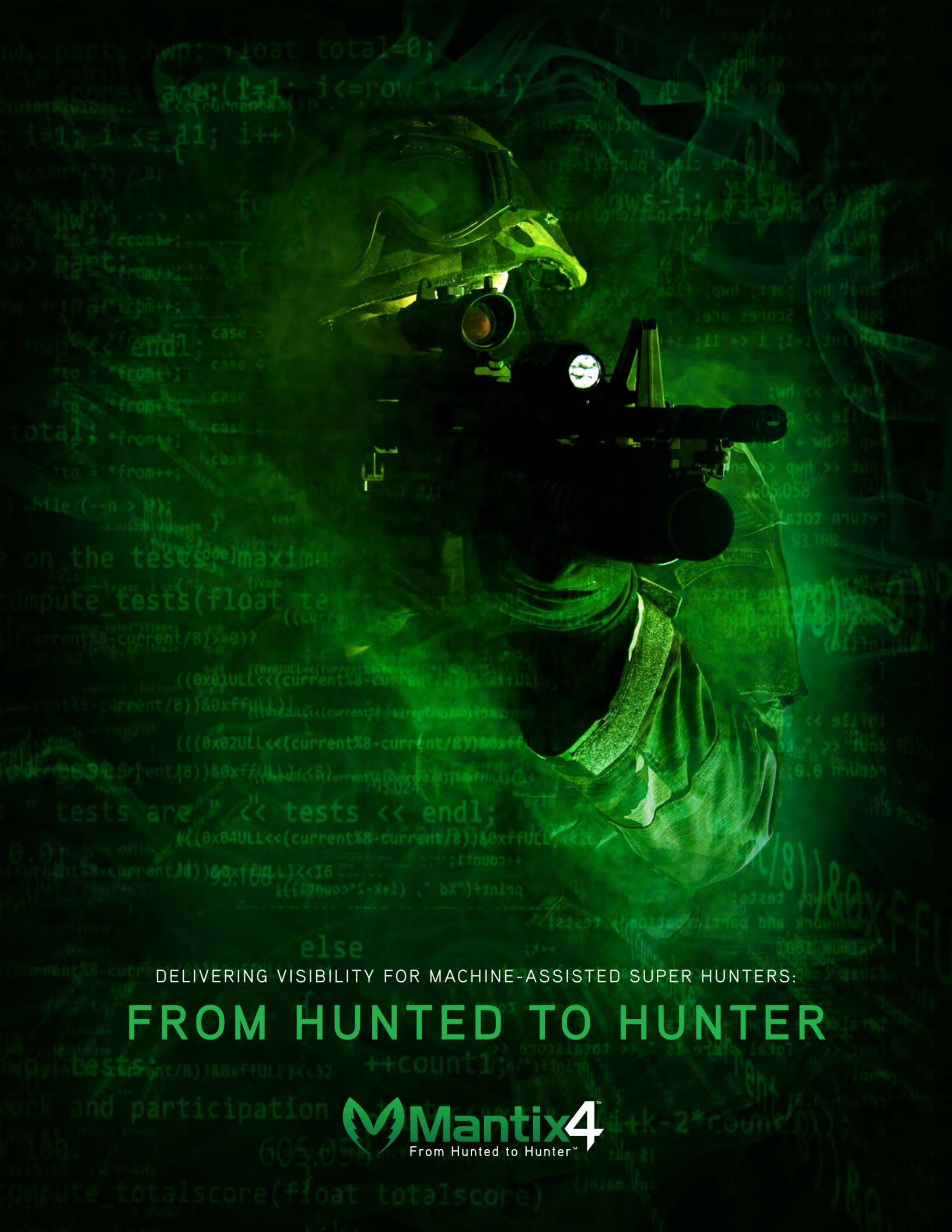

DELIVERING VISIBILITY FOR MACHINE-ASSISTED SUPER HUNTERS:

FROM HUNTED TO HUNTER

Mantix4™

From Hunted to Hunter™

THREE REQUIREMENTS FOR EFFECTIVE CYBER HUNTING

In order to effectively address and respond to the current cyber security threat environment, organizations need to: adopt a proactive security stance that focuses on improving visibility across devices, applications and people; focus on maintaining human-orchestrated responses to human-produced attacks; and apply technology wisely.

1. Visibility is the key to stopping advanced threats. Cyber criminals enter networks and follow an inevitable plan to get what they want. Those actions, known as the cyber kill chain, include things such as penetrating perimeter defenses, delivering payload, executing command + control, mapping domains, accessing additional end-points, escalating privileges, and ultimately exfiltrating, deleting or holding an organization's data hostage. Most of these activities are identical to a normal business user — the difference is authorization and intent. If an organization cannot see devices, applications and people engaged in these behaviors, the organization has zero chance of stopping cyber criminals.

2. Human orchestration is the norm within law enforcement, sports and other scenarios in which the opponent is creative, ambitious and evolving. While some cybersecurity professionals might daydream about automated and analytic-driven boxes being ready to replace people, it's nothing but a fantasy today. Nobody seriously believes the FBI or CIA don't need agents. Could you imagine your favorite sports team replacing their coaching staff with a computer? Would you hire a computer to defend you in court? Of course not.

373 INVERNESS PARKWAY, SUITE 110, ENGLEWOOD, CO | TEL: 877-MANTIX4 | WWW.MANTIX4.COM | INFO@MANTIX4.COM

As was reported in CSO Online:

"Threat Hunting is an offensive posture and a culture that unites man and machine to go on search-and-destroy missions. It is not even a new strategy. Over time we came to rely on technology alone for detection, now we need to evolve. We must bring back the human element, the hunters – real people doing the spy work and scouring systems to find malicious code or a piece of malware that technology alone has failed to detect."

Human criminals and human cybersecurity professionals are matched in a contest that has few rules, no clock and is very unstructured. Criminals are on offense, moving around the cyber kill chain. Cybersecurity professionals use tools to slow them down and make them stand out.

It is safe to assume that criminals will get though the perimeter defenses and into the network. The real goal is to prevent breaches from developing into a full-blown attack causing damage to the business by exfiltrating, deleting or holding an organization's data hostage. Once in the network, the majority of a cyber criminals' activities are identical to a normal business user, subtle differences stand out to human threat hunters. It's human intuition and interpretation of data that spots criminals and shuts them down.

3. Arming cyber threat hunters with the very best technology makes them exceptional. Today, criminals have most of the advantages. They are well financed, don't fear existing legal consequences, are anonymous, have infinite targets to strike, and are highly motivated. Mantix4 turns the tables and makes the hunter the hunted.

Once criminals are inside the network they encounter Mantix4 threat hunters armed with a platform powered by a computer's brute-force ability to memorize and predict moves through the cyber kill chain in advance. Machines perform the laborious processes of automated and analytic data collection, filtering, and sorting. Cyber threat hunters have access to the complete data set methodically organized and operationally efficient. Reactive security products inefficiently use technology to flag enormous numbers of events and produce more alarms, alerts and logs than any organization can process. This overwhelming flood of data causes what is known as alarm-fatigue. Mantix4, on the other hand, uses technology wisely and produces cyber threat hunters that systematically hunt down criminals by identifying behavior consistent with criminal intent.

No longer is it a head-to-head battle between cyber criminals and cyber professionals. Now, its cyber criminals versus machine-assisted super cyber threat hunters.
Game over.

Human-orchestrated, machine-assisted professionals efficiently hunting with comprehensive visibility across all the devices, applications and people that make up the network is the key to turning the hunted into the hunter.

WHY HUNTING WORKS

The Mantix4 Cyber Threat Hunting Platform works by recognizing the "what and how" of cyber attacks and targeting post-breach engagement. At the highest level, Mantix4 combines advanced network traffic analytics and endpoint forensic investigation. Automated Outlier Detection, including scripted hunts for Tunnel Detection, Command & Control, Suspicious Hosts and Statistical Analysis, combined with Human Hunt, Threat Intelligence Detection, Behavioral Analysis, Machine Learning and Forensic Confirmation exposes an adversary as they attempt to infiltrate, expand, and ultimately achieve their primary objective.

Mantix4 contains a collection of threat hunting tools and techniques that incorporate artificial intelligence, automation, machine learning and human intuition.

HH – Human Hunt: Human-orchestrated is the norm in law enforcement, sports and other scenarios in which the opponent is creative, ambitious and evolving. While some cybersecurity professionals might daydream about fully automated and analytic-driven boxes being ready to replace people it's nothing but a fantasy.

TI – Threat Intelligence Detection: In order to provide context, inform better decision-making, and enable improved detection of advanced threats the platform unites a collection of intelligence using open source intelligence, social media sources, human intelligence, technical intelligence and intelligence from the deep and dark web. The platform automatically confirms threat intelligence matches in the IP session artifact list (e.g. IP address, Domain, URL/URI, Filename, File Hash, Geographic location).

BA – Behavioral Analysis: Mantix4 incorporates specific behavioral analysis. Attackers utilize the Server Message Block (SMB) protocol to blend in with network activity, often carrying out their objectives undetected. Post-compromise, attackers use file shares to move laterally, looking for sensitive or confidential data to exfiltrate out of a network. Spotting behaviorally significant activity through custom scripts and log data facilitates rapid detection. Specific weighted activaties include port scan, password guessing, SQL injection attempts, SMB Named-Pipe Detection.

OD – Outlier Detection: Automation dramatically reduces the need for human intervention in the initial suspicious activity collection process. Key network traffic metrics are grouped, quantified and measured to determine if there are outliers within a data-set. There are seventeen critical inquiries essential for identifying post-breach malicious activity are integrated into the Mantix4 platform as automated hunts. Outlier Detection is identified within a 24 hour time slice of data. Based on experience and training,

Mantix4 provides specific hunting methods designed to block the techniques and procedures Cyber Criminals use at each stage of the Post-Breach Cyber Kill Chain.

The techniques and procedures are a sample of those found in the MITRE™ ATT&CK Matrix. Many techniques and procedures can be found at multiple stages of an attack

POST-BREACH CYBER KILL CHAIN

COMMAND + CONTROL

Command & Control:
- Uncommon Ports
- Standard App Protocol
- Custom Protocol
- Beaconing

Tunneling:
- DNS
- HTTP
- HTTPS

Domain Stacking:
- Sub Domain
- Top Level Domain

MAP DOMAIN

Credential Access:
- Brute Force
- NBT-NS Poisoning

Discovery:
- Network Service Scanning
- Network Share Discovery
- Remote System Discovery

Credential Access:
- Hooking
- Network Sning

LATERAL MOVEMENT

Lateral Movement:
- Remote Desktop Protocol
- Exploitation of Remote Services
- Windows Admin Shares

Discovery:
- Account Discovery
- Permission Group Discovery

ESCALATE PRIVILEGES

Privilege Escalation:
- Application Shimming
- DLL Hijacking
- Memory Injection

Persistence:
- Hooking
- Local Job Scheduling
- AppCert DLLs

Defensive Evasion:
- Code Signing
- DLL Search Order Hijacking
- Binary Padding

ACT ON OBJECTIVE

Collection:
- Screen Capture
- Video Capture
- Data from Local System

Exfiltration:
- Over Alternate Protocol
- Over Command & Control
- Data Transfer Size Limits

Mantix4™
From Hunted to Hunter™

The Mantix4 Cyber Threat Hunting Platform combines advanced network traffic analytics and endpoint forensic investigation to expose adversaries as they attempt to infiltrate, expand and ultimately achieve their malicious objectives.

- Automated Outlier Detection including scripted hunts for Tunnel Detection, Command & Control, Suspicious Hosts, and Statistical Analysis
- Human Hunt
- Threat Intelligence Detection
- Behavioral Analytics
- Machine Learning
- Forensic Confirmation

the analyst will deploy some or all of the scripted hunts, which include:

1. Tunnel Detection
a. Long Duration Conns
b. DNS Exfil (UDP Tunnels)
c. DNS Tunnel (Iodine-1)
d. DNS Tunnel (Iodine-2)

2. Command & Control
a. Subdomains Stacking
b. Large HTTP Responses
c. HTTP Beacons
d. DNS Beacons

3. Suspicious Hosts
a. Kaminsky DNS Attack
b. Failed SSL Certificates
c. Top Internal Producers
d. Non-Standard HTTP
e. User-Agents (HTTP)

4. Statistics
a. Top Responder Ports
b. Top Referred Hosts
c. Most Popular Sites
d. Services Breakdown

ML – Machine Learning: The Mantix4 platform automates the process of grouping Network Communication protocol payload ratios into host-protocol pairings and measures over varying time slices (e.g. 5 min, 15 min, 1 hr, 4 hr, 12 hr, 24 hr, 1 week, 1 month) to assess the variance from "normal", looking for anomalous hosts / communications in the network.

FC – Forensic Confirmation: Suspicious user devices and servers will be further triaged with a Forensic State Analysis in two ways. Scans will be run on a regularly scheduled proactive basis and in response to a specific end point that is determined to be exhibiting suspicious network behavior. Forensic State Analysis examines the running binaries inside the host, along with other indicators of compromise including: persistence mechanisms, obfuscated / high-entropy code, dynamic analysis, etc. The Forensic Confirmation uses dissolvable agents to independently collect, identify and evaluate a variety of data (active processes, in-memory executable codes, auto-runs, execution artifacts, OS subversion, API hooks, abnormal configurations, disabled controls and more), then analyzes the data using forensic analytics and file intelligence services. Finally, the process analyzes OS and application persistence mechanisms – which can trigger the execution of code or executables. Forensic Confirmation pinpoints malware and persistent threats, active or dormant, that have successfully breached existing defenses.

373 INVERNESS PARKWAY, SUITE 110, ENGLEWOOD, CO | TEL: 877-MANTIX4 | WWW.MANTIX4.COM | INFO@MANTIX4.COM

EVOLVING FROM HUNTED TO HUNTER: A CASE STUDY IN IDENTIFYING MALICIOUS LATERAL MOVEMENT

Successful cyber criminals evade traditional reactive technology as they progress through the cyber kill chain stages. According to Cybersecurity Insiders, 39% of emerging and advanced threats are missed by traditional security tools. No matter how the breach occurs, once malware has been downloaded, the next step for a cyber criminal is to expand the attack beyond a single machine. In order to achieve this, cyber criminals first map the network and begin moving laterally.

Distinguishing malicious exchanges of data between two end-points in a traditional business network from ordinary interactions required to run a business is particularly difficult for reactive technologies such as SIEMs, next-generation firewalls and network intrusion detection systems. Cyber criminals' activities simply blend in and disappear in the traffic. In other words, they look like everyone else in the network.

Mantix4, focuses on exposing the techniques and procedures that an adversary must use as they infiltrate, expand, and ultimately achieve their primary objectives.

STEP 1 - ANALYTICS

Driven concentration on essential data. Mantix4 has developed a catalogue of specific automated threat hunting tasks including many that target malicious lateral movement. Unlike reactive technologies, the Mantix4 process pieces together the evidence by collecting discrete events to provide a complete picture.

Examples of automated threat hunts include:

1. Tunnel Detection
2. Command & Control Discovery
3. Suspicious Hosts Examination
4. Statistical Anomoly Observation

STEP 2 - VISIBILITY

Assisted collection of corresponding evidence. Mantix4 threat hunters have access to the complete data set. In some circumstances, after reviewing the results of the automated tasks, threat hunters will examine corresponding evidence to complete a more comprehensive description of the malicious activity. This could be to support a targeted response or to isolate and secure malware that has spread quickly to multiple end-points

STEP 3 - FORENSIC CONFIRMATION

Suspicious user devices and servers will be further triaged with a Forensic State Analysis in two ways. Scans will be run on a regularly scheduled proactive basis and in response to a specific end point that is determined to be exhibiting suspicious network behavior. Forensic State Analysis examines the running binaries inside the host, along with other indicators of compromise including: persistence mechanisms, obfuscated / high-entropy code, dynamic analysis, etc. The Forensic Confirmation uses dissolvable agents to independently collect, identify and evaluate a variety of data (active processes, in-memory executable codes, auto-runs, execution artifacts, OS subversion, API hooks, abnormal configurations, disabled controls and more), then analyzes the data using forensic analytics and file intelligence services. Finally, the process analyzes OS and application persistence mechanisms – which can trigger the execution of code or executables. Forensic Confirmation pinpoints malware and persistent threats, active or dormant, that have successfully breached existing defenses.

STEP 4 - HUMAN-ORCHESTRATED RESPONSE

Once the analysis is completed and the malicious lateral movement identified and clarified, human threat hunters can apply experience and intuition to take control of the situation. Immediate remediation may be the right response, or a threat hunter may choose to recommend baiting his opponent into exposing vital details by allowing the malware to persist. Having moved from the hunted to the hunter, the timing of the response is entirely in the hands of the threat hunter.

While reactive technologies struggle to identify and understand malicious lateral movement within networks, Mantix4 provides the necessary blend of visibility and technology to allow successful human-orchestrated responses.

WHAT OUR CUSTOMERS ARE SAYING

"Other technologies simply look at the blinking boxes that flood me with alarms and logs. M4 proactively hunts threats from devices, applications and people. That makes a lot more sense to me."

– CSO North America Tier III Data Center

"Mantix4 creates a powerful visual interface allowing users to interpret large amounts of data in a short period of time, enabling companies to do their own threat hunting with minimal training."

- Head of Cyber Security for Global Consulting Partner

"I've marveled at this product from the beginning. The ability to interrogate your network and identify t ruly what is happening, in a short period of time (Hours) and perform threat hunting live, is awesome! Not to mention the intelligence feed they've put into their eco-system is the best I've seen to date!"

- CISO, VP Client Strategy

"Every other tool needs weeks of data before they can tell me where the problems are. M4 installed in under an hour and started highlighting potential issues that needed immediate attention on day one."

- CSO, International Beverage Company

THE CHANNEL CO. CRN EMERGING VENDORS 2018

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2018

CALL 877-MANTIX4 OR EMAIL INFO@MANTIX4.COM TO GET STARTED.

373 INVERNESS PARKWAY, SUITE 110, ENGLEWOOD, CO | TEL: 877-MANTIX4 | WWW.MANTIX4.COM | INFO@MANTIX4.COM