threatdefence_

SOLUTION BRIEF

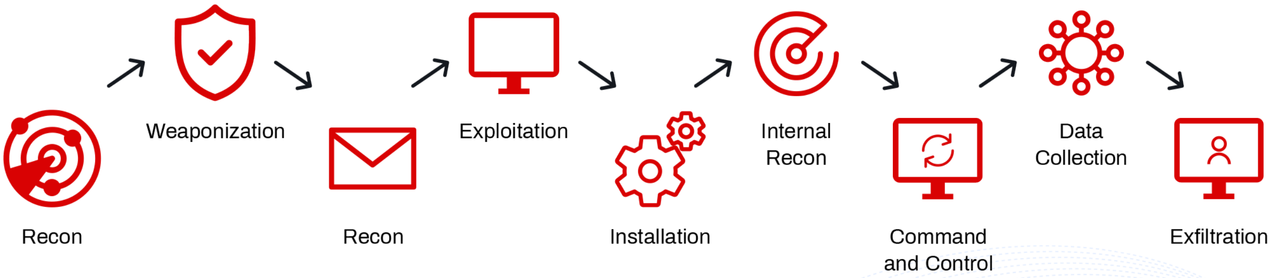
_ENDPOINT

A zero-trust detection and response without boundaries. Hunt the most elusive cyber threats regardless where your data or users reside.

ThreatDefence provides deep detection and response capabilities to your endpoints, 24x7, no matter where users or data reside. _ENDPOINT is a single, lightweight agent that pairs endpoint detection and response (EDR) capabilities with our elite threat hunting team, providing great visibility and eliminating blind spots missed by traditional security tools.

_ENDPOINT is supplied as a core technology with our Extended Detection and Response platform and complemented by our Managed Detection and Response service offerings. The _ENDPOINT agent introduces unmatched visibility capabilities, as well as holistic security inventory functionality to enrich security data collected from our sources and to help reveal the most elusive actions conducted by the most sophisticated threat actors.

The agent supports our managed detection and response capabilities, collecting critical security data from on-premises, cloud, and mobile endpoints and supplying information across the whole cyber-attack chain, from the initial reconnaissance to the malicious data exfiltration.



WHAT IT DOES

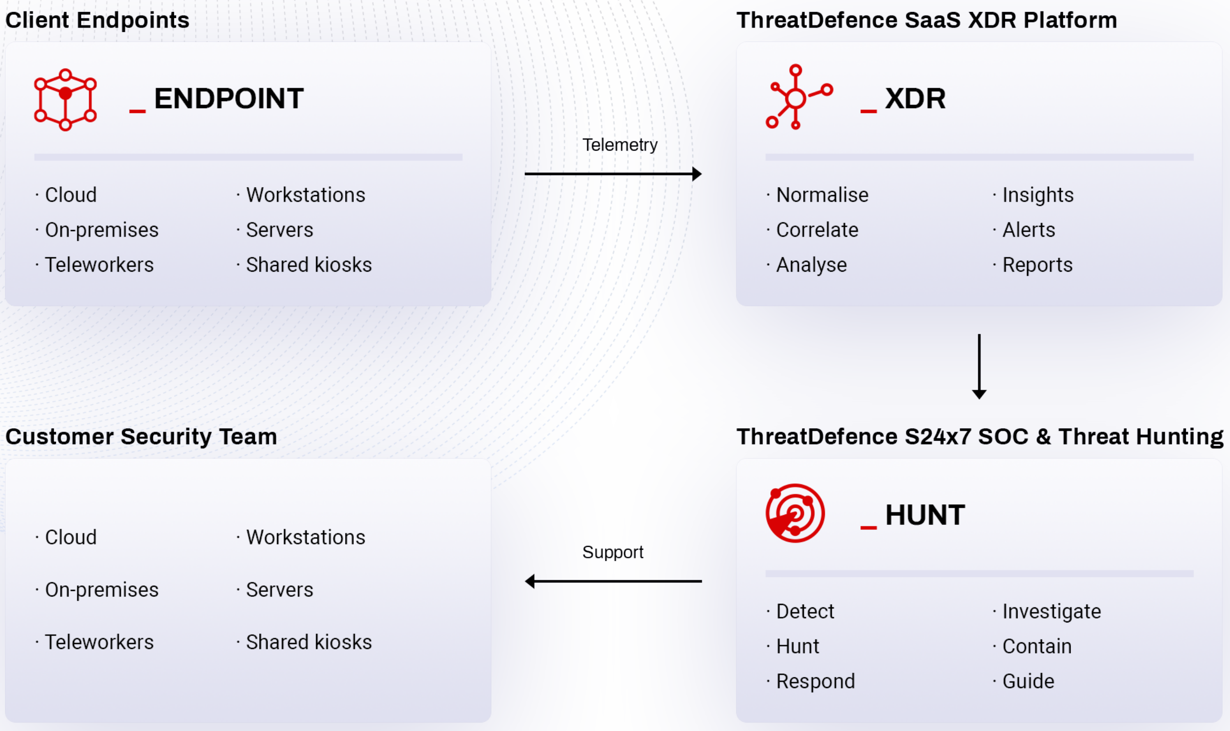
The _ENDPOINT agent derives critical insights from the endpoints in real-time, analysing vulnerability data, system, and process usage telemetry, user behaviour, and many other metrics and indicators. The collected data is correlated with security events collected from any other assets in your organisation and supports our threat hunting team to deliver continuous threat detection. Empowered by the collected data and by our machine-learning technologies, our threat hunters can continuously assess risks, identify any malicious behaviour, and proactively respond to threats before they propagate to the rest of your network.

With an increasingly mobile workforce, businesses can no longer rely on traditional centralised log collection and detection solutions. Advanced endpoint visibility is a crucial component of securing the mobile workforce and teleworkers, which is why we are including the _ENDPOINT as the core technology for all our solutions.

Our _ENDPOINT agent provides:

- Advanced endpoint visibility, including in-depth operational and asset management data
- Endpoint vulnerability management and reporting, including data from the operating system and installed applications
- Detection of malicious activities based on MITRE ATT&CK framework
- Benchmarking of system and application security controls
- Continuous risk reporting
- Managed detection and response services
- Support of major operating systems including Windows (Desktop and Server), Linux, and MacOS devices.

HOW IT WORKS



Client Endpoints

_ ENDPOINT

- Cloud
- On-premises
- Teleworkers
- Workstations
- Servers
- Shared kiosks

Telemetry

ThreatDefence SaaS XDR Platform

_ XDR

- Normalise
- Correlate
- Analyse
- Insights
- Alerts
- Reports

ThreatDefence S24x7 SOC & Threat Hunting

_ HUNT

- Detect
- Hunt
- Respond
- Investigate
- Contain
- Guide

Support

Customer Security Team

- Cloud
- On-premises
- Teleworkers
- Workstations
- Servers
- Shared kiosks

- Unprecedented visibility across workstations, server, cloud and teleworker endpoints
- Automated deployment
- Works from anywhere without specialised connectivity requirements
- Detection of unknown threats
- Delivered at no additional cost as part of our MDR solution
- Security baseline and security configuration monitoring
- Maintain a continuous compliance state
- Cyber risk and security posture continuous assessment and monitoring

FULL ENTERPRISE ATTACK SURFACE COVERAGE

Our XDR platform provides full enterprise coverage, integrating all the security data you can possibly reach into, including data that directly resides within your network and on your endpoints, as well as the external data such as cloud workloads, SaaS applications, Dark Web breaches, compromised credentials, external vulnerabilities, and weaknesses and exposures related to third-party organisations in your supply chain

_ENDPOINT

Advanced endpoint visibility, forensic analysis of endpoint telemetry, detection and response

_NETWORK

Detect insider treat and lateral movement with network-based intrusion detection and packet analysis

_CLOUD

Multi-cloud security insights, cloud workload vulnerability management and continuous risk assessment

_OSINT

Continuously integrated Open Source Intelligence, including indicators from Dark Web, social media, and third-party vulnerabilities

_ANYTHING

Any standard or custom application or log source, completely integrated into the platform

ABOUT THREATDEFENCE_

ThreatDefence provides innovative MDR, SOC-as-a-Service, and proactive cyber defence solutions to MSPs and Enterprises. Our Adaptive XDR Platform was created to help companies of any size to deploy a world-class detection and response, embracing all information that businesses can reach to, would it be within their network, on the Dark Web, or hiding deep into their supply chain. We believe in open ecosystems and connect you to any and all threat intelligence feeds and log sources, instantaneously providing you with actionable security insights. For more information, visit www.threatdefence.com.