WHITEPAPER

ATTIVO NETWORKS DECEPTION TECHNOLOGY FOR MERGERS AND ACQUISITIONS

INTRODUCTION

Mergers & Acquisitions (M&A) are undertaken for a variety of strategic reasons that aim for greater synergy, diversification, improvements to an organization's overall capabilities, and growth. The ROI of these unions heavily depends on how quickly the companies can integrate their organizational components, operational environments, infrastructure, and technologies. The longer these activities take, the higher the acquisition costs and the longer it takes to benefit from the union. Concerns about cybersecurity have become a critical issue for companies considering a merger or acquisition, and a potential acquisition's cybersecurity infrastructure, or lack thereof, can affect the deal price and may even determine whether the deal happens at all.

Combining technology infrastructures can be a complex process. Merging organizations often brings challenges in overlapping and disparate technologies, process misalignment, and differing levels of maturity. The most efficient integration strategies rely on fast and accurate due diligence, letting the organization quickly settle on an integration plan that meets the challenges they've identified.

Announcing a merger or acquisition raises the visibility and profile of both organizations. This increased profile can make both entities more attractive to potential attackers and raises the danger from any persistent threats that may already exist. In Testing the Defenses: Cybersecurity Due Diligence in M&A , West Monroe Partners reported that 40% of acquirers discovered a cybersecurity problem after a deal went through.

Organizations involved in a merger must assess the security integrity, maturity, and current state of the newly acquired entity's network and infrastructure in the context of today's dynamic threat landscape. This drives a need for tools that can rapidly establish visibility into the environment and the means to ascertain the risks and vulnerabilities that may exist related to:

- The state of current security controls and processes
- Identifying potentially active compromises and vulnerabilities that may exist
- Gathering intelligence and understanding the current infrastructure across cloud, data center, end user networks, and even into operational networks like SCADA/ICS/IoT/ POS networks.

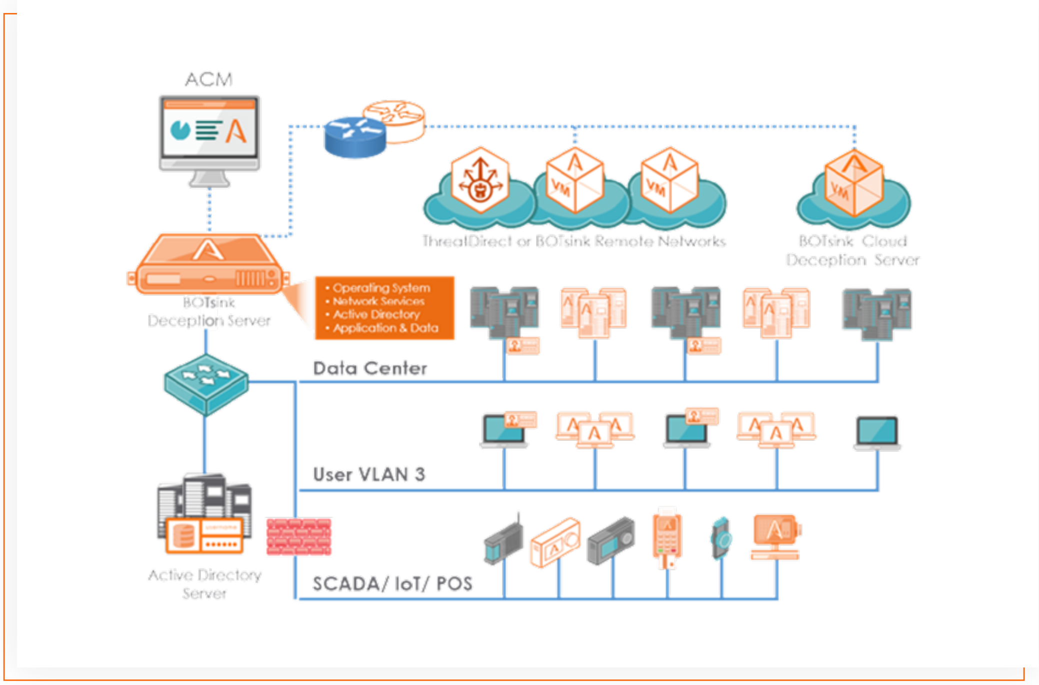
> Deception technology can play a critical role in Mergers and Acquisition situations, providing vital detection and visibility capabilities for due diligence and post-merger integrations.

These discovery elements can be used as due diligence to develop a strategy to address identified deficiencies, aid in reducing risks, and elevate the security posture of the merged environment. An effective assessment, and the development of a remediation plan, ensure that the technological integration doesn't result in 'poisoning the well' and that the acquisition initiatives aren't jeopardized or impeded. However, conventional assessment techniques and technologies, such as audits, penetration tests, intrusion detection systems, etc., may not be enough.

The Attivo Networks® ThreatDefend™ Deception and Response Platform provides a unique solution, based on deception, to detect and defend against human and automated attackers that have successfully bypassed existing perimeter defenses. The solution is delivered through a range of deceptive assets distributed across the network and endpoints that provide detection and defense against Advanced Persistent Threats (APT), credential theft, bots, insider threats, malware, ransomware, and more. Once deployed, the platform provides visibility into the environment and insight into potential or active threats.

NETWORK THREAT VISIBILITY & DETECTION

The ThreatDefend™ platform provides a solution that deploys rapidly and easily, requiring minimal resources and giving the Information Security team efficient and powerful capabilities that other tools cannot match. Using a range of network and asset deception, the ThreatDefend™ platform can identify existing threats that may already exist in the environment, catching an attacker's lateral movement, their efforts to leverage stolen credentials, or exfiltrate data. The suite can also provide insights into potential threats, with visualization tools that make it easier for the assessment team to identify and analyze the environment and exploitation pathways an attacker could leverage.



Organizations have successfully used this methodology, combining deception with conventional tools, to discover and remediate security challenges before, and during, the M&A process. It is a proven technique, returning a high return on investment, and can prove especially useful during a merger when easily and efficiently identifying potential threats is vital.

HOW DECEPTION TECHNOLOGY WORKS

While conventional defenses on the perimeter or endpoints, such as firewalls, IDS, or EDR, work to stop an intrusion or passively identify an intruder's behavior once inside, the fact is that skilled attackers know how to evade and bypass these conventional defenses. Attackers understand that the odds are stacked in their favor. They only need to be right once, while the defender needs to be right every time.

Deception technology takes a different approach. Starting from the assumption that an attacker will get in, deception uses a broad range of decoys to artificially alter the threat landscape and shift the odds in the defender's favor. Now, the attacker needs to be right every time, or risk triggering an alert by using a planted credential or accessing a decoy service.

By implementing a broad range of decoys, from network devices that appear as authentic servers with authentic services, IoT, POS, SCADA, networking and telecom devices, to decoy credentials, shares, documents, and local assets on the endpoints, with the decoy credentials and hosts extending into Active Directory, deception radically alters the apparent attack surface without adding additional workload for IT to manage. The administrators gain visibility and simplified management, while an attacker faces an environment filled with authentic looking traps and decoys that can instantly reveal their presence.

> Organizations have successfully used this methodology, combining deception with conventional tools, to discover and remediate security challenges before, and during, the M&A process.

Decoy hosts and services are projected into the network environment, configured to look like authentic production systems. Since there are no actual production assets on the decoys, an attacker that probes or tries to compromise these hosts is identified without putting production assets at risk. The result is the same whether it is an automated attack or a live intruder.

Local assets and credentials are an inviting target for an attacker, since they can be leveraged to extend the attack across the network. By placing deception credentials, file shares, and documents onto endpoints, an attacker is drawn away from live assets and lured to the deception environment where alert are raised, and attacks analyzed. Tags within decoy documents can also be used to provide geolocation information if an attacker exfiltrates and opens them. The decoy shares can also be instrumental to both slow a ransomware attacker, automated or live, and alert on discovery.

In a merger and acquisition setting, these capabilities provide the tools the information security team needs to quickly identify, and react to, any threats they discover in the new environment.

IDENTIFYING AND UNDERSTANDING ACTIVE COMPROMISES

High-interaction decoys draw in attackers and empower organizations to quickly identify active threats in their environment. The Attivo Networks ThreatDefend™ platform provides unique threat intelligence on attackers by analyzing their activity during the event, showing the threat paths they've followed, and delivering forensics based on their interaction with the decoy systems. Any interaction with the decoys is an anomaly, representing a high-confidence security event.

The platform provides full forensics and attack correlation across the deception environment to reveal actionable threat intelligence on an attacker. The Attack Threat Analysis (ATA) engine can identify the attacker's tactics, techniques, and procedures (TTPs) to identify the attacker's specific target and reveal other potential vulnerabilities in an organization.

Embedding deception into Active Directory gives the solution additional capabilities. By inserting deceptive credentials and adding trust relationships with decoy domains, any activity using those false credentials is immediately identified in both the decoy and production environments. In addition, the ThreatPath capability can identify misconfigurations, trust relationships, and orphaned credentials an attacker could use to move laterally across the network.

In addition to the interactive decoys, the ThreatDefend™ solution features an analysis sandbox engine that can analyze suspicious executables on a dedicated system within the deception environment. This analysis adds to the detection and analysis capabilities inherent in the decoys and provides additional capability, including analyzing suspect files that may have come through email or other sources.

The platform includes native integrations with third-party tools (Firewall, SIEM, Endpoint, NAC, etc.) to automatically share attack information. This gives the organization the power to rapidly and efficiently identify, block, or isolate attacks, and to simplify remediation after an incident. The Attivo Networks ThreatOps™ component lets the information security team create repeatable playbooks that further streamline incident handling and response.

In a merger and acquisition setting, these capabilities provide the tools the information security team needs to quickly identify, and react to, any threats they discover in the new environment.

CENTRAL MANAGEMENT & DISTRIBUTED LOCATION COVERAGE

The ThreatDefend™ platform features the Attivo Central Manager (ACM) System, enabling an organization to centrally manage their entire deception environment, whether it is spread across multiple BOTsink deception appliances or virtual machines, deployed in the cloud, in remote locations or in a hybrid environment.

The platform also includes the ThreatDirect™ solution, that utilizes forwarding technology to facilitate efficient deception deployment into remote locations, such as satellite offices, branches, or retail outlets, without requiring an additional BOTsink system. This feature allows for an easily deployed, light weight solution to protect remote assets while adding minimal infrastructure resources.

Central management and the easy projection of decoys into remote locations provides a unique advantage to organizations who are in the process of examining and integrating diverse and remote environments. The assessment team can efficiently, rapidly, and unobtrusively gain visibility into the combined environment with minimal overhead thanks to the ThreatDefend solution.

EXPOSED ATTACK PATH LATERAL MOVEMENT VISIBILITY

The ThreatDefend™ platform features the ThreatPath solution, which gives an organization the ability to analyze endpoints for exposed or orphaned credentials, or system misconfigurations, that can provide an attacker with lateral pathways to spread through the enterprise. The organization's Information Security team can leverage this information to identify and remediate these potential threats before an attacker can exploit them.

CONCLUSION

Deception technology can play a critical role in Mergers and Acquisition situations, providing vital detection and visibility capabilities for due diligence and post-merger integrations. By revealing hidden threats, providing visibility and detection, and identifying security deficiencies, deception technology gives insights to mitigate risk and strengthen the combined organization's overall security posture.

The Attivo Networks® ThreatDefend™ platform rapidly detects and alerts on suspicious behavior arising from any source, including insiders, suppliers, and contractors. It provides detailed forensics to understand and quickly respond to anomalous behavior. The platform begins working immediately, providing timely visibility, detection, and the attack information required to understand the health and resiliency of a network, shutting down threats before attackers can complete their mission.

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 automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 50 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.Follow Attivo Networks: Twitter and LinkedIn