DATA SHEET

Zscaler™ Security Preview

IS YOUR NETWORK VULNERABLE?

- Common viruses
- Cross-site scripting attacks
- Malicious code
- Phishing attacks
- Malicious websites
- Malware in zipped and executable files
- Browser cookie stealing
- Executable file downloads
- Sensitive data leaks, including credit card data, intellectual property, U.S. Social Security numbers
- Embargoed websites in countries designated by the United States and/or European Union

HOW HEALTHY IS YOUR SECURITY?

Your IT environment has evolved significantly over the past decade, expanding from a centralized data center approach to a more cloud and mobile-centric model. Attackers have adjusted their tactics along the way, shifting their focus from servers in your data center to your users and web browsers, and developing cyber-attacks that elude traditional signature-based security methods Unfortunately, enterprises have largely failed to keep pace with these changes, continuing to use dated methods to thwart attacks, and appliance-based security infrastructure to protect an increasingly cloud and mobile centric workplace. As a result, despite costly on-premise internet security solutions, many enterprises find vulnerabilities in their current infrastructure.

Zscaler Security Preview tests vulnerabilities in your network through a simple, comprehensive Web-based tool to help your organization pinpoint security gaps and recommend the appropriate action to properly secure your network and content. In fact, 85% of companies who run this test find vulnerabilities that require immediate attention, and numerous companies have found security holes resulting from misconfiguration or lack of capacity.

In just 60 seconds, Zscaler Security Preview can give you an instant risk assessment of your current security and compliance infrastructure, with recommendations for closing any gaps. You can run Security Preview at anytime, view the results online and save them as a PDF report, and share the findings with your colleagues.

CHECK YOUR INTERNET SECURITY NOW

Zscaler's quick, confidential and safe test can pinpoint weak spots for you to take action.

FREE RISK ASSESSMENT

http://securitypreview.zscaler.com/

WHAT WE TEST

Zscaler Security Preview runs a series of browser-based tests to quickly check for vulnerabilities in your current Internet security infrastructure. Eight of these tests are focused on security threats, and five of them are focused on compliance enforcement. Note that Security preview runs in your browser, won't access any data, and won't introduce malware or change any settings. You may see alerts in your security system.

Security Tests

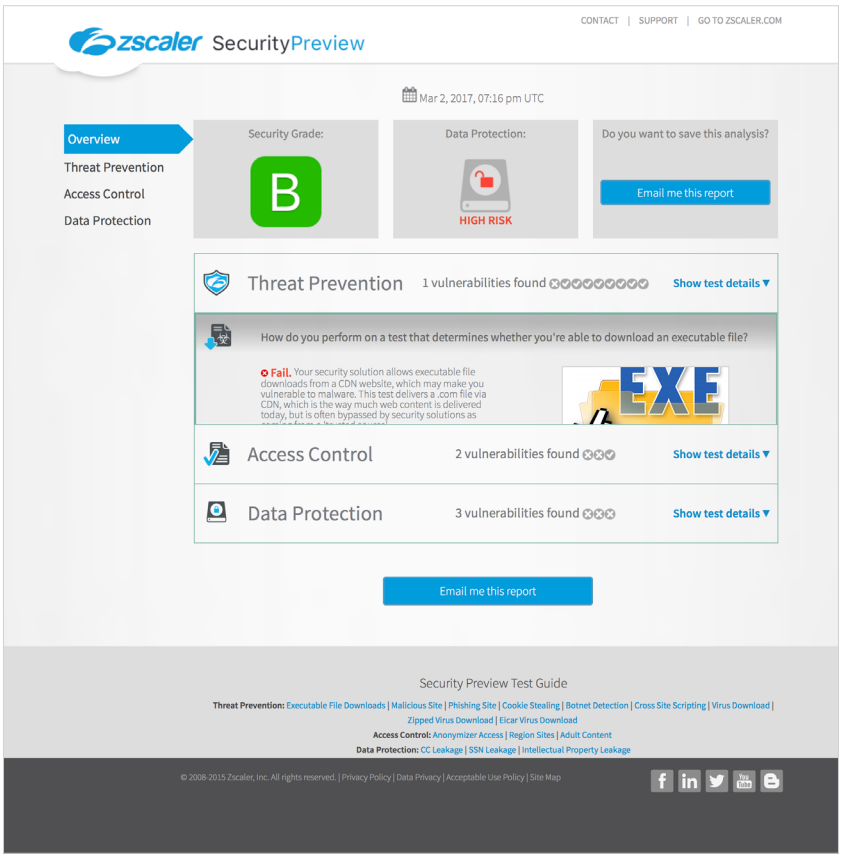
- **Botnets** – Once a device is compromised, it's no longer entirely under your control - criminals can now direct it to exfiltrate your intellectual property, infect other machines on your internal network, participate in Distributed Denial of Service attacks, email spam, spreading spyware, and other malicious attacks. This test tries to contact a known Botnet command and control server ('calling home') to determine if your internet security infrastructure will stop it..
- **Cross-site scripting (XSS)** – Cross-site scripting (XSS) attacks can steal a web visitor's credentials and session keys (e.g. passwords and other sensitive data). This test visits a website that has been compromised by malicious code and checks to see if it is able to compromise your web browser.
- **Viruses** – 99% of anti-virus engines detect and block this common virus at the network level. This tests checks to see if your infrastructure will block a virus coming from a CDN, which is how most web content is delivered today.
- **Phishing** – Criminals typically target phishing attacks at employees to steal corporate credentials or sensitive personal data. This test checks to see if your computer is able to access one of the latest validated phishing sites uncovered by Phishtank.com.
- **Malicious Sites** – Hackers can launch zero day and 'watering hole' attacks by compromising legitimate sites with malicious code. This test checks to see if your security solution blocks a malicious page hosted on a compromised site.
- **Download EXE** – Malware is often distributed through executable files downloaded from unknown websites or app stores. This test tries to download an executable file to test whether your system blocks, analyzes or quarantines it.
- **Zipped Viruses** – Criminals sometimes try to deliver their virus payloads using compressed/zipped files. Unzipping takes computational power that can slow traffic down, so many appliance-based security systems skip analyzing files zipped multiple times. This test attempts to download a file containing a virus that is zipped multiple times.
- **Cookie Hijacking** – Cookie theft is the primary way criminals steal personal information such as logins to Gmail or corporate accounts on Oracle or Salesforce. This test takes a cookie from one website and tries to post it to a second one, a clear sign of an attempt to hijack the web session.

Compliance Tests

- **Data Leaks** – Stealing your customer data and intellectual property is the goal of some of the world's most dangerous hackers. This test checks to see if your security solution can detect and block attempts to leak sensitive data including credit card numbers and social security numbers by various online methods such as posting to a website or emailing.
- **Anonymizers** - Employees often try to bypass company policy by using anonymizing proxies that allow them to visit blacklisted websites, or view pornography or other harmful content. This test checks to see if your security solution allows you to use an anonymizing website by trying to visit a blacklisted website through a well-known anonymizer.
- **Embargoed Countries** – Most companies wish to comply with US and EU trade laws and prevent users from visiting websites in countries that are under embargo. Additionally, compromised websites are often hosted in countries that are hostile to the United States and the European Union. This test checks your ability to visit a website located in North Korea, which is under US and EU Trade embargo.

THE TEST WILL:

- Take less than 60 seconds
- Give you a detailed, printable report
- Not download any malicious content
- Not modify current security policies
- Not access any data on your systems



About Zscaler

By 2008, Zscaler founders could see that business was transforming, moving away from the corporate network and into the cloud. Believing that the only way to deliver security for the cloud would be in the cloud, we set out to build a global, multi-tenant platform with comprehensive, integrated security services and access controls to protect organizations from cyberattacks and prevent data loss. Today, Zscaler operates the world's largest 100% cloud-delivered security platform, helping thousands of leading organizations make the secure transformation to the cloud. Learn more at **www.zscaler.com**.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com