TAG

UNDERSTANDING ACALVIO’S APPROACH TO ACTIVE DEFENSE

DR. EDWARD AMOROSO,
CEO, TAG[1]

ACALVIO

UNDERSTANDING ACALVIO'S APPROACH TO ACTIVE DEFENSE

EDWARD AMOROSO, CEO, TAG

This technical report explains and provides justification for how deception technology, including the use of honey tokens, from commercial cybersecurity vendor Acalvio,[1] provides a sound basis for an effective active cyber defense for enterprises.

INTRODUCTION

The TAG analyst team has maintained a strong interest in deception technologies, with many members having experience operating a variety of different deception platforms in practical settings over the years.[2] Our collective view here is that enterprise teams tend to under-estimate and hence under-utilize this approach to cybersecurity. This leads to a missed opportunity to leverage a powerful means to reduce risk.

One historical challenge has been the difficulty some teams have faced in managing decoys, which are honeypots that simulate real systems, applications, or assets. These tools have been traditionally designed not only to detect attackers but also to deceive and engage them, diverting their attention from legitimate resources and gathering valuable intelligence about their methods and objectives.

The problem in the past, however, has been that decoys have been tough to deploy, often requiring dedicated infrastructure, such as servers, virtual machines, or containers, to convincingly mimic real environments. The realism of these decoys is critical; attackers must be unable to distinguish them from legitimate systems. Yet, in practice, achieving this level of realism has proven challenging, hampering the wider adoption of deception technologies.

In this report, we outline how Acalvio Technologies, a leader in the cyber deception space, has addressed many of these operational challenges by using honey tokens and improved decoy operation. Acalvio creates digital tripwires, such as fake credentials, documents, API keys, and other artifacts designed to appear legitimate and entice an attacker to interact with them.

For instance, a security team might place a honey AWS access key in an S3 bucket. If anyone tries to use that key, an alert is triggered, notifying defenders of the unauthorized activity. Honey tokens are lightweight, easy to deploy, and require minimal maintenance once they are in place. Their simplicity makes them ideal for widespread use and, with Acalvio's implementation, even more ideal for practical deployment.

WHAT IS ACTIVE DEFENSE?

Our view is that active defense encompasses a set of processes, methodologies, strategies, and sets of tools and platforms designed to gain an advantage over adversaries, with the goal of stopping their attacks before they can cause meaningful consequences. This approach relates to the well-known concept of "shifting left", but places greater emphasis on proactive steps and tangible actions rather than solely strengthening passive defenses.

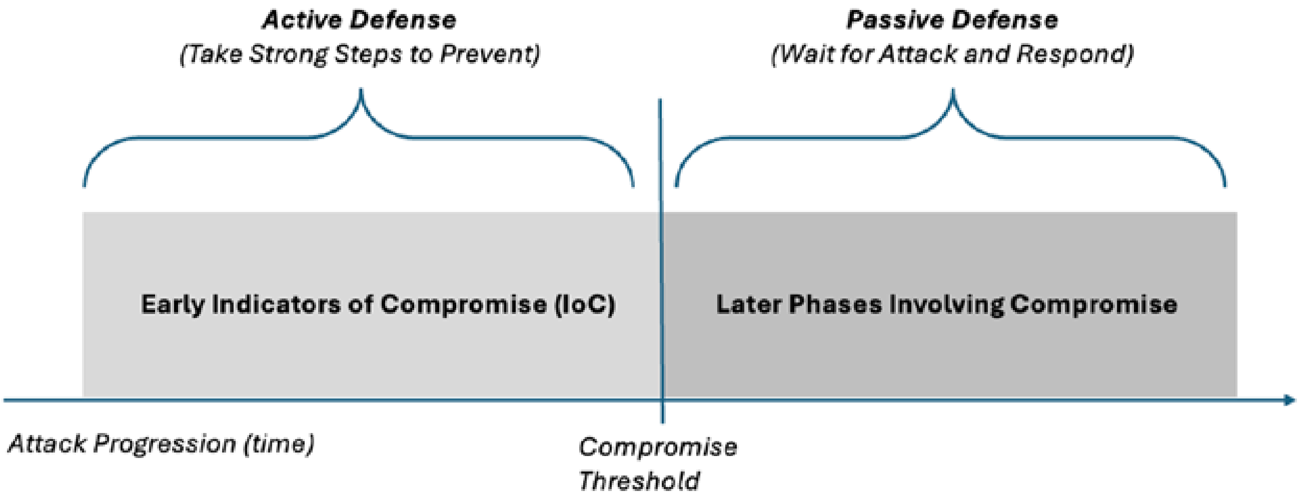
Active Defense
(Take Strong Steps to Prevent)
Passive Defense
(Wait for Attack and Respond)
Early Indicators of Compromise (IoC)
Later Phases Involving Compromise
Attack Progression (time)
Compromise Threshold

Figure 1. Passive Versus Active Defense

The role that deception plays in the establishment of an active defense should be obvious, since the defending team must be thoughtful and engaged in how such controls are performed and monitored. In fact, one of the key aspects of an active defense is that it truly does demand mindful involvement by the security team, both to optimize the results as well as to avoid the negative consequences by being overly aggressive with defensive actions.

ACALVIO'S CORE TECHNOLOGY FOR ACTIVE DEFENSE

In our view, Acalvio excels at creating tools such as honey tokens to drive highly successful active defense campaigns for enterprise security teams. When we look at their platform, we can see that it is built upon several key innovations, each of which enhances the deployment of deception to counter modern enterprise cyber threats. These innovations are listed below:

1. **Advanced Deception Technology:** Acalvio employs a distributed network of high-fidelity decoys that mimic real endpoints, servers, databases, and applications in a way that can be managed with minimal effort.
2. **AI-Powered Detection:** The platform incorporates advanced AI algorithms to analyze attacker behavior in real time. When a deceptive asset is engaged, the AI identifies the adversary's tactics, techniques, and procedures (TTPs).
3. **Scalable Deployment:** Acalvio's patented technology ensures enterprises can deploy honey tokens across large and complex networks without excessive resource consumption.

4. **Identity and Access Protection:** One of Acalvio's strongest features is its focus on identity security. The platform integrates with identity stores and deploys honey tokens in identity stores and across endpoints and cloud services to monitor unauthorized access attempts and detect credential theft.

These core technology features are leveraged by customers, who benefit from assistance in mapping their network to identify critical assets and potential attack vectors. Based on this assessment, the platform deploys honey tokens in strategic locations. Once an attacker infiltrates the network, they are likely to encounter one or more deceptive assets. Interacting with these assets generates alerts, indicating unauthorized access attempts.

The interaction triggers a high-fidelity alert to the enterprise team that bypasses the noise of false positives common in traditional cybersecurity systems. Acalvio's AI analyzes the behavior of the attacker, identifying their objectives, tools, and strategies. This data is fed into the platform's intelligence systems, providing actionable insights for threat hunters and enterprise SOC teams.

With this detailed intelligence in hand, security teams can contain the threat, isolate affected systems, and neutralize the attacker. Acalvio also integrates with other security tools, such as SIEM and SOAR platforms, to automate the response process and reduce mean time to resolution (MTTR). The goal is to avoid harmful consequences by playing an active role in the defensive setup.

THE BENEFITS OF ACALVIO'S ACTIVE DEFENSE

Based on our experience, enterprise teams that deploy Acalvio technology will likely experience a range of useful results, primarily stemming from a more active means for preventing attacks rather than passively responding to incidents after they occur. Key features that we believe will be particularly useful to modern enterprise security teams include the following advances:

1. **Early Threat Detection**: Security measures often rely on signature-based detection or behavioral analytics, which can miss novel threats. Acalvio's decoys ensure early detection by engaging attackers before they reach actual assets.
2. **Reduced False Positives**: High-fidelity security alerts generated by Acalvio's deception technology eliminate the noise of false positives, enabling enterprise security teams to focus on real threats.
3. **Enhanced Threat Intelligence:** By observing attackers in action, Acalvio's platform collects invaluable data on emerging threats. This intelligence helps organizations bolster their defenses and anticipate future attacks.
4. **Cost Efficiency:** Active defense reduces the cost of incident response and remediation by neutralizing threats early. Additionally, Acalvio's lightweight deployment model ensures that enterprises do not need to invest in extensive hardware or additional staff.
5. **Alignment with Zero Trust Principles:** Acalvio's active defense complements Zero Trust security models by monitoring unauthorized access attempts and securing identity systems. This alignment ensures a robust defense against lateral movement.

Modern attacks leverage stealthy offensive techniques such as living-off-the-land exploits, identity-driven attacks, polymorphic ransomware variants, and insider attacks to evade detection through traditional security solutions. While the attacker techniques may vary, the goals of the attacker remain relatively well-defined: to elevate privileges, gain access to critical assets, or exfiltrate sensitive data. Acalvio's solutions deploy strategically designed deceptions to entrap attackers by targeting their goals.

This approach effectively detects threats independent of the attacker techniques, providing visibility to security teams as the threat landscape continues to evolve. Acalvio's intellectual property is based on applying the proven concepts of deception technology into a set of packaged and easy-to-deploy solutions that provide immediate value for customer use cases.

The key use cases for the Acalvio solutions include identity threat detection and response (ITDR), visibility for insider threats, cloud detection and response (CDR), defending against evolving and zero-day ransomware variants, OT and IoT security, active threat hunting, adversary engagement to slow down the threat, protection of critical assets.

ACALVIO METHODOLOGY

The use of deception, including both honey tokens and decoys, is best governed by a well-conceived methodology. Acalvio supports such a methodology, which consists of five steps, each assisted by the use of artificial intelligence (AI). These steps include network discovery, creation and deployment of deceptions, monitoring and triaging of alerts, analysis of adversaries, and then response. The diagram in Figure 2 below shows how Acalvio describes the specifics of each step.

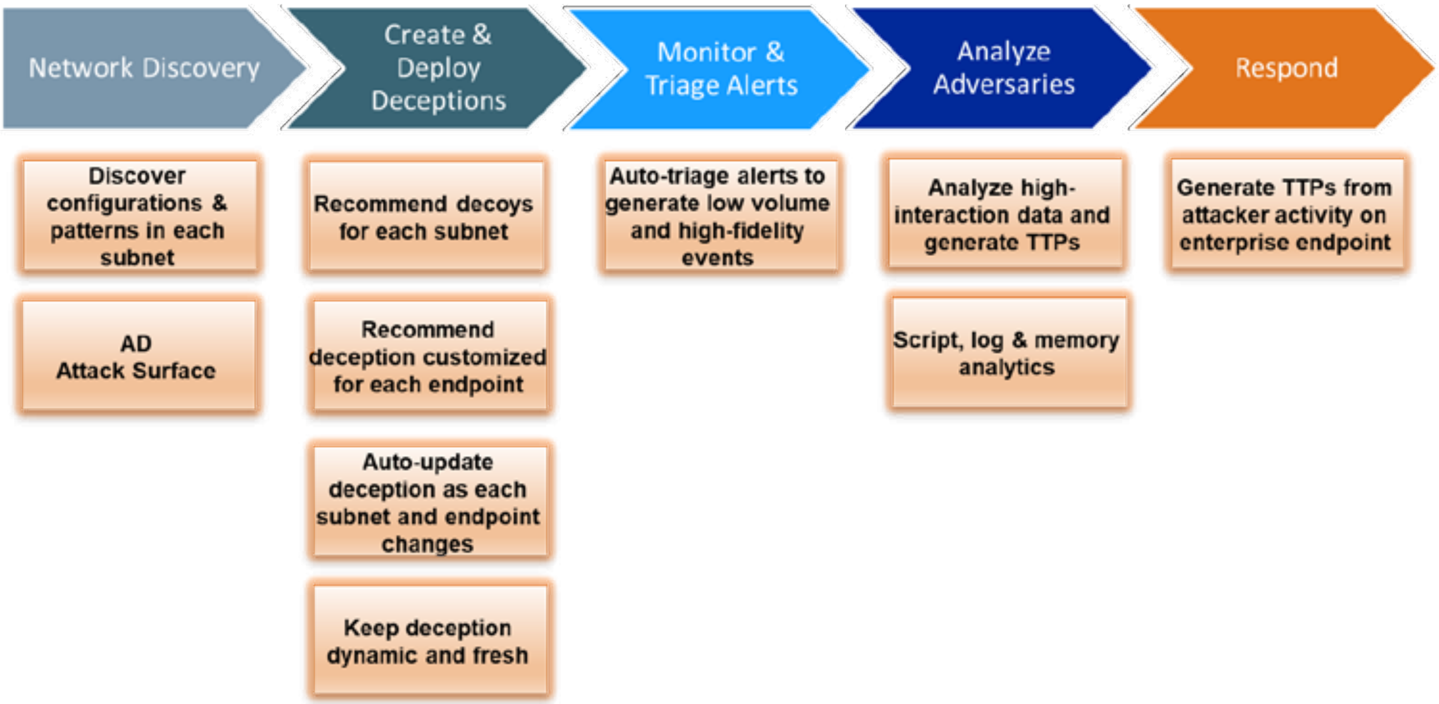
Network Discovery
Create & Deploy Deceptions
Monitor & Triage Alerts
Analyze Adversaries
Respond
Discover configurations & patterns in each subnet
AD Attack Surface
Recommend decoys for each subnet
Recommend deception customized for each endpoint
Auto-update deception as each subnet and endpoint changes
Keep deception dynamic and fresh
Auto-triage alerts to generate low volume and high-fidelity events
Analyze high-interaction data and generate TTPs
Script, log & memory analytics
Generate TTPs from attacker activity on enterprise endpoint

Figure 2. Acalvio Deception Methodology

Ultimately, this type of general methodology will be tailored to the needs of the local environment, but it is valuable to standardize the types of activities that should be present in nearly every deployment. At TAG, we believe enterprises will increasingly recognize the deception management lifecycle as contributing significantly to their overall cybersecurity defensive posture.

ACTION PLAN

In our estimation, Acalvio's active defense strategy represents a welcome paradigm shift in cybersecurity. By combining advanced deception technology with AI-powered analytics, Acalvio provides enterprises with a powerful tool to detect, disrupt, and defeat cyber threats. Its ability to engage attackers, gather intelligence, and protect critical assets makes it an essential component of modern security strategies. With reputed agencies including MITRE and NIST calling for the adoption of deception, Acalvio's solutions enable rapid adoption of deception as part of a robust security posture.

Readers are encouraged to contact the TAG analyst team for expert assistance with deception planning or any other aspect of the enterprise cybersecurity process. In addition, readers can reach out directly to Acalvio for additional details on how they might engage in a proof of concept (POC) or production deployment of their platform. We look forward to hearing from you.

[1] The material included in this report is derived from technical and market discussions with the Acalvio team, as well as from material publicly available reports and other information on their website at https://www.acalvio.com/.

[2] The lead author's first practical deployment experience with deception-based systems involved use of the now-defunct Recourse Technologies system (see https://en.wikipedia.org/wiki/Recourse_Technologies). The lead author wrote extensively about deception in computer security in an early college textbook on the topic published by Prentice-Hall in 1994 (see https://www.amazon.com/Fundamentals-Computer-Security-Technology-Amoroso/dp/0131089293). Much of the material in that early book still applies well to modern deception deployment.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.