TrustOne (Endpoint Security)

TrustOne, based on endpoint security protection expertise over thirty years, provides customers with “Effective、 Lightweight 、AI Model” endpoint security solutions, eliminating “overloaded, complex, ineffective” problems in traditional endpoint security management.

TrustOne empowers enterprises with stronger security protection capabilities through innovative technology and intelligent management, helping them to easily cope with complex and ever-changing threat landscape.

Effective

Combined with attack surface evaluation model, TrustOne continuously detects the asset exposure and defends against known and unknown threats in real time.

Lightweight

Lightweight integration with multiple security capabilities, supporting all operating systems.

AI Model

AI-based assessment on all kinds of risks throughout digital transformation.

70M

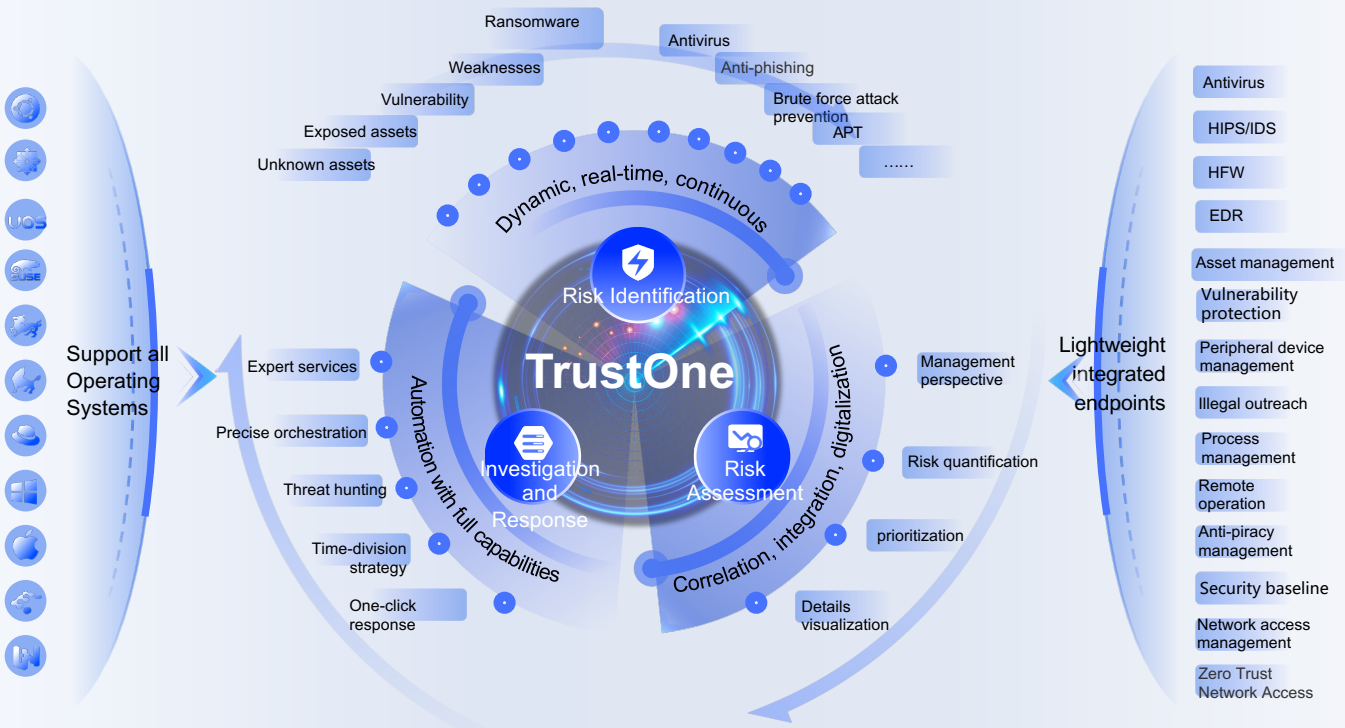
Protected endpoints

30+yrs

Service experience.

8,000+

Clients. Over 70% clients which are among Fortune 500 choose Asiainfo Security



Product Introduction

Product Functions

Attack Surface Management (ASM)

- TrustOne actively identifies and detects known, unknown, and Internet exposed assets through Endpoint Agent 7×24 hours from an attacker's perspective, thus continuously discovering and evaluating weak parts in the organization, making them visible and scoring them based on their risk.
- Based on the risk index, TrustOne can quickly converge assets attack surface before the attack occurs through various mitigation functions. Risks are identified and attacks would be prevented.

Attack Protection

- Combined with machine learning, behaviour monitoring, incident containment, cloud antivirus and traditional threat signatures, TrustOne can effectively prevent all kinds of known and unknown threats.
- TrustOne provides full threat defense and endpoint security management, supports large-scale hierarchical deployment and multilevel management architecture, and provides a complete integrated endpoint security protection solution.

Detection and Response

- Based on well-defined logs, the EDR module combines threat intelligence, IOA rule association analysis, big data intelligent algorithm and visibility feature to provide a complete closed loop of warning before incidents, event logging and response during incidents, and investigation and audit after the incidents.
- The security incident investigation and response time is reduced from weeks to hours.

Vulnerability Protection

TrustOne provides two protection modes: physical patch and virtual patch:

- **Physical patch**: timely access to the installation status through task tracking; timely rollback for defect patches to reduce business impact; built-in patch repair algorithm to reduce download and installation time.
- **Virtual patch:** Industry's first virtual patch, without intrusion into the operating system or application, no extensive application compatibility testing, while intercepting vulnerability attacks from the network side.

Operation and Maintenance Management

- TrustOne combines technology and operation & maintenance tools to strengthen the entire endpoint security system and support Windows/Linux clients at the same time.

Endpoint Access

- Multi-dimensional access control technology, the system can adopt 802.1x, ARP, DHCP, SNMP, policy routing, bypass mirroring, transparent bridge and other access technologies, supporting bypass, serial connection, probe, grading and other deployment forms.

Value

One Step Faster

Identify and respond to attacks in time, effectively mitigate the disadvantages on defense side.

Reduce MTTD from Months to Days, MTTR from Days to Hours.

Pain Points: Traditional security starts from the passive defense when facing threats. Modern cyber attacks are multi-dimension attacks based on huge amount of data. Stacking up passive defense features is not effective, or even invalid.

Value: Dynamic proactive defense starts from attackers' view. TrustOne can constantly identify different known and unknown assets that exposed on the Internet, as well as all kinds of vulnerabilities, thus continuously eliminating the exposure and risks at frontline.

Simple to Install, Use, and Maintain

Pain Points: To effectively protect from attacks, endpoint maintenance has become more and more complicated with antivirus, security baseline, HFW, process management, access management, asset management, vulnerabilities management, DLP, EDR, IDS…… overloaded endpoint security products not only harass system compatibilities, but also waste huge amount of endpoint resources.

Value: TrustOne integrates antivirus, virtual patching, EDR, desktop management, SDP, VP, network access management and several other features all in one. The deployment of TrustOne is lightweight, thus greatly reducing the deployment time and system resources.

95%↓ Install package size

94%↓ Install time

97%↓ CPU usage

89%↓ Memory usage

75%↑ Business continuity

8MB install package with **16** endpoint protection capabilities

7 endpoint protection modules

0 Compatibility Issues

230+ operating system system versions support

AI-based operation

Pain Point: Digital transformation introduces huge amount of endpoint assets into the environment with various problems. Analysis based on manual work can hardly understand the enterprise risks as whole or focus on risks with high priority.

Value: Based on attackers' view, TrustOne can leverage "assets attack surface security assessment model" and "dynamic priority algorithm for vulnerability repair", to prioritize threats, then focus on and respond to key incidents with high risks, achieving the global operation visibility.