NUIX ADAPTIVE SECURITY

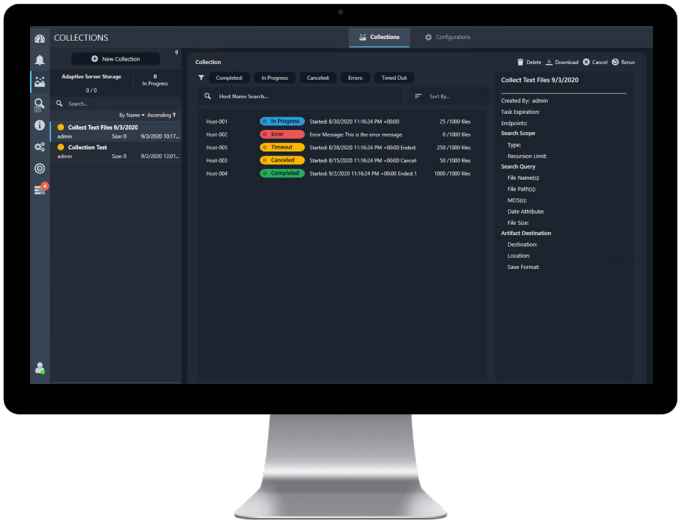
Get the Visibility You Deserve

Visibility into your environment is crucial for detecting, preventing, and investigating breaches. Whether it's by a careless employee, an executive with illegal motives, or a hacker determined to incite chaos and grab priceless sensitive data, data breaches cost the enterprise in large part due to lack of detection, slow response, and inconsistent remediation.

Nuix Adaptive Security provides the visibility, adaptability, control, and data collection capability you've been missing with traditional endpoint products.

THE NUIX ADVANTAGE

- **Compress response time.** Shorten the feedback loop by answering root cause questions in seconds. Use a unified view of live and historical endpoint activity across the enterprise to quickly anticipate and respond to threats.
- **Quickly adapt to changing threats.** Our programmable, intelligent agent gives operators unparalleled power to develop their own detections and automated responses, all based on threat behavior rather than signatures.
- **Stop threats in real time.** A patent-pending, customizable rules engine on the endpoint automatically recognizes and responds in real time to events based on rules and criteria set up by the enterprise.
- **Get intelligent endpoint visibility.** Our lightweight agent (3.5 MB) provides real-time visibility at the kernel level on desktops, laptops, and servers.
- **Collect data forensically.** Move immediately from threat detection to investigations using template-driven forensic data collections from within the alert triage workflow.



Search, filter, and organize single or multiple data sets to effectively triage and respond to an event.

STOP WASTING TIME

By leveraging endpoint analytics across the MITRE ATT&CK framework Nuix Adaptive Security reduces the time it takes to detect an impending or ongoing attack. Our approach accelerates recovery time; makes it easier to adapt to changing environments, regulations, and attack vectors; and ultimately stops incidents in their tracks.

Stop wasting time wading through endless piles of data hunting for elusive threats. Detect and block threats in real time; investigate within minutes; strike back against attackers; and automate response actions to stop data exfiltration and lateral movement. Take back control. Sound good? We think so.

BUCK THE ENDPOINT STATUS QUO

Nuix Adaptive Security has perfected the art of continuous monitoring and response to isolate the important (and often small) signals from the noise and identify uncharacteristic behaviors. How? Nuix Adaptive Security relies on two fundamental and unique elements to drive the protect-detect-respond-remediate process:

- The Digital Behavior Recorder™ continuously monitors and records key digital behaviors including sessions, processes, images, registry, DNS queries, network flow data, files, removable media, printing activity, and keylogs.
- The logic engine provides customizable logic on the endpoint, enabling it to recognize and act on threats in real time.

STAY IN CONTROL FROM THE ENDPOINT TO THE COURTROOM

Start investigations as soon as you confirm there's an incident. Collect seamlessly, either ad-hoc or via templates, and ingest the data directly in Nuix Workstation and Nuix Investigate® for deeper, collaborative analysis.

WHAT YOU CAN DO WITH NUIX ADAPTIVE SECURITY

Nuix Adaptive Security offers a wide portfolio of capabilities, but our customers love the ability to:

- Isolate infected endpoints from the rest of the enterprise
- Immediately distinguish between legitimate and harmful user or application behavior
- Stop ransomware and spearphishing attempts before they execute
- Detect and repel active attackers in real time
- Visualize the execution of a threat as it happens on your monitored endpoints and take direct action to remediate and investigate
- Uncover malware
- Uncover root cause in minutes
- Collect forensic evidence directly from the endpoint
- Keyword search for personally identifiable information (PII) on your endpoints
- Maintain the system's viability—even after being compromised
- Push out remediation across the enterprise
- Mislead adversaries by turning endpoints into decoy targets
- Replace existing antivirus agent with integrated Windows Defender Antivirus
- Automatically record a series of desktop screenshots whenever a potential threat is detected
- Meet Federal Information Processing Standards (FIPS) 140-2 Level 1 requirements

Get the endpoint visibility, adaptability, and control you've been missing.

www.nuix.com/demo

Nuix

Nuix (www.nuix.com, ASX:NXL) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849

PRINT00260223