Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Endpoint
Cyber Security Solution

What is Endpoint Security Solution?

Endpoint cyber security systems protect computers and other devices on a network or in the cloud from cyber security threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats that rely signature-less detection using machine-learning and artificial intelligence defense and prevent techniques.

Key Components

- Machine-learning classification to detect zero-day threats in near real time
- Advanced anti-malware and anti-virus protection to protect, detect, and correct malware across multiple devices and operating systems
- Proactive web security to ensure safe browsing on the web
- Integrated firewall to block hostile network attacks
- Actionable threat forensics to allow administrators to quickly isolate infections
- Centralized endpoint management platform to improve visibility and simplify operations
- Agent and agentless scanning of the network for detection and classification of devices

Why Endpoint Cyber Security Solutions?

TARGETED ATTACKS DATA BREACHES	FILE-LESS ATTACKS	RANSOMWARE
Cyber security landscape is constantly evolving with new more complicated attack methods and never-before seen threats. When a stealth attack or data breach occurs, organizations are typically caught off guard that their defences were compromised or are completely unaware that the attack even took place. Once the attack is finally discovered, organizations then reactively implement mitigations to stop this attack from being repeated. However, this does not protect them from the next attack that may use different kind new vector.	New threats, called file-less malware, exist entirely in computer memory, making it difficult for file scanning based protections to detect it. Furthermore, some file-less attacks will leverage currently installed applications that are built into the OS to make it even harder to detect a malicious payload. For example, the use of PowerShell in these attacks is very common.	Ransomware has been a relentless concern for businesses across the world ever since Crypto-locker in 2013. Despite ransomware surviving for far longer, it was never a major threat that industries were concerned about. However, now a single incidence of ransomware can easily render a business inoperable by encrypting important or necessary files. When a business experiences a ransomware attack, it quickly realizes that the backups it has are not recent enough, so the business feels as though it must pay the ransom.

Endpoint Device Control

DTS offers the perfect endpoint security solution component that examine for new obscure devices and controls access to removable media devices, such as USB drives. It can allow, block, or monitor access to removable media devices, as configured by the security administrator. It's that simple!

Features

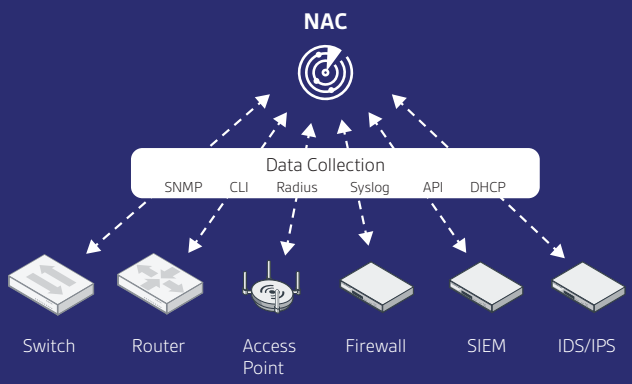
Prevent Data Theft	Make sure unauthorized devices can't copy data, no matter how they get plugged in
Protect Endpoints from Malware	Gain better visibility and control over enduser devices with access to endpoints, such as rogue Wi-Fi/Bluetooth beacons, USB sticks, key loggers, and printers.
Enhance Security Policies	Centrally manage devices and data, using a whitelist / "default deny" approach
Flexible Architecture	DTS's Device Control solution is flexible and easily manageable. Police removable devices across the organization with a scalable solution and central database

Endpoint Cyber Security Solution

Endpoint Network Access Control (NAC)

The phenomenon of Internet of Things (IoT) devices along with threats posed by unauthorized and rogue devices connecting into the network, has made it crucial for organizations to improve their visibility into what is attached to their networks. IT security teams need to know every device and every user accessing their networks. However, they are inherently untrustworthy, with designs that prioritize low-cost over security. DTS Solution's partner NAC product provides the network visibility to see everything connected to the network, as well as the ability to control those devices and users, including dynamic, automated responses.

This is also a key component that is required to establish DTS's Zero-Trust Access Fabric Architecture.



Features and Benefits

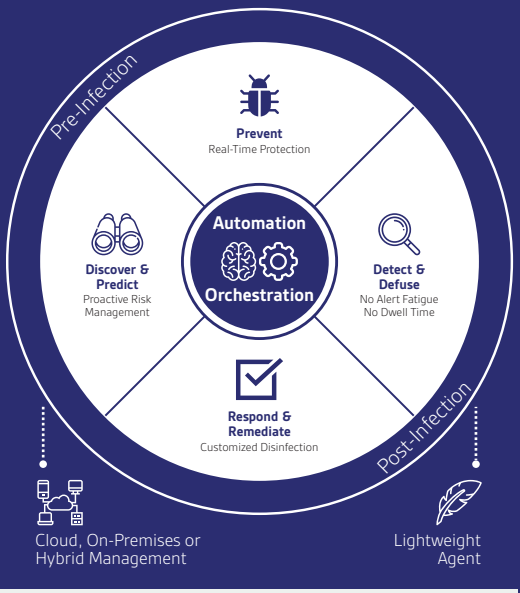
Agentless Scanning	Detect and identify devices as they connect to the network
Simplified On-boarding	Automate onboarding process for large number of endpoints, users, and guests
Micro-segmentation	NAC solution can strictly enforce and restrict network access for those devices to only necessary network assets
Multi-vendor Support	Interact with and configure network devices (switches, wireless access points, firewalls, clients)
Cost-effective Scalability	NAC architecture enables effective scaling to multi-site locations and supporting millions of devices
Zero-Trust Architecture	NAC provides the essential component that supports the Zero-Trust Security Architecture model

Endpoint Detection and Response (EDR)

Advanced attacks take seconds to compromise endpoints and ransomware attacks take seconds to cause damage to an organization's systems and infrastructure. Find out how DTS Solution's partner EDR protects organization's endpoints pre- and post-infection and see how EDR detect and defuse threats in real-time, automatically to protect the endpoint and prevent a breach.

Features

- Discovery with proactive attack surface risk mitigation
- Next-generation antivirus (NGAV)
- Real-time and automated breach protection
- Maps threat detection and protection against MITRE ATT&CK model
- Orchestrate incident response with customizable playbooks
- Guided interface with data enrichment



Platform Support	A single, integrated management console provides prevention, detection, and incident response capabilities.
Offline Protection	Protection and detection happen on the endpoint, protecting disconnected endpoints.
Native Cloud Infrastructure	DTS Solution's partner EDR features multi-tenant management in the cloud. The solution can be deployed as a cloud-native, hybrid, or on-premises. It also supports air-gapped environments.

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com