Company
Telco service provider with millions of subscribers and thousands of employees across 80 locations.

Challenges

- Protecting employees from malware while providing them with secure access to uncategorized and potentially risky sites
- Minimizing operational overhead from complex web access policies and support tickets requesting access to blocked sites

Solution
Symantec™ Web Isolation on-premises and in the cloud, protecting employees at the office and on the road from malware and ransomware.

Benefits

- Eliminate web-borne malware threats by protecting against zero-day exploits
- Enable secure access to uncategorized and risky sites
- Protect against malicious web documents
- Minimize support tickets requesting access to blocked sites
- Simplify and streamline web access security policies

The Threat of the Unknown Web

To protect employees, the telecommunication and cellular service provider has deployed a secure web gateway from a leading vendor (not Symantec). The gateway's policies and URL filtering capabilities blocked access to uncategorized and risky sites. However, this common practice introduced friction between the security team and the business, which required broader web access, and resulted in significant overhead to security operations.

The telco provider blocked uncategorized sites that lacked sufficient reputational information for classification. These sites present considerable risk as they often include new and relaunched malware sites. Preventing access to uncategorized sites helped protect the organization, but it also blocked legitimate, uncategorized business sites, irritating users and reducing business productivity.

Moreover, employees were not allowed to access file sharing and webmail sites, such as Google Drive and Gmail, which were considered risky because they can be used to deliver malware into organizations. By blacklisting these sites, the company blocked an attack vector, but at the expense of inconveniencing executives relying on these services.

Support tickets increased as frustrated users requested access to blocked sites. Furthermore, access policies generated significant complexities. "Maintaining policies was exhausting and hard to track," says the company's chief information security officer (CISO). "You block sites, then open them for some users, block them again or add them to a whitelist." Security was quickly becoming a barrier to business.

Not only was more friction introduced, but the company was still vulnerable to attacks. URL filtering made it possible to manage and minimize risk, but did not eliminate it completely. Malware could still be delivered from whitelisted unclassified websites. In addition, the company was very concerned with attacks delivered via downloaded documents using zero-day exploits in Microsoft Office files and PDFs.

> "With Symantec, we isolate web traffic to eliminate threats from uncategorized and potentially risky sites."
>
> — *Chief Information Security Officer*, Leading Telco Provider

“

It’s rare to find a security solution that actually mitigates an entire attack vector. Symantec Web Isolation allowed us to eliminate the most advanced web-borne malware including zero-day and ransomware.”

— *Chief Information Security Officer*
Leading Telco Provider

The Solution: Symantec Web Isolation

The CISO considered building a solution in-house, using Remote Desktop Protocol or other desktop virtualization technologies, to isolate the corporate network from the internet. However, desktop virtualization is known to have its user experience shortcomings and failed to meet the company’s scalability requirements. “Maybe we could get 30 users per server,” the CISO says, “but we would need hundreds of servers to support all the employees in the company.”

With Web Isolation, the CISO can provide secure, broad internet access for thousands of concurrent users, without over-blocking legitimate business sites.

The Web Isolation solution treats all traffic as malicious, executing and rendering web sessions remotely, away from endpoints. The user’s browser receives a safe visual stream from the Symantec platform, preventing web-borne threats delivered through malicious sites from reaching users’ devices. Web Isolation isolates web-borne threats easily: No client, plug-ins, or agent needs to be installed on endpoints.

Today, the company uses Web Isolation to protect the web traffic of thousands of users. Symantec’s flexible hybrid on-premises and cloud deployment protects employees at the office, on the road, and at home.

Results

With the Symantec solution, users can access any website, safely. “We are now protected against any web-borne threat delivered through uncategorized or risky sites,” says the CISO.

Even senior management is noticing the difference. “An executive came to me the other day, ecstatic about using a file sharing service from home,” says the CISO. “Before deploying Symantec Web Isolation we had to block file sharing and webmail altogether.”

With Symantec Document Isolation capabilities, the company eliminated ransomware and other attacks delivered through files by enabling employees to view and print documents without needing to download them. Web Isolation also allows the company to run files through Symantec Content and Malware Analysis in cases where files need to be downloaded.

The security team also realized operational improvements. Allowing access to uncategorized sites resulted in fewer support tickets and allowed IT to consolidate and unify access policies for the entire organization.

Moreover, by eliminating web-borne threats, Web Isolation minimized security alerts, incidents, and investigations. The criticality of updating and patching browsers decreased, especially as Symantec enabled the company to remove Java and Flash from endpoints—a common security underbelly at organizations supporting legacy applications.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_CS_TelcoUnknownWeb_v1.indd