[Case Study]

Company: Censornet working with IBM Softlayer

Censornet is successfully offering web security services to both enterprise and MSP customers using IBM SoftLayer's global back- end services exclusively.

Censornet's web security services help organisations step up to the challenge of managing an increasingly mobile work environment. Its cloud- based Unified Security Service platform gives greater visibility to senior management, and much better control to the IT department when supervising company-wide internet access and the use of cloud applications across all devices, regardless of a user's location.

Censornet gives organisations the power to address the productivity, security and audit issues associated with the rise in use of cloud apps and mobile devices and helps them safely implement BYOD initiatives.

Benefits for MSPs

The growth in cloud-based services has established the perfect marketplace for MSPs to thrive. But while email as-a-service is now commonplace in an MSP's product portfolio, web security as-a-service offered by MSPs is virtually unheard of. The reason is simple: most vendors in this space are not keen to let their solutions be white-labelled or hosted by an MSP.

As the only vendor to allow MSPs to white-label its web security platform, Censornet provides MSPs with a springboard to deliver their own custom-branded web security services to customers and resellers alike.

So what differentiates Censornet from other web security developed for MSPs. With the rise of cloud apps and the need for greater visibility and analysis current web security vendors do not currently bridge the gap between traditional web security and cloud application control, which is critical in today's application-driven environment, while Censornet does.

According to Chairman and CEO, Ed Macnair, Censornet is in the right place at the right time to meet market needs, in particular, the growth in enterprise reliance on cloud. As applications have moved into the cloud from on- premise infrastructure, so the monitoring, reporting and management point needs to move from traditional measures, such as a firewall, into a cloud- based architecture, where protection is closer to the data.

> "Censornet's cloud-based Unified Security Service platform gives greater visibility to senior management, and much better control to the IT department."
>
> Ed Macnair,
> CEO Censornet

The IBM SoftLayer connection

IBM SoftLayer's role in underpinning the reliability and performance of the services is business critical. Censornet's web security service is fully hosted on SoftLayer which processes, sets up web traffic reporting and deploys its big data analytics engine.

"We run everything on SoftLayer," says Macnair. "So it's crucial that it's scalable and resilient – which it is. Its resilient worldwide network was one of the company's most attractive features, with a set of geographic locations much broader than those of other service providers. We will be able to switch on datacentre hubs in geographies based on market demand which is essential to support our aggressive growth strategy."

Macnair has nothing but praise for the relationship with SoftLayer and the service it provides. From the customer's point of view, it is seamless, always on, and application and web traffic experience low latency as a result of SoftLayer's global reach and high bandwidth links.

The Unified Security Service has been developed with speed and scalability in mind. Unlike other web security and content filtering providers, a key principle in the platform's design is that web requests do not have to pass through one or more proxies at the service provider. Proxying data has a large bandwidth overhead and as a result requires excessive hardware and bandwidth to avoid adding latency to the customer's browsing experience. It makes it harder to scale up for really large numbers of subscribers and often requires equipment to be co-located near to the target market, dramatically increasing the total cost of ownership.

"So from our point of view, using SoftLayer as the global hosting infrastructure for our Web Security platform is a worry-free environment," says Macnair. "We don't have to keep the lights on, there's no hardware to manage, and it's a high resilience environment – everything is taken care of. We suffered outages with previous hosting providers and I am confident that this won't be the case with SoftLayer."

Macnair says that Censornet does not even have to create SLAs, as customers are happy with SoftLayer's SLAs, and the relationship has also helped the company win new business.

"I have a lot of confidence in IBM," he says. "I've worked with IBM in the past and it provides a huge comfort factor. IBM also gives us a level of credibility with prospective customers. They may not know or have heard of us but going via IBM and SoftLayer adds a big a tick in the box."

Macnair said that, after initial contact was made, what impressed him was the speed of deployment. Censornet moved its service infrastructure from an independent datacentre to IBM SoftLayer over the course of a weekend.

"It was completely transparent: customers didn't even blink," he says.

"It was completely transparent: Customers didn't even blink."

How it works

Censornet's software resides between the user and the edge of the network, capturing all web requests and forwarding key meta data to the cloud for inspection and analysis. Once the web request has been approved, the user continues to access the web resource directly, removing any bottleneck or masking that traditional proxies can create. Of course, there are places where proxying makes sense, for example to detect malware, and that is why Censornet offers an on-premise component as part of the Unified Security Service platform in the shape of a thin virtual machine. Customers get the best of both worlds.

"We are not denying connections but acting as a filter," Macnair says. "As we are situated between the user and the application or website, we see all requests, and the request is really the interesting aspect as, in the context of a cloud application, that shows the user's intent, such as a file upload or content creation. Seeing what comes back from the application or website – so we can stop bad things happening, making sure that malware is stopped."

How we got here

Macnair is proud of the company's 10-year heritage and has seen much change in that time. "Ten years ago, web security meant stopping people going to the wrong website. Today, especially over the last couple of years, it has become increasingly about visibility and analysis of activity within cloud applications that employees are accessing regardless of which devices used," he says.

"As a security manager, you need to know what sites and applications your employees are accessing. You don't always know what users are doing with those applications, including enterprise applications, so we give total visibility into employee web traffic. This includes HTTP/S protocols, cloud applications, social media such as Facebook and so on."

So for MSPs, working with Censornet has many benefits. In particular, customers and resellers get Censornet's highly robust web security services and the MSP gets sales and marketing support to boost services revenues. Censornet's white-label model is a fast, reliable and profitable way for MSPs to expand their services portfolio with Web Security-as-a-Service.

CENSORNET LTD
MatrixHouse, Basing View,
Basingstoke, RG21 4DZ, UK

Phone: +44 (0) 845 230 9590

CENSORNET A/S
Park Allé 350D, 2605 Brondby,
Denmark

Phone: +45 70 22 55 33

CENSORNET INC
11801 Domain Blvd, Austin TX
78758, USA

Phone: +1 888 440 8456