SOLUTION BRIEF

# Digital Defense, Inc. and Attivo Launch A Breakthrough Integrated Risk and Threat-Based Deception Solution

Introducing an Innovative Integration that Optimizes Protection and Threat Detection for Business Critical and Unpatchable Assets Using Deception Technology.

## BUSINESS PROBLEM

For years, attackers have successfully exploited different types of vulnerabilities, compromised systems and used deception tactics for breaching networks. They take advantage of infrastructure blind spots and unpatched and un-patchable systems like IoT devices and Industrial Control Systems (ICS) and then use these systems as a jumping point to masquerade as legitimate employees, using stolen credentials and deceptive measures to further infiltrate a network, all while remaining undetected for lengthy dwell times. Security teams have been challenged with identifying and tracking dynamically changing assets, understanding risk in real-time and prioritizing patching efforts, while Digital Defense provides the solution to help security teams address these challenges, it is now time to turn the tables on attackers and combine defensive and offensive approaches adding deception against them.

Marrying the knowledge of where your most critical assets reside and which ones are most susceptible to attack in real-time, with deception, enables security teams go on the offensive and deceive and misdirect an attacker away from their crown jewels in today's dynamic and ever-changing networks. Even better is that security teams can eliminate all the noise from traditional threat detection methods including false positive alert fatigue to know exactly what is under attack as attackers show their hand.

## DIGITAL DEFENSE FRONTLINE.CLOUD™

Digital Defense's **Frontline.Cloud** platform has been purpose-built to be deployed and operate in today's hybrid cloud enterprise environments. Frontline. Cloud, is hosted on Amazon Web Services (AWS) and incorporates Digital Defense's patented and proprietary technology that supports multiple software security systems focused on pro-actively protecting business critical assets. The Frontline.Cloud Software as a Service (SaaS) platform supports Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Threat Sweep™ (Frontline ATS™) leveraging multiple patents that eliminate the deficiencies in similar solutions that are also traditionally based on hardware appliances. Frontline.Cloud is the only solution in the market that can scale to operate on premise, in the cloud or in hybrid network-based implementations to fit the needs of organizations of any size, including even the largest financial, government, healthcare, retail and utility providers in the world.

SCAN
Quickly, comprehensively and accurately assess your network for vulnerabilities.

ANALYZE
Identify which assets are at risk and receive actionable intelligence.

SCORE
Benefit from a clear, easy-to-understand metric to determine your organization's security posture.

AUTOMATE
Seamlessly integrate Frontline vulnerability finding into my security workflow.

## ATTIVO BOTSINK SOLUTION

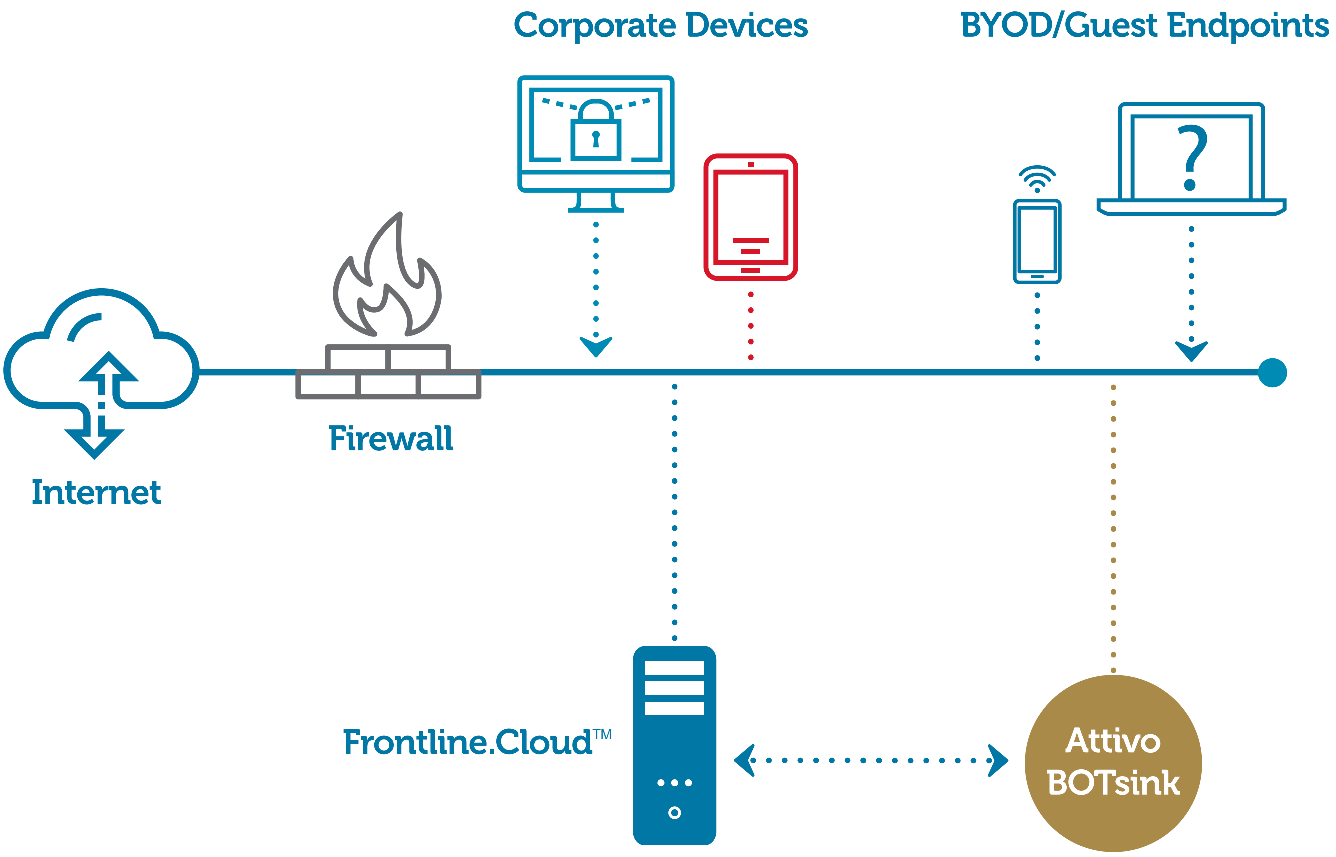
Using dynamic deception techniques and a matrix of distributed decoy systems, the entire network becomes a trap designed to deceive attackers and their automated tools. As an early warning system for in-network threats, the **Attivo Networks BOTsink** solution quickly and accurately detects threats that have bypassed other security controls. The solution efficiently detects attacker reconnaissance and lateral movement without relying on known attack patterns or signatures. Working with Digital Defense Frontline. Cloud, the Attivo deception technology projects decoys that appear indistinguishable from real production assets and are designed to engage and misdirect an attacker based on vulnerability and threat risk posture. For authenticity, decoys run real operating systems and services and can be customized with production "golden images" to better blend in with other network assets. Out-of-the-box decoy deception campaigns cover a wide variety of attack surfaces and include configurations for identical appearance to production servers, endpoints, industrial control systems, IoT devices, point-of-sale units, network infrastructure and VOIP systems. The solution creates a deception "hall of mirrors" for the adversary and when combined with application, data, database, and endpoint deceptions is able to detect attacks from all attack vectors early in the attack cycle. Once an attacker engages, the Attack Threat Analysis (ATA) engine analyzes their movement, methods, and actions, generating high-fidelity alerts and visual maps containing a time-lapsed attack replay. Security operations teams will gain the adversary intelligence they need to fully understand the attack and for root cause analysis.

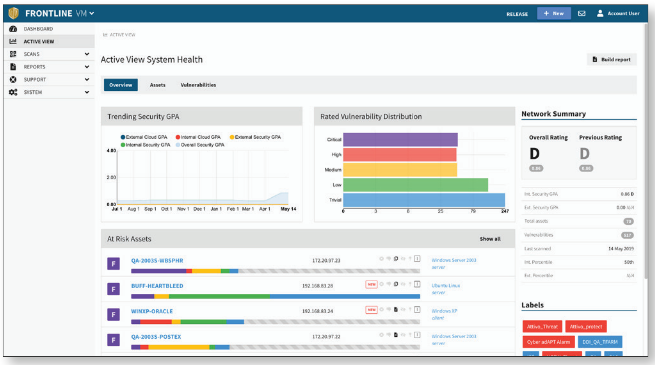
## SOLUTION SUMMARY

Digital Defense's Frontline.Cloud vulnerability management and threat assessment platform identifies high-risk/critical assets with business context that are highly vulnerable to exploits, remain unpatched, are un-patchable or have already been infected in real-time. Integrated with BOTsink, administrators can make intelligent, potentially automated, decisions on where to dynamically deploy deception technology to protect the network and resources from a potential compromise or attack, even as conditions or the infrastructure itself changes.

A significant security capability for ICS networks and critical infrastructure is drawing attackers away from these systems and detecting how they are trying to exploit vulnerabilities. This is especially true in these environments where it is often a challenge to patch systems due to limited access and minimal maintenance windows or in many cases no patch for a known vulnerability is even available.

## FRONTLINE.CLOUD/ATTIVO NETWORKS BOTSINK SOLUTION INTEGRATION





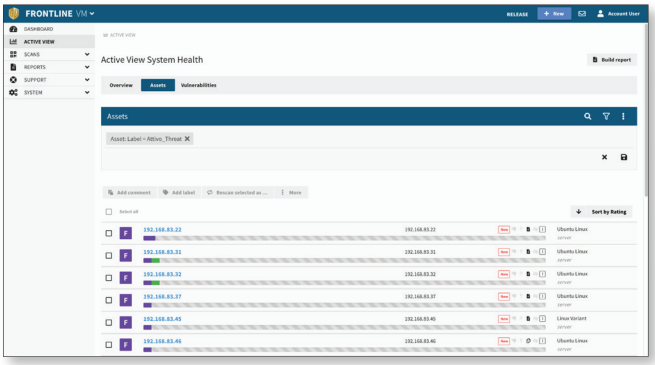
Network Summary

| Overall Rating | Previous Rating |
|---|---|
| D | D |
| 0.86 | 0.86 |

| | |
|---|---|
| Int. Security GPA | 0.86 D |
| Ext. Security GPA | 0.00 N/A |
| Total assets | 70 |
| Vulnerabilities | 517 |
| Last scanned | 14 May 2019 |
| Int. Percentile | 50th |
| Ext. Percentile | N/A |

At Risk Assets

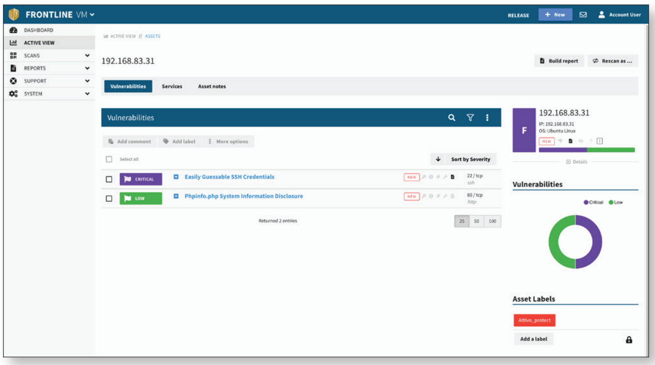
| | | | |
|---|---|---|---|
| F | QA-2003S-WBSPHR | 172.20.97.23 | Windows Server 2003<br>server |
| F | BUFF-HEARTBLEED | 192.168.83.28 | Ubuntu Linux<br>server |
| F | WINXP-ORACLE | 192.168.83.24 | Windows XP<br>client |
| F | QA-2003S-POSTEX | 172.20.97.22 | Windows Server 2003<br>server |



Assets

Asset: Label = Attivo_Threat

| | | | | |
|---|---|---|---|---|
| □ | F | 192.168.83.22 | 192.168.83.22 | Ubuntu Linux<br>server |
| □ | F | 192.168.83.31 | 192.168.83.31 | Ubuntu Linux<br>server |
| □ | F | 192.168.83.32 | 192.168.83.32 | Ubuntu Linux<br>server |
| □ | F | 192.168.83.37 | 192.168.83.37 | Ubuntu Linux<br>server |
| □ | F | 192.168.83.45 | 192.168.83.45 | Linux Variant<br>server |
| □ | F | 192.168.83.46 | 192.168.83.46 | Ubuntu Linux<br>server |



192.168.83.31

Vulnerabilities

| | | | |
|---|---|---|---|
| □ | CRITICAL | Easily Guessable SSH Credentials | 22 / tcp<br>ssh |
| □ | LOW | Phpinfo.php System Information Disclosure | 80 / tcp<br>http |

Returned 2 entries

F 192.168.83.31
IP: 192.168.83.31
OS: Ubuntu Linux

Vulnerabilities

## SOLUTION DESCRIPTION

***Combine Vulnerability Risk with Threat Data*** Digital Defense's Frontline.Cloud digitally fingerprints the hosts as contiguous entities, reconciles asset changes from scan to scan utilizing patented correlation algorithms (helping to minimize duplicates or unknown devices), prioritizes vulnerabilities, and automates workflow across the hybrid network to make better risk management decisions, quickly. Frontline.Cloud then consumes detected threat information from BOTsink to understand and convey which assets are at immediate risk.

### *Optimize Real-Time Deployment of Deception*

Attivo BOTsink is already optimized to self-learn where to deploy deception campaigns. However, to take the guesswork out of where the most business critical assets need protecting and which of those are most at risk, Attivo works with Digital Defense Frontline.Cloud for dynamically adjusting deception campaigns to better protect the most important systems. Frontline.Cloud provides the only on-demand real-time risk and threat assessment platform in the market today. As we add threat intelligence from BOTsink, we can determine the most business critical at-risk assets and deploy or re-deploy deception decoys even as assets may move or change. With the combined solution, we can more effectively make sure attackers are drawn away from the crown jewels and provide security operations teams with critical asset, threat and attack activity to respond more quickly and effectively.

## LEARN MORE

To learn more about the advantages of the Digital Defense, Inc. Frontline.Cloud platform with Attivo BOTsink solution:

Sales can be reached at: sales@digitaldefense.com

Technical support questions can be directed to: integrations@digitaldefense.com

## About Digital Defense, Inc.

Founded in 1999, Digital Defense, Inc. is an industry recognized provider of security assessment solutions. Digital Defense provides vulnerability and threat assessment Software-as-a-Service (SaaS) solutions and services purpose-built to operate in today's hybrid cloud enterprise environments. Digital Defense's proprietary platform, Frontline.Cloud, incorporates patented technologies and offers multiple software security systems focused on pro-actively hardening business critical assets from being compromised and breached. The Frontline.Cloud platform supports Frontline Vulnerability Manager™ (Frontline VM™), Frontline Web Application Scanning™ (Frontline WAS™), and Frontline Active Threat Sweep™ (Frontline ATS™) that provide agent-less discovery, vulnerability and threat assessment of dynamic assets, while eliminating manual processes and integrating with market-leading 3rd party security and IT offerings to eliminate gaps in visibility and enable faster remediation. Frontline.Cloud is the only solution in the market that is built to be scaled across any size organization and operate on premise, in the cloud or in hybrid network-based implementations.

## About Attivo Networks®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide-variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations that automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. www.attivonetworks.com