# Dole Food Company

*The Dole Food Company defends its online brand and vital web applications with XyberShield, a behavior-based, Software-as-a-Service Internet security platform*

## Overview

**Challenge**
With more than 2 million web sessions per month, Dole.com is a choice target for malicious activity on the Internet. Keeping pace with rapidly-evolving attacks was a formidable challenge, and the company's multiple web applications were particularly vulnerable.

**Solution**
To protect its website, Dole uses XyberShield Enterprise Protection, which actively defends against SQL injection, HTTP response splitting, and other top attacks as defined by OWASP.

**Benefits**
System recognized and stopped every single attack. No additional burden to Dole's personnel, infrastructure, or network performance. Regular visitors enjoyed full access to site. Forensic information on all attempted attacks was gathered and analyzed.

Dole Food Company, Inc. is an U.S.-based agricultural multinational corporation headquartered in Westlake Village, California. The company is the largest producer of fruits and vegetables in the world, responsible for over 300 products in 90 countries. Its high public profile and active online presence mark the company's websites as choice targets for malicious activity on the Internet.

The company implemented XyberShield to protect its web applications and, in the process, blocked hundreds of attacks while experiencing no additional burden to its personnel, infrastructure, or network performance.

## A High Profile Target

In October of 2009 Dole became a publicly traded company on the New York Stock Exchange. In addition to being publicly listed, the company received increased media attention due to several national marketing campaigns. This increase in public awareness corresponded to a swell of hacker activity on the main corporate website, **www.dole.com**. For example, the company experienced as many as 100 attacks per day, several of which were coordinated attempts from multiple locations designed to deface the site, access and change confidential data, and discover financial information. The attempted incursions included SQL injection attacks, which are among the most potentially costly hacks. Historically, a single successful SQL injection attack can cost a company up to $6.6 million.

With more than two million visitor sessions a month, protecting the Dole corporate website was a formidable challenge. To compound the problem, most of the attacks were focused on the aspect of a website left most vulnerable by traditional network-based defenses: the company's web applications.

XYBERSHIELD©

*"Dole.com is our corporate flagship; the premier touchpoint between customers and the Dole brand.*

*"XyberShield protects our brand equity by defending our site against online threats, and as we continue to gain market awareness and build our presence online, the protection scales to match our growth. XyberShield is simply the best way to guard the distinctive Dole name online."*

— Marty Ordman, Vice President of Marketing Services for Dole Food Company, Inc.

## Web Application Defense

A web application is any type of interactive software that runs in a browser. Any action by a user on the web other than reading and basic navigation requires a web application, including online calendars, web-based email, enterprise portals, personal online profiles (LinkedIn, Facebook, eHarmony), and nearly all of the Google services.

Network firewalls protect networks and infrastructures. Web application defenses protect e-commerce, software, and the databases associated with valuable information. While network firewalls are necessary, hackers have moved beyond network-level attacks and are increasingly focused on people's personal and sensitive information.

Customers use web applications to interact with the software and information behind the network layer; such interactions require an intentional "gap" in the network's defense. These intentional openings require a specific kind of protection.

## Behavior-based, Real-time Protection

For Dole, XyberShield provides an adaptive, effective web application defense. As the number of attacks increased, XyberShield successfully detected and blocked each one, preventing all malicious activity on the website. During the entire month of October 2009, **www.dole.com** experienced no downtime and suffered no adverse consequence despite the amount of hacker activity directed at it. The site's 2 million-plus legitimate visitors enjoyed full access.

Currently, a typical month sees the Dole corporate website receiving 2,215,170 visitor sessions. During a recent timeframe, 346 high-level threats were detected and shut down by XyberShield. Cross-site scripting attacks accounted for 293 of the attempted incursions, while the other 53 attacks were of the SQL injection variety.

As attacks become more sophisticated, XyberShield learns and adapts to meet the challenge. The system collects information on each potential threat for forensic analysis, constantly informing its behavior analysis and correlation engine (BACE) to configure defenses as new forms of attacks arise. This additional experience regarding threat variants allows XyberShield to recognize and respond to the latest hacking techniques by creating alerts or stopping the active web sessions immediately, before malicious activity can affect the website in any way.

*"At Dole, we take every necessary security measure when it comes to our web applications and online data.*

*"XyberShield's cloud-based infrastructure, behavioral analysis, and correlation abilities are tremendously efficient. Since we began using XyberShield in 2009, it has protected us seamlessly. XyberShield is our number one tool for protecting our web applications."*

— Michael Contreras, Digital Marketing Manager for Dole Food Company, Inc.

## Defense via the Global Cloud

Because XyberShield is a true cloud-based service, it globally leverages the experiences of every user of the service, not just the Dole Food Company. As information about new types of malicious behavior is detected and stopped at the site of one customer, all the users of the service become protected. Without being aware of it, companies using the XyberShield service, like Dole, mutually benefit from the experiences of each other.

The security solution activates within minutes and scales dynamically to fit changing business requirements. Updates occur invisibly. A true cloud security solution, unlike an appliance, adds no additional burden to a company's personnel, infrastructure, or network performance.

One obstacle faced by many cloud-based security solutions is that they require the user to redirect all web traffic to the security provider's systems. This can result in latency issues—extra time needed to access the website. Other cloud-based services require the user to host their website and valuable data on the servers of the service provider, thus losing a measure of control over their own data and potentially violating their own security policies regarding the safeguarding of data.

Like most members of the Fortune 500, The Dole Food Company needed to maintain control over its own data and reduce latency. Dole chose XyberShield, a no-host, no-proxy solution which makes use of a single script of code known as a XyberObserver.

## The Constant Observer

Users of XyberShield install a small piece of code, known as a XyberObserver at the top level of their web server. This script is in constant communication with XyberSecure's remote global service platform, where all the heavy computational lifting is done.

This very light approach places all the work of protection squarely on the resources of XyberSecure, while allowing Dole to maintain complete control of its own data, unlike a hosted solution. No web traffic is re-routed for filtering purposes (the challenge with a proxy).

The script on Dole's server observes all actions in every single session of website use. The instant that inbound malicious activity is detected, the defensive system takes action, either warning the visitor, diverting them to another website, or blocking them outright.

## Solution Components:

- XyberShield Enterprise Service
- Active XyberFrames:

OWASP Bundle
SQL Injection
SSI Injection
HTTP Response Splitting

Additionally, XyberShield correlates information from all the sessions of every website protected by a XyberObserver, to improve the security for all users of the solution, not just the Dole Food Company.

Based on their ongoing experience, Dole chose to activate multiple security options available within XyberShield.

## XyberFrames: Adaptive, Modular Protection

XyberFrames are adaptive modules designed to prevent specific application-level attacks. **Dole.com** is protected by the SQL Injection XyberFrame. Other XyberFrames currently active on **www.dole.com** include Functional Abuse, Navigational Abuse, Brute Force, and the OWASP bundle.

The Open Web Application Security Foundation (OWASP) is a not-for-profit worldwide organization focused on improving the security of application software. The OWASP-specific XyberFrame bundle defends against the top ten most dangerous activities on the internet as defined by OWASP, including cross-site scripting, cross-site request forgery, SSI injection, SQL injection, and HTTP response splitting.

Other modules are available to address specific industry needs, such as the PCI XyberFrame, which aids users who seek PCI compliance.

Security breaches via web application attacks are some of the costliest, consumptive threats to online business. Since the integration of XyberShield into its security framework, the Dole Food Company has experienced no negative business impact due to attempted web application attacks.

## For more information

Contact your XyberShield sales representative or XyberSecure Business Partner, or visit us at:
www.xybershield.com

For more information on Dole Food Company, visit:

www.dole.com

## About XyberShield, Inc.

XyberSecure, Inc. provides easy to-deploy web application security services and real time website threat intelligence solutions. XyberSecure employs a global Tier-1 infrastructure with tactical operations centers on both coasts of North America and 55 points of presence in 22 countries. XyberSecure is a privately held company.



XyberSecure
575 Market Street,
40th Floor
San Francisco, CA 94105
U.S.A.

Produced in the United States of America
March 2011


Document approved 23 March 2011

Please Recycle