IS YOUR ORGANIZATION ADEQUATELY PROTECTED AGAINST INTERNET THREATS?

When employees use the internet at work, they expose organizations to an array of security threats such as phishing, viruses, malware, and ransomware.

According to a Verizon report from 2016, **30% of phishing messages** are opened by users

– Business Insider

As many as **one million** new malware threats are released daily

– Symantec and Verizon

In 2015, the average cost of web-based attacks for organizations was over **$7 million**

– Ponemon Institute

Our recent survey of executives and IT security professionals working for large organizations across many industries including finance, healthcare, government, IT, technology, education, and retail revealed insights into the challenges of internet-related security vulnerabilities.

THE INTERNET IS A STRATEGIC ASSET FOR BUSINESS.

96% of respondents' companies allow their employees to browse the public internet from their work devices

93% of respondents
indicated that their company's employees need internet access for work-related research

Top employee needs
for internet browsing include research, training, and access to cloud-based applications

...But not all browsing is business-related.

Almost half of respondents
indicate that their employees use the internet for personal uses such as checking private email accounts and accessing social media

Regardless of how employees use the internet, organizations are a simple click or download away from being compromised by a virus or malware.

ORGANIZATIONS ARE TRYING TO MAKE INTERNET BROWSING MORE SECURE.

In addition to firewalls,
46% of respondents' companies
use a commercial security product such as a proxy or virus filter

Regardless of the security measures they already have in place, most IT professionals feel they are unprepared to handle external threats and security breaches resulting from employee internet browsing.

Over 20% of respondents
indicate that their organization does not have a strategy in place to manage secure browsing

BY ISOLATING THE BROWSING EXPERIENCE, ORGANIZATIONS CAN PROTECT THEMSELVES FROM INTERNET-BORNE THREATS.

Transparent to users, a virtual secure browsing solution provides an additional layer of security, making it simple for employees to access web-based information and cloud applications without compromising an organization's IT resources.

USING A VIRTUAL SECURE BROWSING SOLUTION, ORGANIZATIONS CAN:

- Enable safe browsing while isolating threats from the network
- Ensure a natural user experience using common browsers
- Enhance existing security investments by adding another layer of protection
- Mitigate the threats associated with malware and ransomware such as CryptoWall

A VIRTUAL SECURE BROWSING SOLUTION IS A WIN-WIN FOR EMPLOYEES AND ORGANIZATIONS

For employees, a virtual secure browser offers a **transparent** user experience that looks and feels like a standard browser – because it is.

For organizations, a virtual secure browser offers an **effective** solution that isolates malware and ransomware from the local network.

ERICOM'S COMPLETE VIRTUAL SECURE BROWSING SOLUTION:

- Leverages existing security investments
- Isolates the browsing environment outside of the local network to minimize security threats associated with viruses and malware
- Lets employees access the internet freely using any standard browser
- Allows organizations to provide internet access without compromising security or exposing the local network to threats
- Offers centralized management, eliminating the need for endpoint installation and maintenance

TO LEARN MORE ABOUT ERICOM'S VIRTUAL SECURE BROWSING SOLUTION, VISIT:

www.ericom.com/demosite/secure-browsing.html