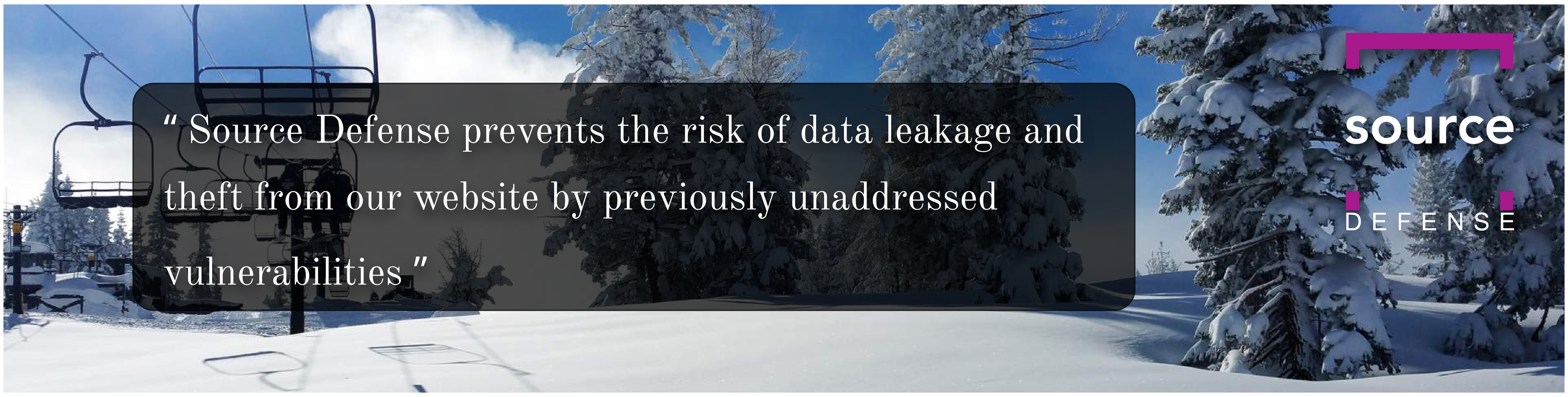

“ Source Defense prevents the risk of data leakage and theft from our website by previously unaddressed vulnerabilities ”

source DEFENSE

COMPLIANCE AND CUSTOMER DATA PRIVACY: WHEN THE VULNERABILITY IS OUTSIDE OF YOUR SECURITY PERIMETER

Bear Valley Resort ("Bear Valley") is one of California's exclusive ski resorts and destinations. Offering skiing, lodging, dining, events, entertainment, and more, Bear Valley caters to a discerning guest who desires the most of their getaway whether it be a wedding, a vacation, weekend, or simply a day of fun.

Bear Valley allows its guests to book mountain passes, lodging, dining, and entertainment packages online. As such, they are vigilant about maintaining customer data privacy and compliance. Bear Valley chose to deploy the Source Defense V.I.C.E. Service on their corporate website as a preventative measure designed to eliminate the threat of customer and payment data theft through 3rd party website partners or the hackers that might exploit them. A Bear Valley executive commented, "Our business is built to serve our guests in all ways possible. As such, we work hard every day to offer our guests experiences and options that create a complete resort vacation. Alongside that goal is our mission to honor our guests by taking seriously the protection of their privacy - even online. We chose to work with Source Defense because their service prevents the risk of data leakage and theft from our website by previously unaddressed vulnerabilities presented by external 3rd parties".

Nearly every corporate website endeavors to provide the most engaging customer experience. To this goal, they rely on external 3rd parties to deliver critical website content, components, and capabilities that could otherwise not be developed internally. However, along with the benefits these 3rd parties deliver, they introduce serious security and privacy risks. In fact, once these 3rd parties are included on a corporate website they immediately have nearly unlimited access to the entire webpage. Such access introduces vulnerabilities that gives 3rd parties (and the hackers that might exploit them) the ability to record every user keystroke, inject new form fields to harvest customer information, and redirect customers to unauthorized external websites where customer data can be phished and stolen. To make matters worse, most corporate websites rely on dozens of 3rd parties to provide a complete customer experience. Each of these third parties multiplies the extent of exposure.

Along with the serious security and customer privacy concerns of these vulnerabilities comes regulatory and compliance concerns. Whenever customer and payment data is at risk, organizations must immediately question their level of compliance with applicable standards such as GDPR, PCI, HIPAA, and more. Safeguarding this information is critical. However, it becomes difficult to impossible to do so when the vector of compromise is outside of your corporate security perimeter. Source Defense's CEO observes, "The 3rd parties corporate websites rely on are stored on remote servers that are external to your corporate environment. This means that they load in your customers' browser outside of your corporate security perimeter and after every layer of your corporate security program has done its job. This is why organizations rely on Source Defense as a unique company offering the only solution to this previously unmanageable vulnerability. Without Source Defense, customer data is likely in jeopardy and compliance is called into question".

“ Our mission to honor our guests by taking seriously the protection of their privacy”

BEAR VALLEY

source DEFENSE

Source Defense
+972-72-255-5793
www.sourcedefense.com
77 Ha'Energia, Beer-Sheva
8470912, Israel

Goals:

- Maintain compliance related to customer and payment data
- Prevent customer and payment data theft through attack vectors that are outside of the current corporate security perimeter
- Safeguard customer privacy