Intrado
LIFE & SAFETY

Intuitus Managed Detection and Response Service Guide

Version 2021.01.27

Contents

1. Introduction 2
2. Services Overview 2
3. Services Details 2
3.1. Intuitus Managed Detection and Response (MDR) with Cyber SOC Services 2
3.1.1 Intuitus MDR Service Features: 3
3.1.2. Intuitus MDR Deliverables 3
3.2. Intuitus Endpoint Protection 4
3.3. Intuitus Secure Messaging 4
3.4. Intuitus Managed Network Firewall Service 4
4. Intuitus Cyber Security Operations Center 5
4.1. Disclaimers 5
5. Customer Obligations 5
5.1. Cooperation with Intrado and Intuitus 5
5.2. Data and Information 5
5.3. Equipment 6
5.4. Intuitus Appliance 6
5.5. Customer Security Program 6
5.6. Customer Incident Response and Remediation 6
5.7. Customer Contacts 6
5.8. Network Change Notification 7
6. Other Customer Obligations 7
7. Support 7
8. Services Limitations 7

1. Introduction

This Service Guide describes the different cybersecurity services offered by Cyber Business Analytics, Inc. d/b/a “Intuitus” and resold by Intrado Safety Solutions Corp. (“Intrado”), which are performed for end customers (each, a “Customer”), each as detailed more fully herein (collectively “Services”).

2. Services Overview

- **Intuitus Managed Detection and Response (“Intuitus MDR”)** is a cybersecurity and network situational awareness tool that monitors data within the Public Safety Answering Point (“PSAP”) networks and between those networks and external data sources. Intuitus MDR visualizes the traffic, and helps Customer protect its network. A full 24/7/365 cyber Security Operations Center (“SOC”) and weekly and monthly reports are included.
- **Intuitus Endpoint Protection (EPP)** is a lightweight cognitive agent with 24/7 monitoring, which learns the common activity patterns of your system to detect anomalies and uses machine learning algorithms to prevent new attacks before they can be launched. Intuitus EPP can identify and block attacks whether they are known or unknown, and file-based or file-less, all before execution.
- **Intuitus Secure Messaging** utilizes Secrata’s innovative patented enterprise security platform that chunks and encrypts data end-to-end, protecting and hardening security for cloud, mobile and Big Data. Its Enterprise File Sync and Share (EFSS) is a secure and high-performance way for an enterprise to move and manage files across content locations and devices.
- **Intuitus Managed Network Firewall Service** comes with the a high degree of attention to protect critical assets and provide protection at the network perimeter. Whether customers want a fully managed firewall solution where Intuitus experts modify security configurations as needed, or delegated administration where client technical staff maintains an active role in the administration of the firewall, Intuitus can provide expertise to stop constantly evolving threats before they get inside your network.

3. Services Details

3.1. Intuitus Managed Detection and Response (MDR) with Cyber SOC Services

Intuitus MDR provides network situational awareness using both signature and algorithmic network security and traffic anomaly detectors. It provides correlated cybersecurity features comparable to those found in other stand-alone competitive products. These include:

- Managed Service
- Protocol Analyzer
- SIEM (Security Information and Event Management)
- Intrusion Detection System (“IDS”)
- Security Analytics and Reporting
- Netflow Analyzer
- Cloud, IoT, and ICS Compatibility
- Packet Capture and Storage

Intuitus MDR identifies active and potential breaches as well as quickly detecting potential insider threats and acts of fraud. Intuitus MDR can provide forensic reconstruction of cybersecurity events. And, Intuitus MDR is a passive and cloaked system designed to be invisible to threat actors.

Intuitus MDR utilizes patent-pending cybersecurity appliances that monitor all IP-based traffic entering and leaving the PSAP or Emergency Call Center, thereby enabling the visualization of the PSAP network and the traffic flow between the PSAP and the outside world. As a result, Customers can be notified of traffic coming from or heading to potentially malicious Internet locations. This form of visualization and notification brings greater cyber situational awareness to appropriate PSAP personnel, so that the communication can be blocked or modified by Customer as appropriate. Intuitus MDR can detect polymorphic attacks, where the IP location of the attacker varies in random fashion, as well as detection of externally compromised sites which were previously considered to be safe. The Intuitus MDR installs on standard hardware and can be scaled from monitoring small single networks to large and complex interconnected webs of devices. Intuitus MDR works in conjunction with a defense-in-depth strategy and supplements existing cybersecurity measures.

3.1.1. Intuitus MDR Service Features:

- Cyber Security Operations Center (SOC) services that provide 24/7/365 security monitoring of both signature-based and anomaly-based threats.
- Assigned professional Cyber Defense Analyst team to detect, analyze, and report malicious network traffic in a timely manner.
- Easily understandable expert recommendations on how to mitigate risks to Customer’s network.
- Weekly and monthly cybersecurity reports that highlight trends and significant events.
- Forensic analysis support as required to remediate and/or mitigate future breaches.
- IDS tailored to each Customer’s unique network and safeguarding priorities via questionnaire and initial interviews.
- Continuous fine-tuning of the IDS.
- Installation and maintenance of sensor hardware.
- Continuous packet capture and storage (optional)
- Secure communication of all sensitive documents and reports
- Up to three end user accounts to Intuitus MDR
- User-based Intuitus MDR training
- Incident response and training
- Change management support

3.1.2. Intuitus MDR Deliverables

Intuitus will analyze the Customer’s network(s) and develop a plan that determines where Intuitus MDR security appliances should be located and configured, which will also determine the overall cost. Intuitus will install hardware appliances or will provide detailed instruction to install the appliances. Appliances will be serviced and maintained. Intuitus will set up user accounts and provide initial Intuitus MDR user training.

Secure messaging and file sharing accounts will be provided for secure communication. A cyber SOC with professional Cyber Defense Analysts will provide 24/7/365 monitoring to detect, analyze, and report malicious network traffic in a timely manner.

The IDS will be tailored to the Customer’s unique network and safeguarding priorities. Weekly and monthly cybersecurity reports will be sent which address alert highlights, reporting statistics, and trends. In addition, all other services and features listed under Intuitus MDR Service Features are provided.

3.2. Intuitus Endpoint Protection

Adding an endpoint protection (EPP) platform is critical when the network is accessed by remote devices like smartphones, laptops, tablets, or other wireless devices. An EPP platform protects devices outside the network firewall by installing advanced security software on those "endpoints". Intuitus Endpoint Protection enhances that protection by adding 24/7 monitoring. The 24/7 monitoring provides:

- Humans—not just software—observing and assessing alerts
- Action taken immediately after a threat is detected.
- Cybersecurity experts providing recommended changes to configuration settings to improve security
- EPP reporting: Know what your EPP is doing for you

Intuitus Endpoint Protection combines DeepArmor's best-in-breed EPP platform with 24/7 monitoring by Cyber Defense Analysts. DeepArmor's platform is built not just using AI, but entirely from AI. Its lightweight cognitive agent learns the common activity patterns of your system to detect anomalies and uses machine learning algorithms to prevent new attacks before they can be launched. Intuitus EPP can identify and block attacks whether they are known or unknown, and file-based or file-less, all before execution.

Intuitus Endpoint Protection is only offered in conjunction with Intuitus MDR.

3.3. Intuitus Secure Messaging

Intuitus Secure Messaging utilizes Secrata's innovative patented enterprise security platform that chunks and encrypts data end-to-end protecting and hardening security for cloud, mobile and Big Data. Its Enterprise File Sync and Share (EFSS) is the most secure and high-performance way for an enterprise to move and manage files across content locations and devices.

Use secure messaging to keep your organizations communication private. Especially in the event of a cyber incident, secure messaging keeps sensitive communication private until—or if—you choose to release it.

Three (3) Intuitus Secure Messaging Customer accounts come with Intuitus Managed Detection and Response to allow secure communication between the Customer and Intuitus. Additional Customer accounts can be added for a $200 annual fee.

Intuitus Secure Messaging is a great option if a Customer wants secure communication with their organization. The cost is less than you would expect.

Intuitus Secure Messaging is only offered in conjunction with Intuitus MDR.

3.4. Intuitus Managed Network Firewall Service

Managed firewalls protect your network from unauthorized access and malicious attacks. Firewalls are the critical gateway into a network, and firewalls managed by Intuitus come with the highest degree of attention and expertise to protect critical assets and provide protection at the perimeter. Intuitus Managed Network Firewall Service is available in two categories:

1) Managed Firewalls - A fully managed firewall solution, including policy and configuration. The service is tailored to meet the Customer's changing business requirements.

2) Delegated Administration - A solution for agencies that want their technical staff to maintain an active role in the administration of the agency perimeter firewall.

The Intuitus Managed Network Firewall Service provides Customers with a monitored and administered firewall. The service provides a firewall management solution to stop constantly evolving threats at the edge of your network. This allows Intuitus to make recommendations and take action at a much faster rate.

Intuitus Managed Network Firewall Service is only offered in conjunction with Intuitus MDR.

4. Intuitus Cyber Security Operations Center

Intuitus Services are operated out of a cyber Security Operations Center (SOC) that supports Customers 24/7/365. The Intuitus cyber SOC is staffed by expert Cyber Defense Analysts and other cybersecurity experts, and provides both security monitoring and network monitoring. More information about the Intuitus cyber SOC, such as: how risk is quantified, how the alert Risk Levels are defined, and notification procedures, is available to Customers.

4.1. Disclaimers

- Customer recognizes its own responsibilities herein with respect to its cybersecurity program. Customer acknowledges that it must participate in its own defense and work with Intuitus to create a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to establish an ongoing process to identify, assess, and manage cyber risk throughout Customer’s network.
- Customer acknowledges that Intuitus MDR is not intended nor designed to prevent unauthorized access to or activities involving Customer’s network(s) or to any computers, equipment, or data which constitute or are accessible through Customer’s network(s), and that neither Intuitus nor Intrado is responsible for Customer’s use of or response to alerts or reports from the Intuitus MDR and services, unless and only to the extent Intrado may expressly assume such responsibility in providing additional services under a service order.
- Neither Intuitus nor Intrado makes any guarantees regarding the effectiveness of its Services with respect to overall cybersecurity program, due to lack of control over numerous aspects of Customer’s operations, personnel, and information systems.
- Additional services, such as cybersecurity consulting services, are separately available from Intrado.

5. Customer Obligations

5.1. Cooperation with Intrado and Intuitus

Customer will cooperate and assist Intrado and Intuitus as reasonably necessary regarding installation and maintenance of the Intuitus Services, including but not limited to (a) the review and acceptance of the Order and any schedules or other documentation applicable to the Order; (b) if Customer elects additional services, the review and acceptance of the Order and any other documentation applicable to the Order; (c) the prompt communication of any questions or issues potentially affecting or pertaining to performance of the Intuitus Services to Intrado; and (d) prompt response to Intrado queries and requests on issues and matters pertaining to the Intuitus Services and other matters arising under this Service Guide.

5.2. Data and Information

Customer will make available in a timely manner at no charge to Intrado and Intuitus all technical data, computer facilities, programs, files, documentation, test data, sample output, or other information and resources reasonably required by Intrado or Intuitus for the implementation and provisioning of the Intuitus Services. Customer will be responsible for ensuring the correctness, accuracy, and completeness of all data, materials, and information supplied by Customer.

5.3. Equipment

Customer will provide access to equipment, network connectivity, personnel and Customer expertise and institutional knowledge required by Intrado or Intuitus for the implementation and provisioning of the Intuitus Services.

5.4. Intuitus Appliance

Intuitus Appliances are the physical hardware that allows cyber threats to be detected. Intuitus Appliances include: Secure Utility Server (SUS), Forensic Data Collector (FDC), and OneBox. Customer acknowledges that any Intuitus Appliance located at Customer's facilities is the property of Intuitus. Customer will provide and maintain a secure environment at its facilities for the Intuitus Appliance(s), including safeguards to prevent unauthorized physical access and ensure protection against fire and other disasters. Customer will ensure that the Intuitus Appliance(s) have reliable power, reliable connectivity to the network(s) to be monitored, and reliable connectivity to the Internet, and will notify Intrado reasonably in advance of any planned outages affecting power or connectivity of the Intuitus Appliance(s). Customer will permit Intuitus as the delivery agent, to inspect the Intuitus Appliance(s) during ordinary business hours upon reasonable prior notice.

Appliance(s) must be returned to Intuitus within 14 days of the end of service term. End of service may be the end of the service term, end of a trial or pilot period, or other reason for termination. Appliance(s) can be mailed to Intuitus offices.

5.5. Customer Security Program

Customer acknowledges that it will provide the following controls, tools and processes to directly support the Intuitus Services, and that failure to do so may impact Intuitus's ability to perform the Services effectively:

- A written governance, risk and compliance (GRC) policy or policies, approved by a Senior Officer or equivalent, setting forth Customer's policies and procedures for the protection of its information systems and nonpublic information stored on those information systems (aka "Cybersecurity Policy");
- A written Incident Response Action Plan that is exercised and/or practiced with key scenario driven evaluations (i.e., tabletop exercises) on at least an annual basis;
- Designate two or more employees, executives, or agents who will respond to any security alerts and take recommended actions to mitigate harm to Customer's network; and,
- Although not required, it is recommended that each Customer conducts a periodic risk and vulnerability assessment to address changes to information systems, nonpublic information, and/or business operations. The risk and vulnerability assessment should allow for revision of controls to respond to technological developments and evolving threats.

5.6. Customer Incident Response and Remediation

Customer will be responsible for determining and undertaking or arranging for the undertaking of any action(s) in response to a security alert or report from Intrado, unless Intrado has expressly agreed to do so as an additional service under an Order.

5.7. Customer Contacts

Customer will appoint in writing a primary and alternate technical-level employee or agent to act as the primary contact person for all technical communication between the Customer and Intuitus related to the Services. Customer will also designate a managerial-level contact person. These contact persons will be responsible for monitoring the status of the Services, respond to any security alerts, take recommended actions to mitigate harm to Customer's network, receive cybersecurity reports, and will confer with Intuitus as needed.

5.8. Network Change Notification

Customer will immediately inform Intuitus and Intrado of any physical change to the Customer network.

6. Other Customer Obligations

Customer will be solely responsible for ensuring that it is not subject to contractual obligations materially affecting the implementation or use of the Intuitus Services.

7. Support

Customer may contact the Intuitus SOC at:

- Help Desk Number: 253-514-5695
- Email Support: cybersupport@intuituscyber.com
- Hours: 24x7

8. Services Limitations

The following Services limitations and disclaimers apply:

- Services provide information to Customer to enable Customer to better assess security threats and take appropriate action. Services do not actively protect Customer's network or information from intrusion or cyberattack.
- Intuitus is the sole provider of Services; Intrado is acting as a reseller only.
- Customer may contact Intrado or Intuitus for support for any issues with Services.
- For Intuitus MDR, Customer must:
  - Maintain Internet connectivity to enable remote monitoring; and
  - Open ports and/or allow Intuitus to install necessary equipment that enables Intuitus MDR to inspect IP traffic passing through Customer's network.
- Customer agrees to review with Intuitus the Customer's architecture, including any and all changes to the architecture that may affect performance of the Services.
- A 6-week period is required to baseline network traffic, during which time the system is under full operational monitoring.