Cellcom Israel Ltd.

סלקום

INDUSTRY
Cellular Communication

COUNTRY
Israel

PRODUCT TYPE
Forcepoint Web Security & DLP

SIZE
8,150 Users

SECURITY ISSUE
Data Leakage

> "The money we invested in Forcepoint has already been proven — we feel we have certainly achieved a return on investment."

— Amir Shahar, Information Security Manager, Cellcom Israel Ltd.

OVERVIEW

Cellcom Israel Ltd. was established in 1994 and is now the leading cellular provider in Israel. Cellcom provides its 3 million subscribers with a range of value-added services including cellular and landline telephones, roaming services for tourists in Israel as well as additional services including music, video, and mobile office technology. It has 6,000 employees and operates 360 retail outlets and 30 customer service centers across Israel. Cellcom is a public company and its shares are traded both on the New York Stock Exchange and the Tel Aviv Stock Exchange.

CHALLENGE

As with all organizations, Cellcom has large amounts of sensitive and company proprietary information held on their corporate network. However, it was not until a serious data leak occurred that Cellcom realized that their sensitive data needed to be better identified, monitored, and protected from potential misuse.

> "We had a serious incident a couple of years ago when very important company documents were leaked to the press. Although we were not hurt financially — at least not directly — the documents were published and our reputation was certainly damaged. Not only was this embarrassing to the company, but if this kind of event were to happen again, potential losses could be significant."
>
> — Amir Shahar, Information Security Manager, Cellcom Israel Ltd.

As a result of this high-profile security breach, Cellcom assessed its data security situation and decided to look for a data loss prevention solution that would ensure valuable company data was identified and kept inside the organization.

SOLUTION

Cellcom had already been using Forcepoint Web Security for a number of years to protect its network from Web threats and to monitor Web usage so it was familiar with the comprehensive protection of the Forcepoint security portfolio. After looking at a number of solutions on the market, Cellcom selected Forcepoint DLP to detect and prevent unauthorized use of confidential company information.

> "Forcepoint DLP was the strongest solution we found to protect and prevent against data leakage. We looked at Microsoft Rights Management Services (RMS) but this solution only went so far as allowing the owner of a document to select documents to be protected; it did not actually identify and automatically apply policies to protect confidential information as TRITON architecture does. The most powerful feature of TRITON architecture is that it monitors the information that you hold within the organization and identifies which information is confidential and potentially at risk. At that point, policies can be automatically put in place to determine who has access to this data and what they can do with it."
>
> — Shahar

Forcepoint offers leading data loss prevention (DLP) technology to identify, monitor, and protect confidential data. Leveraging the combined content inspection techniques of TRITON architecture and DLP technologies, the solution accurately prevents data loss, secures business processes, and manages compliance and risk. Providing a modular approach to solving the problem of data loss, TRITON architecture includes powerful monitoring capabilities that provide visibility into who is sending what data and where they are sending it.

Forcepoint DLP enabled Cellcom to understand their position in terms of data security risk and then define a remediation strategy.

> "The first stage of implementation was to identify all of the files on the network that contained sensitive information. We first monitored the network without employees knowing that the network was being monitored. This was necessary to understand how much sensitive information we had, where it was located, and how it was being used. This monitoring phase was extremely effective and informative. TRITON architecture helped us identify 200 gigs of data on the network that we had not realized was sensitive. In fact, we did not even know that these documents existed. Alerts also told us when sensitive data was moved or sent out of the organization."
>
> — Shahar

Using this intelligence, Cellcom put together a set of policy-based controls, which was then published to employees and enforced by Forcepoint DLP.

> "Once we had a good understanding of where the sensitive data was on the network, we could decide who would be able to access this data and what they could do with it. This way we can prevent employees either by accident or intent, from sending company sensitive information outside the network. Forcepoint enables us to better identify and control our confidential data — and puts us in a very strong position in terms of our overall data security.
>
> People generally do not breach security on purpose. In fact, they often do not understand the risks and consequences if important information leaves the company network, whether it is sensitive commercial, customer, or regulatory information. Once we published and implemented our data security policies through TRITON architecture, and everyone had a good understanding of what we were trying to achieve and why, security breach alerts dropped from 100 a day to maybe 10 a day."
>
> — Shahar

Because the original security breach was high profile, Shahar and his team had the immediate backing of senior management to implement a comprehensive data security solution, which Shahar says is particularly important in company-wide acceptance of data security policy:

> "As you would expect, implementing a comprehensive data security solution like TRITON architecture does take some effort. In total, implementation took a couple of months but what we got out of it was a complete data security solution that provides us with the confidence that we know what sensitive data we have, where it is stored, and can control who has access to this data and what they can do with it. For a high-performance company like Cellcom, this is important to our ongoing competitiveness."
>
> — Shahar

RESULTS

Forcepoint Web Security & DLP provide Cellcom with a comprehensive security solution which comprehensively identified sensitive data:

> "Forcepoint DLP has enabled us to set policy on information rather than just on specific documents. Even if I do not know where sensitive information is held, the system will automatically identify this and monitor how that information is being used — whether it be Microsoft Word, Excel, or email. TRITON architecture is a very powerful tool that has transformed how we identify, manage, and protect our important company data."
>
> — Shahar

It also secures sensitive data and business processes:

> "Forcepoint DLP allows us to set policies to manage which employees can access sensitive data and what they can do with it. The solution enables us to block critical information from leaving the organization, which is what caused the security breach in the first place."
>
> — Shahar

Finally, it is a complete solution from a trusted vendor and we have achieved a significant return on investment for the company:

> "We have been using Forcepoint DLP for three years now and have been very pleased with the results. The local Forcepoint employees in Israel are experts in their field and have been very professional in helping us to implement our data security solution. The money we invested in Forcepoint has already been proven — we feel we have certainly achieved a return on investment and our senior management now has the confidence that we are doing everything we can to keep our data safe."
>
> — Shahar

Cellcom Israel Ltd. has relied on Forcepoint security solutions since 2004.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[CASESTUDY_CELLCOM_EN] 300009.021317