Trustwave®
Smart security on demand

# BLENDED THREATS MODULE AND SECURE EMAIL GATEWAY

## WIPE OUT TARGETED ATTACKS

## OVERVIEW

Criminals who organize targeted attacks based on blended threats emails use social engineering techniques to craft email messages that appear to be from a trusted sender but actually contain a link to a website hosting malicious code. They will then use a variety of tools for greater access to information and systems.

Trustwave Blended Threats Module, used in conjunction with Trustwave Secure Email Gateway (SEG products), provides a powerful solution to targeted attacks and blended threats. Using real-time behavioral analysis and content inspection, the Trustwave Blended Threats Module blocks any site serving suspicious or malicious code. Because the service doesn't rely on signatures, it is never out of date when it comes to catching and neutralizing new exploits.

### How it works

**Trustwave SEG products (on-premise)**
Trustwave SEG is used to configure which URLs are rewritten and when. Administrators can use numerous rule criteria to ensure that their policy exactly meets their requirements and add URLs to a white list, providing further flexibility and control when creating URL rewriting rules. Any URLs that have been rewritten will subsequently be redirected through the cloud-based Trustwave Blended Threats Module.

**Trustwave Blended Threats Module (cloud-based service)**
The Trustwave Blended Threats Module provides uncompromising security with no management overheads. Running as a cloud-based service means that protection is extended to any recipient who is forwarded a link that has been rewritten by Trustwave SEG products.

The Trustwave Blended Threats Module analyzes millions of URLs daily, providing protection against targeted attacks and blended threats and feeding into Trustwave Lab's research.

The Trustwave Blended Threat Module uses the same technology as the Trustwave SWG to analyze the true intent of a webpage. Rather than relying on reputation or signature-based protection, it separates a webpage into its individual components (HTML, Java, Flash, ActiveX, etc) putting each through their own dedicated analytical engines. Any obfuscated or hidden information is decoded and also subjected to rigorous analysis. Then additional deep code analysis determines a behavioral profile that reveals any potential malicious combination of the separate functions. This identifies and mitigates both unknown and dynamic threats.

When a website is determined to be hosting malicious code, the Trustwave Blended Threats Module will inform the user that access has been denied. As the URL has already been rewritten by Trustwave SEG products, this protection will be afforded to anybody who is subsequently forwarded the message, including users trying to access the compromised website via a mobile device or over webmail.

## SEG PRODUCTS FLOW


1. Trustwave SEG products receives the email for scanning and decides that a URL in the message body needs to be analyzed. It rewrites the URL, prepending it with a unique customer reference and a link to the Trustwave Blended Threats Module.
2. When a user clicks on the link, the request is directed through the Trustwave Blended Threats Module for analysis.
3. The Trustwave Blended Threats Module analyzes Web content associated with the link, subjecting it to numerous checks for behavior and intent.
4. If the webpage is free from malicious code, it is served to the user. If not, then the user receives a block page indicating that he or she has been protected from a targeted attack.

## FEATURE/BENEFIT MATRIX

| FEATURE | BENEFITS |
|---|---|
| **Multi-layered anti-malware engine featuring Trustwave SWG dynamic and real-time code analysis** | Both targeted and opportunistic attacks use advanced techniques to evade detection, exploit vulnerabilities and compromise computers. Real-time code analysis identifies the behavior and intent of code being served by a webpage. It does not rely on signatures to ensure protection against both known and previously unseen attacks, which account for 60% of the modern malware missed by anti-virus, firewall, IPS/IDS and reputation-based solutions. Preventing machines from being compromised in the first place removes the costs associated with being the victim of any successful malware attack, such as desktop reimaging, loss of data, damage to reputation or even fines. |
| **Rewrites URLs** | With a rewritten URL, the link is scanned by the Trustwave Blended Threats Module whenever a user clicks on the link, even if that email has been subsequently forwarded. This ensures that the target website is scanned at the time of access so there is no window of opportunity for an attack to take place. |
| **Scans websites on access** | During a staged targeted attack, the malicious code on a webpage may only become active after a certain period of time or for short spells during a day. This ability to hide, combined with the way active malicious code may change, means that it is essential to scan a website each and every time it is accessed from an untrusted link and the dynamic nature of the webpages. |
| **Reports back to Trustwave SEG products** | The Trustwave Blended Threats Module feeds information back into Trustwave SEG products on a frequent basis to provide essential data for reporting and analysis. This data allows administrators to identify users who may be a particular target or those who may need additional security awareness training. It can also be used to demonstrate a return on investment from the service based on the number of attacks it has prevented. |
| **Block page informs users of a threat** | Notifying users of a potential threat not only stops them from visiting a website hosting malicious code, but it also acts as a reminder about safe computing habits, encouraging them to adopt a more cautious approach when browsing the Internet. |
| **Hybrid architecture** | A hybrid approach provides both the benefits of a service combined with the precision of an on-premise product. Reducing management overheads and ensuring security, the Trustwave Blended Threats Module is simple to configure and manage, with on going security updates managed by Trustwave in line with the latest research and threat intelligence available from the Trustwave SpiderLabs team. |

LEARN MORE AT TRUSTWAVE.COM

Trustwave®
Smart security on demand

For more information: https://www.trustwave.com.