OREV Secured Networks – Executive Summary

The Solution for the New Normal in a changing world

A typical enterprise's infrastructure has grown increasingly complex. It may include several internal networks, remote offices with their own local infrastructure, remote and/or mobile individuals, and cloud services. This complexity has outstripped traditional methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise.

The Zero Trust Framework

The OREV architecture adheres to the principles of the Zero Trust Framework. OREV operates on the premise the network perimeter has essentially ceased to exist and attackers will breach the perimeter, further lateral movement is unhindered.

OREV repositions cybersecurity defenses from static, network-based perimeters to focus on identity, users, assets, access management, operations, endpoints, hosting environments and the interconnecting infrastructure. OREV emphasizes resource protection and the belief that trust is never granted implicitly but must be continually evaluated.

OREV coalesces key elements of best of breed Endpoint Protection Platform (EPP) and Threat Detection & Response (TDR) solutions to deliver one singular, comprehensive business and cyber security platform.

OREV combines multiple essential security capabilities – Elimination of security blind spots, vulnerability assessment, intrusion detection, behavioral monitoring, asset discovery, endpoint protection, detection and response, resulting in a unified live end-to-end response and remediation – in one unified console.

OREV is a fully integrated endpoint security solution that combines real-time endpoint monitoring and a vast collection of endpoint data with rules-based automated response and root cause analysis and triage capabilities. The solution provides greater visibility and transparency of user data across endpoints, providing a seamless response and remediation protocol.

OREV is deployed on endpoint devices to protect from file-based malware attacks, detect malicious activities and provide proactive forensic investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

A deep six level correlation analysis is performed; utilizing collected data, proprietary algorithms, and machine learning to find threats across large and disparate data sets, finding anomalies, analyze threat levels, and determine what mitigative actions may be required in response.

OREV's state of the art capabilities enable today's advanced Security Operation Center (SOC) to issue alerts and respond in real time to critical cybersecurity events, providing one focal control point for the entire enterprise digital footprint and assure 24/7 system viability.

What differentiates OREV from the competition? – Critical Advantage: *It's not just reactive, it's predictive*

1) Intelligent Surveillance Technology (IST) Agents – Proprietary, self-sufficient agents, providing "on the spot" analysis and remediation at each end point. By monitoring all workstations, servers, peripheral equipment, and analyzing all operational activities, computing processes, running programs, hardware devices, file, and profile changes – all in real time.

2) Hardware and Asset Management – Out-of-the-box hardware management and visibility into peripheral equipment performance events and infrastructure failures. Monitoring and analysis is predictive as to potential failures and interruption of business activities, keeping the network viable 24/7/365.

3) Insider Threat Protection – Predictive insider threat monitoring and customizable behavioral detection through identity profiling, collating common attributes and continuous monitoring of all transactions to identify potential fraud.

4) Predictive Forensic Investigation – The "Orev Data Universe" The massive data collected and recorded by the Intelligent Surveillance Technology (IST) agents becomes a virtual "data universe", a microcosm of all that transpired in the network, providing an actual subset, replicating the entire activity. The information aggregated facilitates the ability to recreate the tracing of the origins and causes of all events

Total Cost of Ownership:

OREV reduces the total cost of ownership by as much as 50% vs competition:

- The out of the box solution replaces the traditional technology stack with a single platform
- Requires fewer resources, who are expensive and in high demand
- Reduces the variation of skill-sets needed through software simplification and process automation
- Easy to install, deploy, and maintain
- Eliminates multiple legacy solutions
- Cost effective with a significantly lower price point

Use Cases:

- Insider threat detection
- Incident response
- Root cause analysis and triage
- Forensic investigations
- Breach preparation
- Endpoint isolation

Key Benefits:

- Gain greater visibility across all endpoints
- Unified live end-to-end response and remediation
- Lower total cost of ownership by eliminating multiple legacy solutions
- Fewer help desk tickets
- Easier to use – Reduces the variation of skill set needed through software simplification and process automation

Key Capabilities:

- Predictive insider threat monitoring and customizable behavioral detection
- Live end-to-end response and remediation
- Interactive attack chain visualization
- Hardware management and visibility into peripheral equipment performance events
- Audit trail of all network operations at all endpoints

Scalability:

Out-of-the-box, OREV is scalable and works across any platform. OREV can secure and monitor networks of 1,000 to over 200,000 IP addresses, made up of any combination or variety of peripheral equipment, without interference to any other business operations.

OREV performance and functionality supersedes the major competitors:

"We evaluated CrowdStrike and Cylance and decided to implement OREV. It identified a Ransomware bug upon installation - no others did" – Inframerica Airport

INFRAMERICA

LIONSGATE

"We're using other security software, but, OREV gives us an awareness and security depth none else offers" – Lions Gate Entertainment Corp.

"Our network administrator loves the comprehensive dashboard reporting. It saves time, manpower, and we have better control over the network" – Banco Bradesco

bradesco