Breach Resilience – Rapidly Restoring Normal Business Operations After a Breach

Historically, cyber security companies have focused on prevention and detection, which have proven to be inadequate – Breaches still occur daily.

"Security and Risk management leaders should slash defensive cybersecurity spending immediately and redirect it to resilience initiatives."
– Gartner Maverick Research, July 2021

OREV Breach Resilience:

Enables organizations to immediately Identify Breach Root Cause and Recover from compromises faster. Reduce network down time - accelerate identification of any process, file, or application altered AFTER the breach.

Breach Resilience:
- ✓ Recover from compromises faster
- ✓ Reduces network down time
- ✓ Reduces cyber insurance rates
- ✓ Root cause analysis and triage can be performed accurately and rapidly

Forensics:
- ✓ File & process change management
- ✓ Current & historical data
- ✓ Root cause analysis and triage

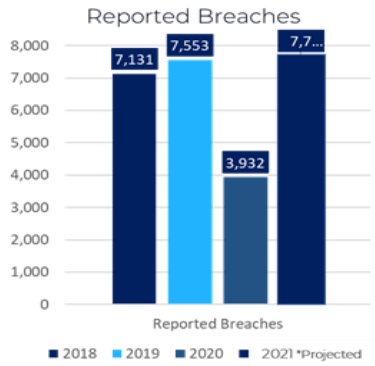
"Transforming cybersecurity into cyber-resilience involves prioritizing breach resilience over defense"
-Gartner Maverick Research, 2021

Visibility:
- ✓ Pervasive visibility across all endpoints
- ✓ Granular telemetry across monitored devices
- ✓ Illuminates security blind spots
- ✓ Gain visibility into performance events
- ✓ First detect (Patent Pending)

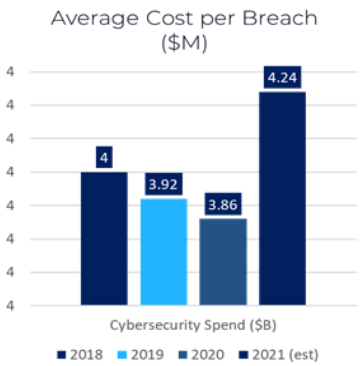
Hardware and Asset Management:
- ✓ Hardware/SW management and optimization
- ✓ Visibility into peripheral equipment
- ✓ Predict infrastructure failures

Scalability: Out-of-the-box, the platform is scalable with demonstrated ability to secure and monitor networks from under 1,000 to over 200,000 endpoints with any combination or variety of peripheral equipment with zero measurable latency on operations.

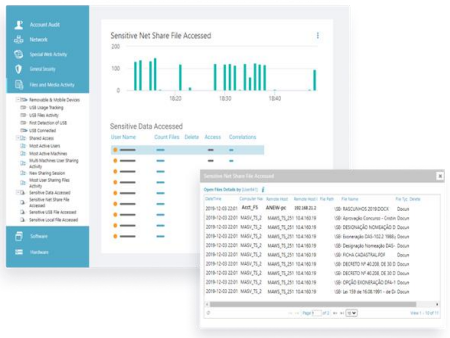
Reported Breaches



Average Cost per Breach



Rapid Root Cause Analysis



Identification and Containment

	Without OREV		With OREV
Root Cause Identification	**5-10 Days**	→	**2 Hours**
Breach Containment	**Up To 75 Days**	→	**2 Days**

OREV Platform:

OREV is a comprehensive, self-contained, cyber risk and threat detection platform with unparalleled data collection and analysis at the source that includes the ability to act, analyze and augment data with little or no latency across devices and the network.

"A cyber-resilient organization (CRO) is one in which the cybersecurity focus has little to do with traditional metrics and strategies and a great deal to do with preventing business damage (above all else) by means of resilience and recovery strategy."
-IBM, 2021

OREV can reduce and limit the length of Business Interruption

- Provides incident responders and security analysts the tools they need to embrace Breach Resilience.
- Enabled by broad distribution at all end points of OREV proprietary Intelligent Surveillance Technology (IST) data collection agents.
- Deep data collected by OREV's Intelligent Agent Technology allows instant breach identification with Root Cause Analysis (RCA) and Triage completed in about an hour or two.
- Identify and isolate malware-impacted devices and deactivate processes in minutes/hours readying them for immediate restoration from back-up.
- Alternative solutions require multiple tools and manual processes steps taking days, extending business disruption time and loss of revenue.

"It's also apparent that companies are still not prepared enough for breaches even though they are becoming more commonplace."
-Varonis, April 2021

Alan Porten, VP Sales and Business Development
AlanP@orevsn.com.com / (404) 422-2043
www.orevsn.com