INCREASED PROTECTION FROM RANSOMWARE ATTACKS WITH DECEPTION TECHNOLOGY

Honeywell Threat Defense Platform
Powered by Acalvio®

Honeywell

EXECUTIVE SUMMARY

The Honeywell Threat Defense Platform (HTDP) implements Active Defense to provide accurate, low-risk internal network threat detection for Operational Technology (OT) environments. It is based on deception, an approach recommended by US government standard bodies because of its ability to detect known and unknown (zero-day) attacks. The service includes deployment and ongoing monitoring, freeing up internal security team resources. It is well-suited to organizations who desire advanced detection of intrusions within the building facilities network without having to install or operate complex technology.

Cybersecurity veterans have indicated that determined attackers will eventually find a way into your network. Therefore, organizations must make this assumption as part of their OT risk management process.

> "Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks."
>
> Ransomware Guide
> Cybersecurity and Infrastructure Security Agency (CISA)

STATE OF THE ART IN THREAT DETECTION

The Honeywell Threat Defense Platform meets all key intruder detection requirements. It uses the proven concept of deception. It helps deploy decoy assets such as PCs, servers, OT/IoT devices on the network that look and operate like the device. It then waits for the attacker to try to hack into the decoy and can quarantine attackers using patented deception technologies. Once trapped in the HTDP deception fabric, the attacker is rendered harmless and we can watch and learn from their behaviors. This technique of active defense sets HTDP apart.

Deception has the benefit of making the 'real' valuable devices harder to find, slowing down the attackers and helping capture them faster. It can be deployed in any network, but our service is optimized for Building Management System environments, making it more effective than alternative technologies.

WHY IS DECEPTION A SUPERIOR APPROACH TO THREAT DETECTION?

Accuracy
The Honeywell Threat Defense Platform doesn't try to figure out every approach the attacker might take. Instead we wait for the attacker to come to us. This means very low false alerts, and a high chance of detection. It also means that it even works for "zero day" attacks that have never been seen before.

Low Risk
Deception doesn't put extra software on OT/IoT devices, nor does it require network devices that create a failure point. Hence, it can't cause a service disruption.

Ease of Operations
The Cloud-based Threat Detection Service handles the deployment, ongoing operations, and alert management, so facilities and security teams can focus on other tasks.

THE NEED FOR ACTIVE DEFENSE

To effectively reduce risk, security teams must adopt active defense, and move beyond a passive approach. Active defense blends several tactics that dynamically modify defenses in response to actual threat activity. Deception is the cornerstone of active defense.

DECEPTION – A RECOMMENDED BEST PRACTICE

Organizations (NIST and MITRE) that operate federal government cybersecurity programs have long seen the value of deception for accurate threat detection: "Carefully constructed deception systems are often indistinguishable from production systems and can serve as high-fidelity detection systems." MITRE, An Introduction to MITRE Shield, 2020

THE SIMPLEST PATH TO THE MOST SOPHISTICATED THREAT DETECTION CAPABILITY

The Honeywell Threat Detection Platform is simple, easy to deploy and operate.

1
Easily deploys single Sensor on network

2
Sensor projects fake assets across the network

3
Honeywell Team / Company's Cyber Team monitors and receives threat alerts

4
Honeywell Team interacts with customer to resolve alerts

SECURELY & ACTIVELY ENGAGE ATTACKERS

Removes the attacker from the network. It is sufficient to detect and neutralize, but we take the preferred tactic to monitor and understand the attack in a secure environment. Active defense provides containment for dynamically evolving decoy environments.

SPEEDY DEPLOYMENT

Spin up sensor on existing machine or as a standalone appliance, run playbooks for quick deployment in minutes.

UNMATCHED SCALABILITY

Autonomous capabilities mean little setup interaction is required. Manages the blending, personalization, and scaling of deceptions without manual intervention. Playbooks make for a two-step deployment process.

COMPLETELY AGENTLESS

No software on any elements. The sensor is not an agent and resides on VM's of dedicated servers.

DEEP VISIBILITY

Provides a unique perspective, the attacker's view. Provides deep visibility into hosts, applications, users, servers and critical network assets.

THREAT HUNTING AND ANALYTICS

Extensively monitors the environment providing unequaled opportunity for attackers to reveal themselves. Decoys can be deployed for modeling and to test hypotheses. Activity on a decoy is a near certainty of bad activity. Provides situational awareness on attacker's intentions and tactics.

ADVANCED FORENSIC ANALYSIS

Performs script and memory analysis, lateral movement insights, privilege escalation and other techniques to gain deep insights into attack patterns.

RICH DECEPTION

Existing library of both IT and OT decoys. Allows for custom decoys to be developed. Other deception artifacts such as breadcrumbs, lures and baits extend its capabilities and provides enticing targets for attackers.

PACKAGED SOLUTIONS

First of its kind in deception, Acalvio playbooks incorporate design, intent and industry specific knowledge into a seamless workflow. For example, playbooks simplify the implementation of zero-day ransomware detection and response, data extract detection and response etc.

HOW DOES DECEPTION PROVIDE ACTIVE DEFENSE?

- Attacker sees several instances of each type.
- Decoys are not part of the operational processes. A single access to a decoy raises a highfidelity alert and the attacker is identified.
- Decoys are completely blended, configured by an AI engine with matching systems, interfaces, ports and services – following same naming schemes and even MAC addresses from the same manufacturer.

RANSOMWARE SOLUTION

Honeywell Threat Defense Platform's Autonomous Deception Technology integrated with advanced Artificial Intelligence (AI), provides effective ransomware solution that is easy to use and scale.

- Agentless
- Non-signature based
- Uses deception & AI
- Detects known & Zero-day ransomware
- Very precise & fast

RAPID DETECTION OF RANSOMWARE

A comprehensive deception-based solution to detect ransomware at every step of the Kill Chain. Its specially crafted baits, breadcrumbs and decoys detect ransomware, even zero-day ones, with precision and speed.

AUTOMATED, REAL-TIME RESPONSE

High-fidelity detection enables automated and real-time response. Extensive partner integrations allow to leverage customer's security ecosystem for rapid and comprehensive ransomware containment.

For more information
Buildings.Honeywell.com

Honeywell Building Technologies
715 Peachtree St. NE
Atlanta, GA 30308
honeywell.com

HTDP-SB I 03/22

THE FUTURE IS WHAT WE MAKE IT

Honeywell