement to the Watchguard firewalls they were already using.

The relationship between Careys' and Stonesoft began in April 2010 with the implementation of Stonegate Advanced Firewall and Intrusion Protection System (IPS) devices at headquarters. "With existing security infrastructure in place, we didn't need to forklift out our core and our perimeter at the same time. We thought that was too risky and still believe that is the case, so the way we decided to implement was to upgrade the core and then phase Stonesoft into the perimeter from the inside out," explains McMenamin.

“The interface on the Stonegate Management Centre is drag and drop, object orientated and basically light years ahead of the competition, and we have seen a few over the years! ”

Eoin McMenamin
Network Technical Manager at Careys

Working with wide area network specialist CI-Net, Carey’s adopted a co-vendor approach to securing communications because of the criticality of its network services which it could not leave to chance. “We cannot sign, seal, fire and forget – they worked with us in a co-operative sense in that we retained technical talent here and saw CI-Net as a team extension. It was co-sourced, because we had mixed experiences with other service providers – some good, some dismally bad - so what we weren’t prepared to do was just give the crown jewels away in one go,” said McMenamin.

With CI-Net’s help, Carey’s used Stonesoft’s StoneGate multi-link technology to create a highly-resilient VPN mesh which, along with the Stonegate firewalls, is centrally managed using the Stonegate Management Centre.

“Working with CI-Net and Stonesoft, we quickly arrived at a robust, efficient process for gearing up new sites,” continued McMenamin. “We have standard site packages for standard site set-ups, it literally is a ‘site-in-a-box’. That was the end game we were aiming for and that is now how we present our role to the business. The business now has its expectations set and it has worked quite well for all involved.”

So what has the implementation enabled? “We have been able to multi-link our virtual private networks more effectively than with any other vendor we assessed – the firmware is rock solid and as far as we can see they have got build control and when we did find any issues with firmware they were very quick to respond, either with a workaround or an update package,” said McMenamin.

In terms of overall benefits, Carey’s is now able to deploy multi-linked firewalls very quickly, while day-to-day management has been greatly simplified by the Stonegate Management centre, with McMenamin describing the log server and the logging system as ‘gorgeous!’

McMenamin explains: “The interface on the Stonegate Management Centre is drag and drop, object orientated and basically light years ahead of the competition, and we have seen a few over the years! The user interface is what sold us on Stonesoft more than anything else. There is quite a steep learning curve, but it’s easy to get your head around and once you reach the plateau you realise just how functional it is. There are many ways of doing the same process which allows the firewall administrator to do things the way that suits them, it even allows us to monitor our Watchguard firewalls from the same, single interface.”

In fact, the multi-vendor management capabilities baked into the Stonegate Management Centre has become one of the stand out benefits of the move to Stonesoft. Furthermore, monitoring and reacting to suspicious activity has become much more straight-forward with Stonegate IPS.

“The logging of potential security breaches is a lot clearer and a lot more concise. I can click on a potential log entry of a particular security breach and go to Google Maps and see exactly where it came from. Now we do the majority of our business in the British Isles, so if I can see suspicious activity coming from Alberta I know that there is something wrong and I can block that particular traffic,” explains McMenamin.

Carey’s is also using the Stonegate IPS to monitor internal traffic and the device has not only identified a small number of zombie PCs but also enabled McMenamin’s team to quickly pinpoint internal security breaches. From a security point of view, this value became quickly evident when Carey’s upgraded its web filters and it could see how much HTTP and web-borne traffic was being filtered out. As McMenamin concludes, “it showed us just how much of a difference the Stonegate devices were making so we could position the move not just as a cost-saving to the business but in terms of the value it was delivering by preventing threats to business continuity.”

About Stonesoft

Stonesoft Corporation (NASDAQ OMX: SFT1V) is an innovative provider of integrated network security solutions to secure the information flow of distributed organizations. Stonesoft customers include enterprises with growing business needs requiring advanced network security and always-on business connectivity.

The StoneGate™ secure connectivity solution unifies firewall, VPN, IPS and SSL VPN blending network security, end-to-end availability and award-winning load balancing into a unified and centrally managed system. The key benefits of StoneGate secure connectivity solution include low TCO, excellent price-performance ratio and high ROI. The virtual StoneGate solution protects the network and ensures business continuity in both virtual and physical network environments.

StoneGate Management Center provides unified management for StoneGate Firewall with VPN, IPS and SSL VPN. StoneGate Firewall and IPS work together to provide intelligent defense throughout the enterprise network while StoneGate SSL VPN provides enhanced security for mobile and remote use.

Founded in 1990, Stonesoft Corporation is a global company with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit www.stonesoft.com



Stonesoft Corporation International Headquarters
Itälahdenkatu 22 A FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1349
www.stonesoft.com

STONESOFT
Network Security

Stonesoft Inc. Americas Headquarters
1050 Crown Pointe Parkway, Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075 | fax. +1 770 668 1131