todyl

Endpoint Security (EDR + NGAV)

Endpoint Detection & Response and Next-Generation Anti-Virus

End attacks before they become a breach

Today's threat landscape demands better endpoint security. Threat actors constantly evolve their approach to bypass defenses, frequently executing sophisticated attacks in-memory to stealthily evade detection. To make matters worse, many endpoint security products rely on static signatures, such as detecting hashes of binaries, that threat actors can easily bypass.

Todyl's Endpoint Security module combines EDR and NGAV into a powerful, cloud-first solution. Advanced machine learning (ML) and behavioral analytics continuously optimize Todyl's Endpoint Security, helping businesses stay ahead of evolving threats and detect the latest exploits, vulnerabilities, and Zero-Days. It delivers powerful Malware, Ransomware, Malicious Behavior, and Memory Threat Protection, providing advanced defenses against known and unknown threats.

Benefits

Stops Attacks in Real-Time
Advanced ML and behavioral analytics identify and analyze attack artifacts in real-time to prevent attacks

Deep Detection Without the Noise
Receive actionable alerts with continuously optimized detection rules to eliminate alert fatigue

Prevent Tomorrow's Threats
Block sophisticated in-memory attacks and fileless malware with industry-leading Memory Threat Protection

Highlights

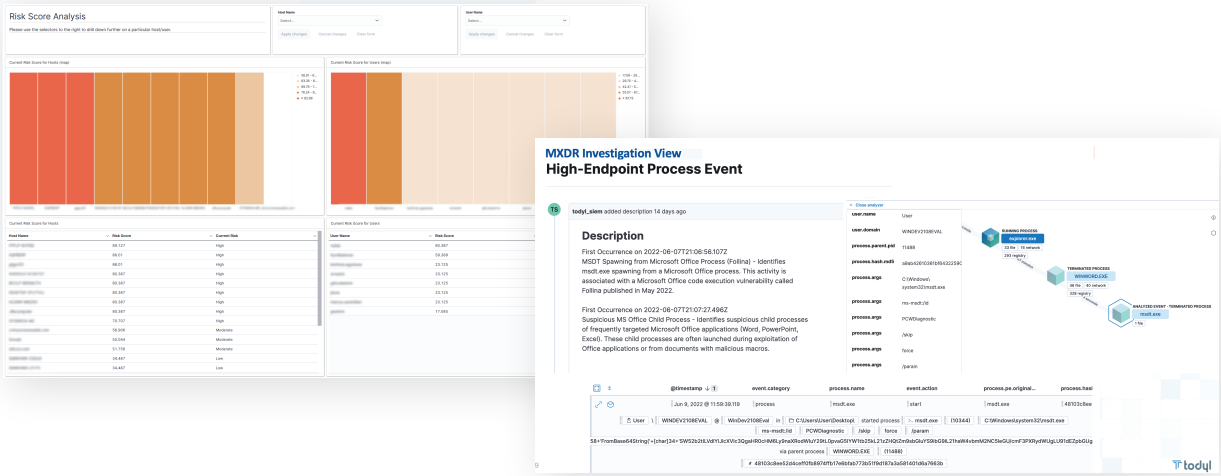
Real-Time, Global Updates
Managed detection rules go out globally in real-time to prevent and detect the latest exploits, vulnerabilities, and Zero-Days.

Complete Visibility
Continuously monitor endpoints with kernel-level data collection for full spectrum insights, from process to file to memory and more.

Ransomware Canaries
Identify and shut down potential infections earlier in the attack lifecycle to reduce the risk of a successful ransomware attack.

AI and Behavioral Analytics
Detect and prevent evolving, advanced threats with host-based behavior analytics that dynamically identify changes that indicate an attack.

Complete Protection
Malware, Ransomware, Malicious Behavior, and Memory Threat Protection defend against evolving threats without reliance on static signatures such as binaries.



More Powerful Together:
Todyl's Endpoint Security + SIEM

Todyl's Endpoint Security is purposefully integrated with the Todyl Managed Cloud SIEM. When an incident is detected, a case automatically opens with enriched data to power investigation and analysis. The SIEM correlates data from across environments, providing invaluable context and unmatched visibility, enabling you to:

- Leverage managed threat hunting dashboards
- Search and analyze logs with enriched telemetry and aggregated information across environments
- Build interactive visualizations to investigate events
- Run queries against environments to see if the same activity can be found on other endpoints

Key Capabilities

Cloud-First
As a cloud delivered solution, Todyl's Endpoint Security is quick to deploy, continuously optimized, and highly scalable. It delivers cutting edge protection with nearly zero impact on endpoint performance.

Machine Learning and Behavioral Analytics
A powerful analysis engine identifies and alerts to changes that deviate from your baseline, leveraging threshold and sequenced-based indicators.

Ransomware Protection
The integrated ransomware protection leverages advanced machine-based analytics and ransomware canaries to detect and stop evolving ransomware variants.

Memory Threat Protection
By efficiently identifying and analyzing attack artifacts to identify memory manipulation, Todyl prevents and detects in-memory attacks in near real-time.

Malware Protection
The advanced machine learning model detects and stops malicious attacks by searching for static attributes to determine if a file is malicious or safe.

Malicious Behavior Protection
Analyze system activities or behaviors associated with known and potential Indicators of Attack (IoA) to detect and stop a broad range of attack techniques.