



### ABOUT TRUSTe

Since 1997, TRUSTe—the leading trustmark and recognized authority on Internet privacy—has been helping the most successful online brands confidently manage Web site privacy complexity and satisfy regulatory compliance.

TRUSTe Privacy Seals help consumers click with confidence by guiding them to trustworthy Web sites. Thousand of Web sites rely on TRUSTe to provide an industry-leading platform to deliver privacy and security across multiple geographies, continuously scan and monitor for vulnerabilities, and independently mediate and resolve customer disputes.

In 2009, TRUSTe acquired state-of-the-art malware detection and scanning capabilities to address more points where consumer privacy can be compromised. Most of the top fifty Web sites are certified by TRUSTe, including Yahoo, Facebook, MSN, eBay, AOL, Disney, New York Times, Comcast and Apple.

## TRUSTe SITE REPUTATION SERVICES: STOPPING MALWARE AND PROTECTING BRANDS

Today, corporate sites use rich, user-generated content in the form of web-app mash-ups, user photos and videos to foster community and support e-commerce sales. These sites also use portals, discussion boards and blogs to help better communicate with customers, partners and suppliers, and include multiple direct content feeds from third parties, including advertisers. But as these technologies grow more popular, they also present new security risks. Previously, companies could avoid the brand risk and legal liability of site security breaches (\$6.6 million per incident in 2008 according to the Ponemon Institute) by focusing their efforts on perimeter security. But cybercriminals have begun to penetrate established, well-known sites through both their user-generated content and third-party content-providers in order to harm users and steal sensitive information directly from customers.

Unfortunately, criminals are targeting well-known legitimate sites because they're popular. In one month, TRUSTe's content scanning and detection service found crimeware attacks on 23% of the Alexa Top 100. Top brands have the largest audiences, which makes them the most desirable target for fraudsters. When a site becomes a conduit for user harm and fraud, both the corporate brand and user trust are at stake. TRUSTe Site Reputation Programs provide a proactive reputation filtering and scanning solution that allows top brands to leverage social and third-party content without leaving their sites vulnerable and ruining their carefully built reputations.

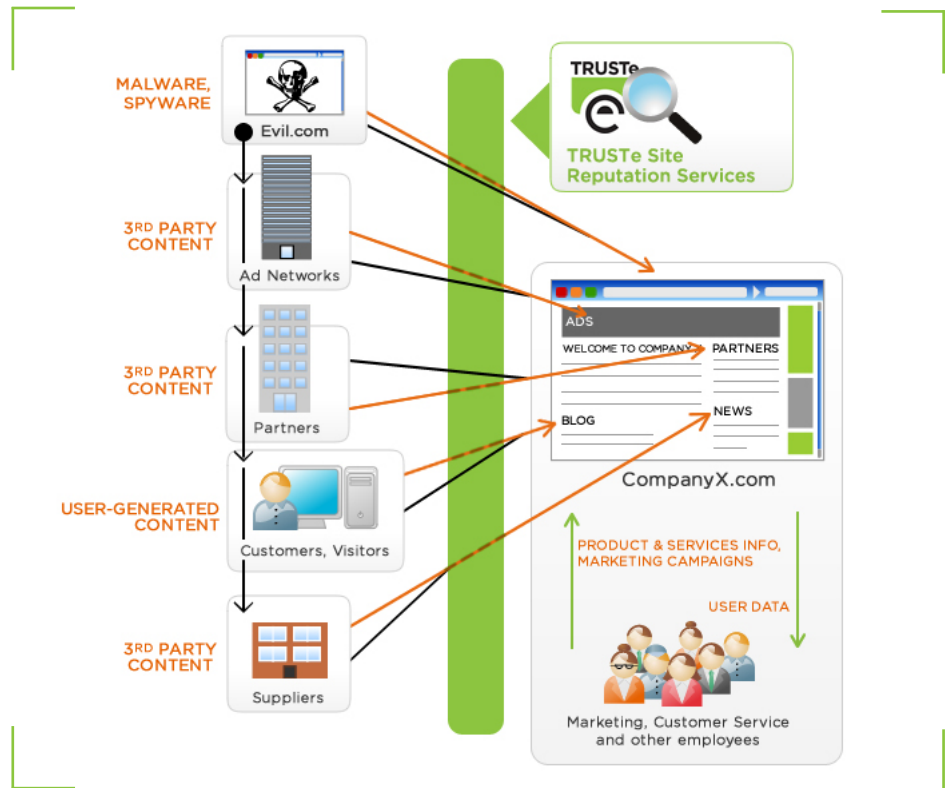


Figure 1: Company Web sites interact with many entities - making them vulnerable at many points

## TRUSTe SITE REPUTATION SERVICES

TRUSTe Site Reputation Services (TSRS) consist of four components that offer high-level protection for today's Web sites:

### Heuristics-based Dynamic Scanning Engine



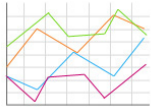
- Scans forms for types of personally identifiable information (PII), checks downloadable content and user age information, etc.
- Scans all types of user-generated content (UGC) and third-party content such as Flash, mash-ups, photos, videos, blogs etc.
- Detects dynamic malware that appears as a user to Web sites; triggers full site behaviors and evaluates resulting activity

### Rich Site-Reputation Database



- Offers a rich, granular data-set of 10 million sites & 500 million URLs
- Grows at a rate of 3 million URLs per day
- Keeps accuracy rate of less than 20 false-positives over the past two years

### Automated Recording & Replay Capabilities



- Captures and records the details of each attack
- Provides full playback for analysis and documentation

### Customizable and Flexible Scanning & Monitoring Capabilities



- Customizes scanning based on breadth and depth of the site, scan frequency etc.
- Pinpoints infection at an individual URL level, not just the entire site
- Scans and monitors highly dynamic sites 24/7

TSRS has three different delivery models to better meet our customers' needs.

<b>Deep Site Scanning</b>	Provides comprehensive vulnerability scanning for all sites, including those with active or frequently updated content, or high-value transactions. This type of scanning is especially suited for any site that has UGC or third-party content.
<b>Malicious URL Feed</b>	Issues from a constantly updated database. Allows network-security providers to strengthen their coverage of malicious sites. Ideal for ISPs and other service providers and web portals.
<b>Real-Time Content Reputation API</b>	Allows site-owners to check the safety of any content against TRUSTe's site-reputation database before content is uploaded. Protects site reputations on an ongoing basis. This API is suitable for publishers and content aggregators that allow upload of URLs with data for blogs, Wikis, news feeds, etc.

## BENEFITS

TSRS integrates quickly and easily into existing web content infrastructure to ensure the safety of user-generated and third-party content, protecting a company's brand and ensuring that users maintain confidence transacting at their site. Our solution is unique in several respects:

- Highly targeted to address social and third-party attack vectors
- Leading-edge threat-detection capability
- Rich data to support advanced decision-making algorithms
- Flexible implementation options to ensure ease of setup for range of site types and use cases

## DID YOU KNOW?

- 1 in every 10 web pages contains malware  
*-Google*
- 12,000 new URLs are infected every day  
*-Secure Computing*
- 5 million malware programs were introduced in 2007  
*-McAfee*
- 60% of the top 100 most popular Web sites have either hosted or been involved in malicious activity in the first half of 2008  
*-Websense*
- Even the best anti-virus engines in the market fail to cover a significant fraction of web malware  
*-Google*

TRUSTe  
55 2nd Street, 2nd Floor  
San Francisco, CA 94105  
T 415.520.3400  
E [nflowers@truste.com](mailto:nflowers@truste.com)  
F 415.520.3420  
W [www.truste.com](http://www.truste.com)