

BUSINESS-CENTRIC MANAGED SECURITY SERVICES ONLY FROM INTELISECURE



Conventional MSSP offerings are no longer sufficient to protect critical assets

InteliSecure is the first and only Managed Security Service Provider (MSSP) to challenge the status quo in cybersecurity by delivering business-centric capabilities that surpass conventional MSSP's on several key attributes as illustrated here.

Conventional/Legacy Managed Security Services **VS.** Business-Centric Managed Security Services

TRADITIONAL

INTELISECURE



STATIC & REACTIVE

Static, reactive approach to monitoring security posture, often locked into legacy systems



BLANKET PERIMETER APPROACH

Programs designed as a "blanket perimeter"



ONE SIZE FITS ALL

Bucketed business model to minimize costs



ONE DIMENSIONAL

One dimensional perspective on threat defense typically focused on external threats



STANDARD CORRELATION

Collect bits and bytes from multiple point products



LIMITED VISIBILITY

No/limited visibility into how information moves through the organization



LIMITED ACCESS MANAGEMENT

No/limited point product privileged access management and change control



LIMITED CHANGE CAPABILITY & CONTROL

Only MSSP can make changes, and no way to fully prevent unauthorized changes



LITTLE OR NO FOLLOW-UP

Initial configuration with standard periodic updates, and only reactive configuration changes



FORMULAIC RESPONSE

Conventional, anonymous tiered support escalation layers

PROACTIVE & DYNAMIC

Proactive, dynamic systems and culture bringing together proven methodology, expertise, latest technologies and the human element in security



FOCUS ON CRITICAL ASSETS

Programs designed and focused around critical assets



CUSTOM-TAILORED

Customized execution tailored to each client's critical asset protection situation and needs



MULTI-DIMENSIONAL

Multi-dimensional visibility protects against both internal and external threats



SINGLE INTELLIGENT PLATFORM

Compound correlation from all security devices combined with behavioral analytics through single portal powered by the Enigma Intelligence Platform



GUIDED BY CONTENT & CONTEXT

Guided by policies defining the content and context of critical asset usage and users



SECURE ACCESS MANAGEMENT

Proprietary privileged access management to track user access and assure change management integrity



CUSTOMER CONTROL & FLEXIBILITY

Validation process to prevent unauthorized changes, while customers retain true co-management control and flexibility



CONTINUOUS IMPROVEMENT

Continuous improvement process for fine-tuning technologies guided by a dedicated Cyber Intelligence Team



ENGAGED INSIGHT & FORESIGHT

Dedicated Cyber Intelligence Team members utilize insights and knowledge gained from knowing their customer's information eco-system and technology infrastructure



LEARN MORE