TRELLIX ENDPOINT SECURITY SUITE (TRXE1)

REAL–TIME ENDPOINT PROTECTION, DETECTION, INVESTIGATION, AND RESPONSE TO ADVANCED THREATS

A security suite that extends the Trellix Protect Plus EDR for Endpoint bundle with investigation and endpoint analysis features. A forensic-powered solution that allows on–premises deployments. It helps collect forensic data and look for signs of compromise; allows connecting to a workstation to gather additional data and remediate threats.

ADVANTAGES:

- Search and investigate known and unknown threats across thousands of endpoints in minutes
- Reduce threat detection and response time to minimize potential disruption
- Respond and manage the threat defense lifecycle to maintain user and administrator productivity
- Detect and prevent new malware through to machine learning
- Automate and simplify complex workflows
- Increase IT department productivity by managing the suite from a single console
- Reduce the need for additional SOC resources through managed investigations

COMPONENTS:

ePolicy Orchestrator (ePO) – a central endpoint management server that can be deployed on-premises or in the cloud, including SaaS

- Manual/automated deployment and security tools updating
- Security policy configuration for threat and data leak protection and OS built–in encryption management
- Infrastructure health queries and reports
- Infrastructure compliance with security standards
- Automated administration and response to any threats
- Integration with third–party solutions
- Ability to manage infrastructure from anywhere

Endpoint Security (ENS) – next-gen protection for Windows, macOS, and Linux

- Behavioral and signature analysis based on reputation
- Containerization – dynamic application containment
- Protection against scripting attacks
- Isolation of systems with suspicious activity
- Automatic recovery after threat elimination

Trellix Endpoint – a Windows Defender upgrade with Endpoint Security features

- Centralized management of Windows Defender, Firewall, and Exploit Guard
- Windows Defender extension with next–gen technologies
- Optimal solution for protecting systems with minimal resources
- Minimal use of resources

Trellix Insights – a cyberattack information database and security policy auditing tool

- Practical recommendations for security improvements
- Source of Indicators of Compromise (IoC)
- Integration with Trellix EDR for IoC search in your infrastructure
- Security policy auditing

Trellix Endpoint Forensics (HX) – performs fast and accurate forensic investigations on thousands of endpoints

- Cyberattack prevention on endpoints
- Detection of malware and other signs of compromise on workstations across the enterprise
- Quick response to endpoint security incidents

Application Control for PCs – module for application launch control based on black/white lists

- Fixing applications and their versions in the OS
- Blocking of any executable files
- No signatures
- Low use of system resources
- Windows XP support

Threat Intelligence Exchange (TIE) – central reputation database of executable files

- Reputation aggregation from security solutions (including third–party ones)
- File reputation exchange between security solutions
- Manual centralized reputation management

Data Exchange Layer (DXL) – a technology for storing and sharing system information, telemetry, and reputations

- Near–instant information sharing and real–time task coordination
- Reduced delay, facilitated and simplified integration of multi–vendor solutions

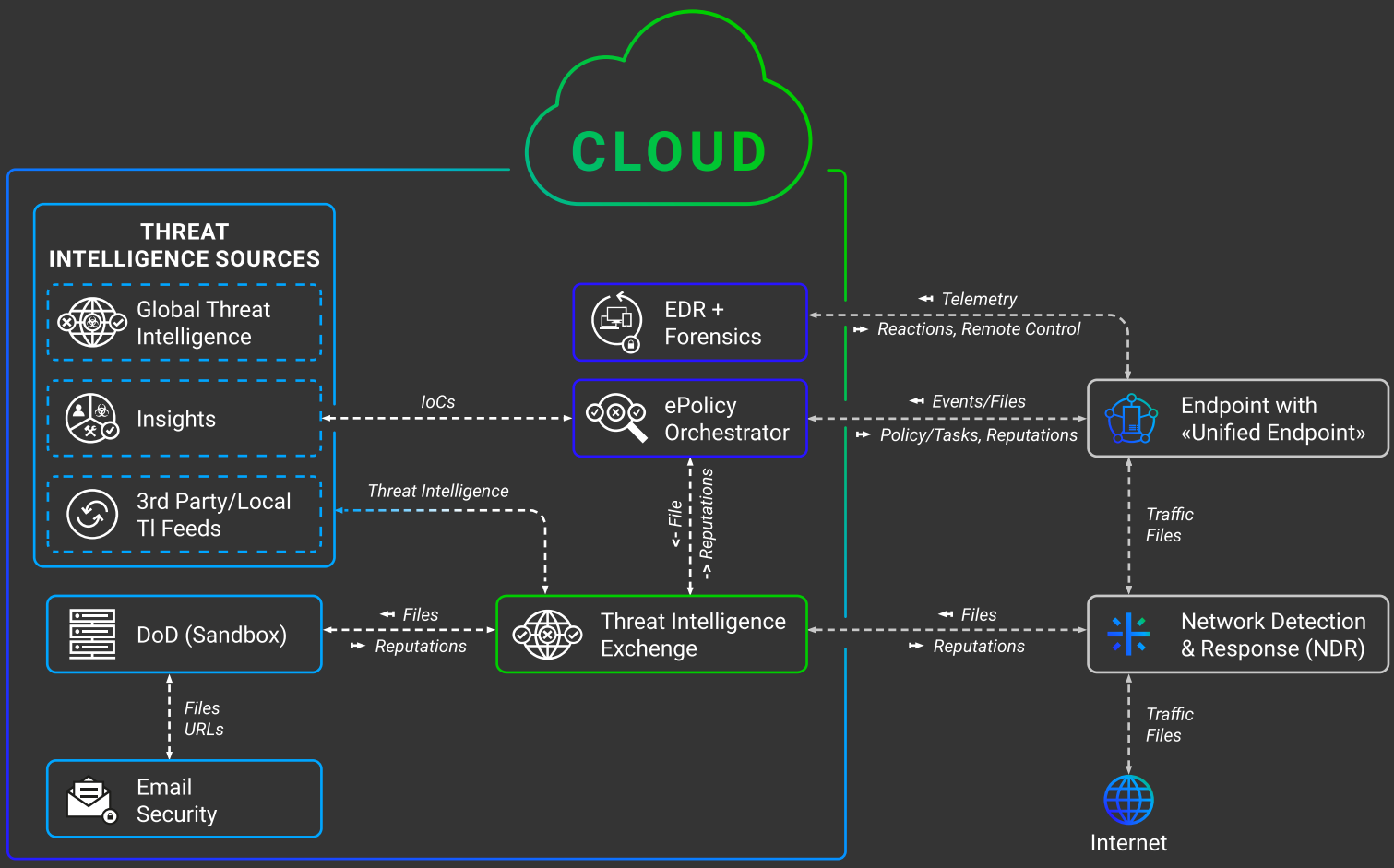
Trellix EDR – an advanced threat detection and response tool

- Continuous endpoint monitoring
- Professional investigation with artificial intelligence
- Real–time search for traces on endpoints
- Incident response through running scripts (including custom ones)

Device Control – a tool for monitoring and managing any device connected to your systems

- Black/whitelists of devices
- Prevention of reading/recording onto storage media
- Control of mobile device connection
- Detailed reports for each incident

ARCHITECTURE:



Note: Email Security, DoD, and NDR are not included in this package