

# 防網頁竄改攻擊

## ZERO TRUST

TrustONE

### 担心网站网页被黑客开了后门漏洞吗？

近年黑客入侵网站事件频传，常见许多网站遭「一句话木马」攻击导致数百万个资被窃，因此许多企业机关纷纷导入网站防护措施，然而市面上常见WAF网站防火墙、网页侦测或回复类型的防网页篡改产品，还是有其技术上的瓶颈



## BOTTLENECKS 瓶颈

1. 若遇到新型态攻击或防火墙规则定义不完整，还是无法有效预防网页被篡改。
2. 透过侦测网页异动来自动回复，容易产生回复次数过度密集，影响系统效能的问题。
3. 当网站内容频繁更新，难以做到实时性的比对回复，此时的空窗期若被搜索引擎发现网站含有恶意软件，就会被列为有害网站，严重影响公司声誉与流量

# TrustONE 防网页篡改解决方案

面对新型态攻击与既有防网页篡改产品之瓶颈，TrustONE以「ZeroTrust零信任」技术为主轴，可防止黑客从内部入侵网站服务器或从外部攻击网页漏洞，避免网页被删除篡改、被放置恶意软件或植入后门程序等威胁。

## 防护功能

# PROTECTION

### 1. 零信任Zero Trust可因应新型态攻击

- 以「零信任」为技术主轴。将网站文件夹设为「匿踪保护区」，保护区内的文件夹即使透过安全程序也无法删写，如同将网页制成光盘，只能浏览无法写入，不让黑客有篡改机会。

### 2. 不影响主机效能

- 不进行侦测或回复，无须消耗硬件系统运作效能，即可做到网页防篡改效果。

### 3. 可保护常见网页格式

- 针对目前常见的网页格式提供防骇保护，就算黑客窃取到最高管理者权限，也无法修改或删除。

# MANAGEMENT

## 管理功能

### 事件纪录及主动警示



可搭配TrustONE Server的事件纪录及主动警示功能，监控受保护的网页档案文件夹，将违规事件纪录提供给管理者，如果达到大量违规条件，系统将主动警示管理者。

### 可提供API整合第三方平台



TrustONE Server提供API功能，可以与第三方应用程序协同作业，如：SOC资安监控服务，将搜集到的威胁情资汇出以便管理者判断分析。

零信任保护：即使黑客取得AD管理帐号也无法中断TrustONE的防御

受到保护的WEB网站

黑客无法修改网页数据  
(ex: "一句话木马"恶意代码)

匿踪网站网页文件夹  
(jsp/php/asp/aspx...)  
零信任保护：连安全程序也无法删写

ATTACK 1  
从内部入侵主机

ATTACK 2  
从外部入侵网站

# TECHONE

志壹网络科技(上海)有限公司  
TECHONE (Shanghai) Co., Ltd.

業務洽詢：  
上海市闵行区程家桥路175号206室（虹桥奕境文创园）  
400-100-2592  
(紧急联系电话：18621311066 黄先生)