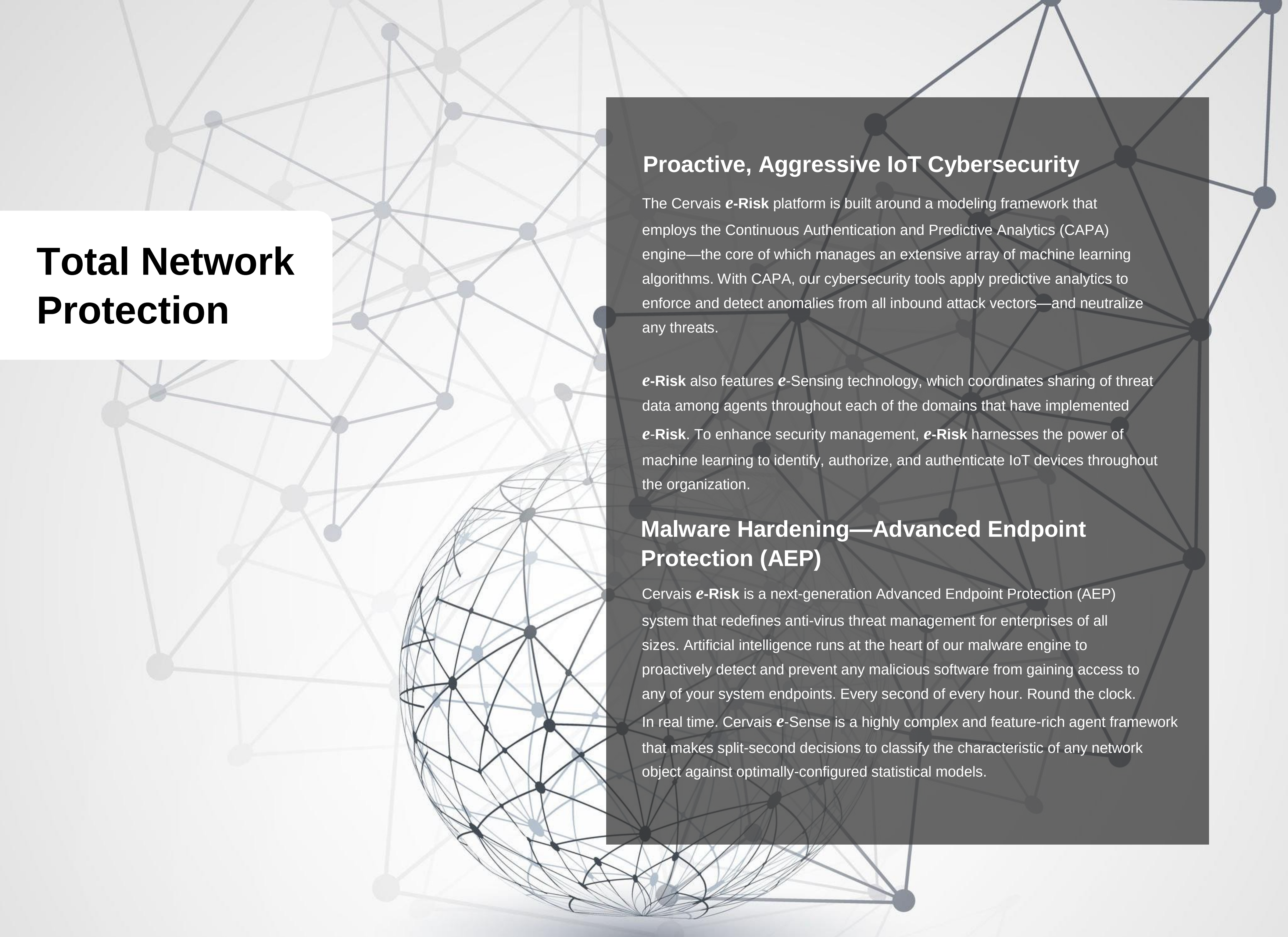
Global IoT Network Protection

Cervais

e-Risk



Total Network Protection

Proactive, Aggressive IoT Cybersecurity

The Cervais **_e_-Risk** platform is built around a modeling framework that employs the Continuous Authentication and Predictive Analytics (CAPA) engine—the core of which manages an extensive array of machine learning algorithms. With CAPA, our cybersecurity tools apply predictive analytics to enforce and detect anomalies from all inbound attack vectors—and neutralize any threats.

_e_-Risk also features **_e_**-Sensing technology, which coordinates sharing of threat data among agents throughout each of the domains that have implemented **_e_-Risk**. To enhance security management, **_e_-Risk** harnesses the power of machine learning to identify, authorize, and authenticate IoT devices throughout the organization.

Malware Hardening—Advanced Endpoint Protection (AEP)

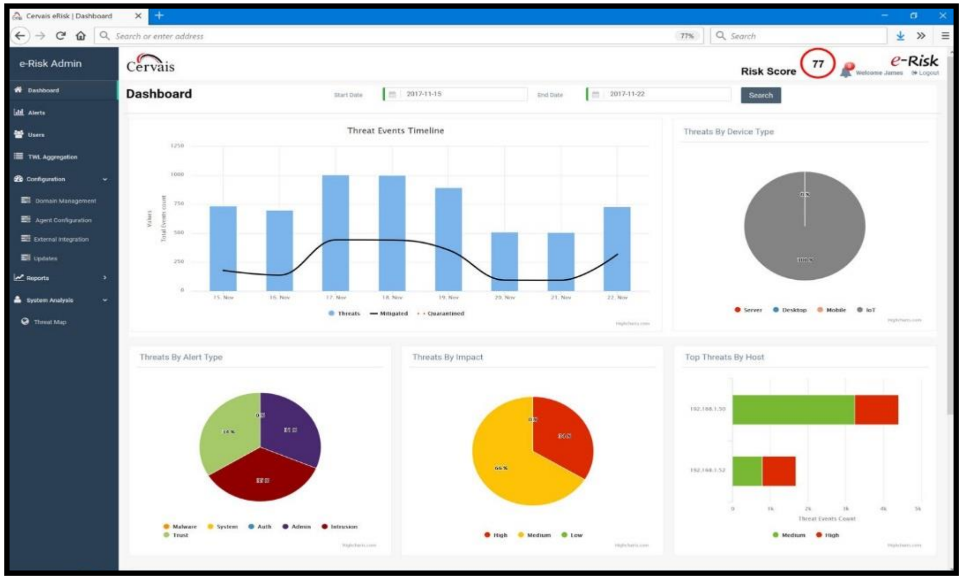
Cervais **_e_-Risk** is a next-generation Advanced Endpoint Protection (AEP) system that redefines anti-virus threat management for enterprises of all sizes. Artificial intelligence runs at the heart of our malware engine to proactively detect and prevent any malicious software from gaining access to any of your system endpoints. Every second of every hour. Round the clock. In real time. Cervais **_e_**-Sense is a highly complex and feature-rich agent framework that makes split-second decisions to classify the characteristic of any network object against optimally-configured statistical models.

e-Risk Threat Monitoring

> “***e*-Risk** PROTECTS INTERNET OF THINGS (IOT) ENDPOINTS—AND ALL DEVICES WITHIN AN ENTERPRISE ENVIRONMENT—BY PROACTIVELY DETECTING AND THWARTING CYBERATTACKS – BEFORE THEY CAN PENETRATE A SYSTEM OR DEVICE. PROPRIETARY MACHINE LEARNING ALGORITHMS DRIVE ***e*-Risk** TO CONTINUOUSLY IDENTIFY BOTH KNOWN AND UNKNOWN THREATS IN REAL TIME.”

When it comes to detecting and mitigating cyber threats, ***e*-Risk** offers best-in-class capability, including static/dynamic analysis and predictive analytics. No other vendor offers a comparable solution. The core of the ***e*-Risk** architecture is the ***e*-Risk Continuous Authentication and Predictive Analytics** (CAPA) engine, which manages an extensive array of artificial intelligence algorithms.

With **CAPA**, our cybersecurity tools apply predictive analytics to enforce and detect anomalies in all inbound attack vectors—and neutralize any threats. ***e*-Risk** continuously monitors all executables, processes, and behaviors to confirm that any suspicious activity is flagged for investigation by your security team.



Start Date 2017-11-15
End Date 2017-11-22

Advanced Data Forensics

Data Forensics

Cervais **_e_-Risk** employs the most advanced data forensics detection and monitoring techniques—including real-time events, process initiation, file system changes, and Windows registry alterations. In addition, Cervais ***e***-Sensing agents are built with highly sensitive threat-intelligence capabilities, which proactively mitigate all threats against the entire network. If necessary, the agent ensures that any intrusion is contained to the endpoint on which it occurs.

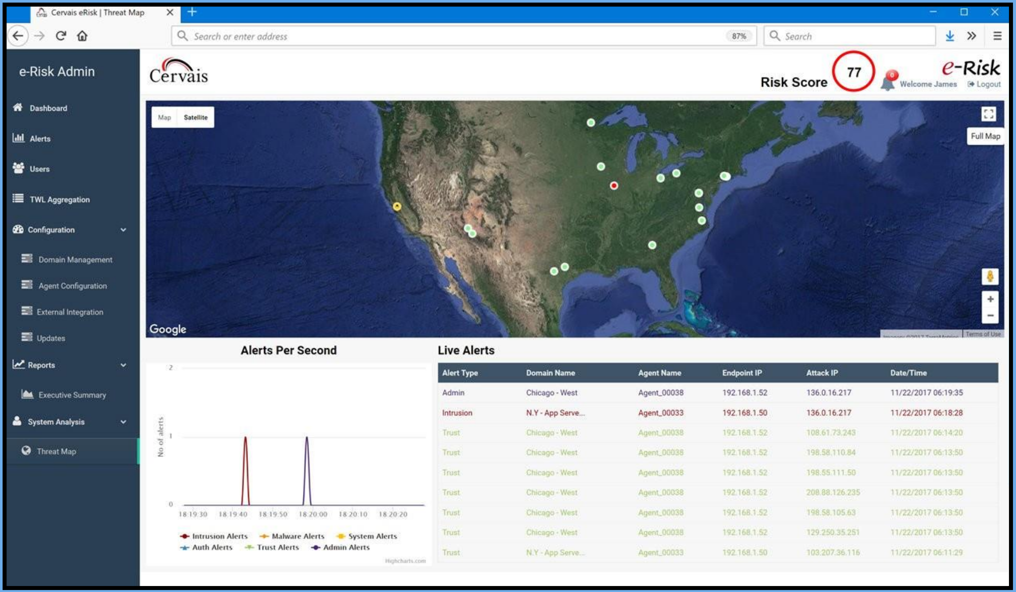
Continuous Dynamic Authentication

User authentication is an elemental feature of any cyber security program. To protect a system, application, or network, an organization ensures that a user is authorized by enforcing positive identification according to username, password, or biometrics.

In some organizations, conventional authentication procedures are insufficient to provide strong security during a lengthy user work session. There is potential exposure when, for example, a user leaves the workstation. **_e_-Risk** includes an integral feature that we call Continuous Risk-Based Authentication (CRA), which extends user authentication beyond the login event—so that it is now a continuous process. CRA is a background subsystem that continuously monitors user input and will trigger an alert if it detects a pattern that indicates unauthorized access.

e-Risk Robust Endpoint Solution

- Provides agent or agent-less integration for management of all types of IoT devices—medical, SCADA, smart meters, cameras, home appliances, and more.
- Performs integrity checks to test for malicious files, on either Windows or Linux.
- Positive identification using behavioral analytics — continuously authenticates users to ensure valid permissions from any endpoint device.
- Real-time verification of trusted relationships (device, human or application) through with device-credentialing services.
- Collects attack-context data as input to incident response intelligence. The ***e*-Risk** console provides pre-execution insights and detonation intelligence from static analysis, dynamic analysis, and predictive analytics.
- Collects external threat intelligence by integrating APIs with a specific threat source.
- Manages sharing of threat data among external organizations that also run the ***e*-Risk** solution.



Live Alerts

Alert Type	Domain Name	Agent Name	Endpoint IP	Attack IP	Date/Time
Admin	Chicago - West	Agent_00038	192.168.1.52	136.0.16.217	11/22/2017 06:19:35
Intrusion	N.Y - App Serve...	Agent_00033	192.168.1.50	136.0.16.217	11/22/2017 06:18:28
Trust	Chicago - West	Agent_00038	192.168.1.52	108.61.73.243	11/22/2017 06:14:20
Trust	Chicago - West	Agent_00038	192.168.1.52	198.58.110.84	11/22/2017 06:13:50
Trust	Chicago - West	Agent_00038	192.168.1.52	198.55.111.50	11/22/2017 06:13:50
Trust	Chicago - West	Agent_00038	192.168.1.52	208.88.126.235	11/22/2017 06:13:50
Trust	Chicago - West	Agent_00038	192.168.1.52	198.58.105.63	11/22/2017 06:13:50
Trust	Chicago - West	Agent_00038	192.168.1.52	129.250.35.251	11/22/2017 06:13:50
Trust	N.Y - App Serve...	Agent_00033	192.168.1.50	103.207.36.116	11/22/2017 06:11:29

KEY BENEFITS

- Stay ahead of the threat curve with next generation, predictive analytics
- Integrated Continuous Diagnostics and Mitigation Support (CDM)
- Central, global dashboard view of potential and actual vulnerabilities
- Drastically reduces overall cybersecurity investment
- Accurate, real-time security event monitoring
- Greatly increases speed to resolution

Cervais

Headquarters Office:
44050 Ashburn Plaza
Suite 195
Ashburn, VA 20147
Office: (202) 873-9234
Toll Free: (855) 910-9141
www.cervais.com

Cervais is a premier, innovative provider of world-class IT security products and systems. We deliver robust, high-performance security solutions that bring you leading-edge capability in managing risk, reducing threats, and securing technology perimeters.

With IoT deployments on the rise, Cervais stands ready to help you implement comprehensive enterprise cybersecurity, identity management, planning, and security services.