ACALVIO
AI-POWERED DECEPTION

DATASHEET

# ShadowPlex Targeted Threat Intel

## Threat Intelligence for Preemptive Cyber Security

## What is Targeted Threat Intelligence

Threat intelligence is a collection of data that helps organizations understand and respond to cyber threats. It is used to identify potential risks, understand the motivations of attackers, and develop long-term security strategies.

Generic threat intelligence provides broad insights about emerging attack vectors and threat trends across industries, while "targeted threat intelligence" focuses on specific information about a particular organization or threat actor, tailored to their unique vulnerabilities and potential attack methods, allowing for more proactive defense strategies against imminent threats.

Advanced attackers such as the Midnight Blizzard APT threat group leverage password spraying against a limited number of accounts to gain initial access. Generic threat intelligence is less effective against such precise attacks, requiring targeted threat intelligence to identify the threat activity and enable proactive response actions.

## ShadowPlex Threat Intel

ShadowPlex TTI deploys external-facing decoys for web applications, APIs and other services that are typical of the services exposed for an organization. ShadowPlex TI filters the noise and generates specific intelligence on the threats targeting the enterprise. The threat intel is shared using standard formats so that the organization can automatically consume and react on the intelligence.

Targeted intelligence provides actionable insights to directly address specific threats against an organization and includes detailed indicators of compromise (IoCs) like IP addresses, compromised credentials, geolocation and specific TTPs used, such as password spraying, brute force, credential stuffing attacks.

Gartner defines preemptive cyber security as “an emerging category of cybersecurity technologies that are designed to prevent, stop or deter cyberattacks from achieving their objectives” and highlighted Acalvio as the innovator in Advanced Cyber Deception. ShadowPlex TTI is a key pillar of preemptive cyber security by providing early threat detection, enabling security teams to proactively build appropriate security measures.

## KEY BENEFITS

- Detailed and actionable threat intelligence on the attacks specifically targeting  an organization
- Alerts on even zero-day exploits
- Immediate notification, enabling quick proactive strengthening of the security posture
- Identification of stolen credentials, addressing one of the biggest threat vectors
- Detailed TTPs enable threat hunting
- Key part of preemptive cyber security

## FEATURES

- Easy and quick deployment
- Completely managed service
- Standard based notification
- Periodic report generation

## SOLUTION

**ShadowPlex Targeted Threat Intel (TTI) is provided both as a managed service or an appliance.**

1. Managed Service: Acalvio hosts the service in Acalvio cloud. All the decoys are spun up and managed by Acalvio. ***No Acalvio component needs to be deployed in the customer's premises.***
2. For customers who want to host the service on-premises or in their cloud, Acalvio provides TTI as hardware or virtual appliances (including cloud VM images).

### Decoy Customization

Customer can choose from a variety of decoy types and Acalvio will help customize the decoys as appropriate for the customer. Additional decoy types can also be created.

### Hosting the Decoys

As managed service, Acalvio will host and manage all the decoys in our own cloud infrastructure. This also removes all attacks against the decoys completely away from the customer's network.

### Threat Intel

All threat intelligence generated by the decoys is shared immediately using STIX format. In addition, periodic reports can be scheduled.

### Management Console

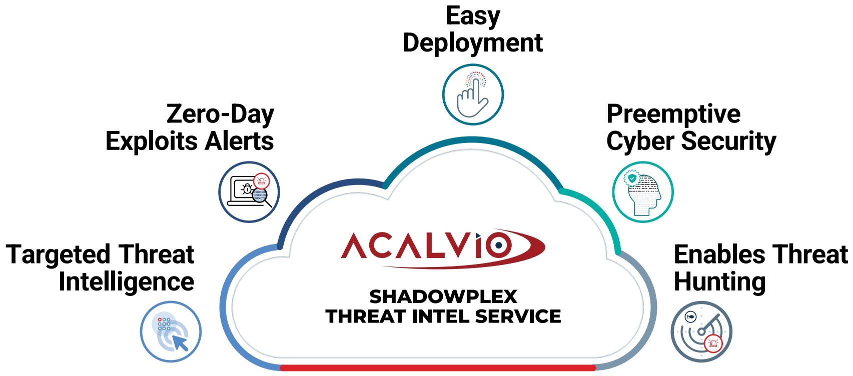
Customers can use the management console to view threat intel data, schedule reports, configure integrations etc.

**Preemptive Cyber Defense**

ShadowPlex TTI provides enterprises detailed threat intel that helps deploy defenses against exploits, including zero days, actively being used by the attackers against the enterprise. ShadowPlex TTI also provides the malicious source IP addresses and the credentials used by the attacks and these can be blocked.

## Threat Hunting

Targeted Threat intel enables threat hunting to search for malicious activity that may have bypassed existing security measures. By using information about threats specifically targeting the enterprise and the attacker tactics, threat hunters can develop hypotheses and hunt for potential threats.


Easy Deployment
Zero-Day Exploits Alerts
Preemptive Cyber Security
Targeted Threat Intelligence
ACALVIO
SHADOWPLEX THREAT INTEL SERVICE
Enables Threat Hunting

Acalvio is the leader in autonomous cyber deception, defending against APTs, insider threats, and ransomware. Its AI-powered Preemptive Cybersecurity Platform, protected by 25 patents, delivers threat detection across IT, OT, and cloud environments and advances Identity Threat Detection and Response (ITDR) with Honeytoken-driven Zero Trust security.

Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from the Cloud, on-premises, or through managed service providers. **www.acalvio.com**

© 2025 Acalvio Technologies, Inc. All rights reserved.