



# CTS® Cardinal Technology Solutions, Inc.

EDR + 24/7 MDR **ENDGAME.**

## COMPREHENSIVE ENDPOINT SECURITY

### Endpoint Detection & Response + 24/7 Managed Detection & Response

Fully managed and fully customizable prevention, detection and response solution that runs in-line on the endpoint and follows your custom playbooks and business processes. Unlike traditional anti-virus software that only prevents known threats based on a signature-based detection methodology, our EDR/MDR solution prevents known and unknown threats leveraging machine learning, behavioral analysis, external threat intelligence and signature-based methodologies for comprehensive protection.

**Malware and Ransomware Prevention:** Machine learning-powered malware prevention for known or unknown malware, with 99% block rate and zero false positives. Behavior-based ransomware prevention blocks attacks before full disk encryption.

**Phishing Prevention:** Industry's first machine-learning based phishing prevention for Microsoft Office documents. The platform blocks malicious macros pre-execution, achieving greater than 99% efficacy.

**Exploit and Fileless Attack Prevention:** Full protection against memory-based attacks with patent-pending process injection prevention. A unique malware scoring system prevents malicious module loads, DLL injection, and shell code injection, preventing adversary evasion and fileless attacks.

**MITRE ATT&CK Alignment:** Bring consistency to incident information and allow for faster alert triage, assessment and decision making with more than one-hundred pre-built ATT&CK rules.

**Managed Detection & Response:** Highly-trained security experts work as an extension of our team to provide 24x7 prevention, detection and response services to protect your users, systems and data.

- Prevent: Analyze potential security gaps and adjust countermeasures
- Detect: Continuous monitoring and analysis of alerts and anomalous behavior
- Respond: Neutralize threats and manage the incident following customer defined playbooks



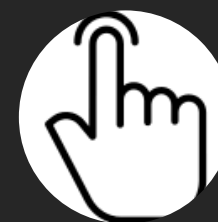
### Always-On Protection:

Single agent with always-on protection for off-network or off-line devices



### Comprehensive OS

**Support:** Protects Windows, Mac, Linux and Solaris Operating Systems



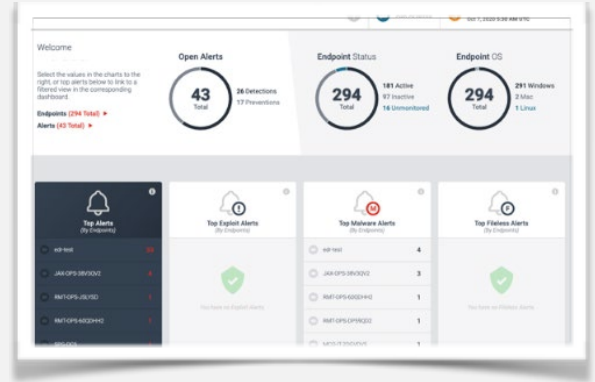
### One-Click Containment:

Terminate a process or isolate a device

# PREVENTION, DETECTION AND RESPONSE

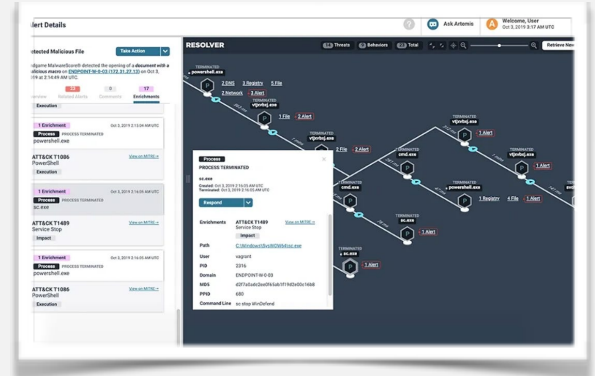
## Intuitive Dashboards

Our dashboards streamline all our administration and agent management, enhance our operations visibility, optimize security incident response, and advanced threat hunting capabilities. Real-time detection and response workflows surface suspicious artifacts across millions of records.



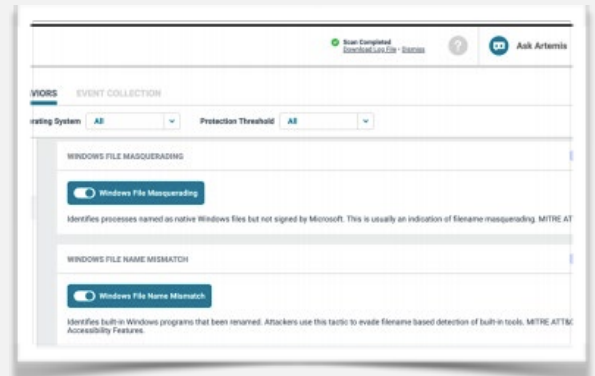
## Attack Visualization

We can visually render the complete incident timeline with real-time activity analysis of your critical data. One-click containment empowers our team to investigate incidents at enterprise scale with zero business disruption.



## Precision Response

We can isolate an endpoint in the event that it's compromised. The response action will lock down the endpoint and only allow it to talk to the MDR/EDR server. We can create separate policies and apply them to designated endpoints as appropriate.



## Third-Party Validation

PCI-DSS and HIPPA Compliant. Pre and post-execution validation from AV Comparatives, NSS Labs, VirusTotal, Forrester, SE Labs, and MITRE. Participation in MITRE's program for public testing, submitting to MITRE researchers for independent testing against targeted attacks.

