



# A Moving Target Defense for Data Storage Devices

## SNIA Storage Security Summit

### May 11, 2022

**Don Matthews**

President & CEO

NexiTech, Inc.

# Protecting Critical Data with Moving Target Defenses

- **What** we do
  - Layers and fit
  - Foundational work
- **How** we do it
  - Technical attributes
  - Reference architecture
- **Why** does it matter to you?
  - This solution provides ransomware protection
  - Cyber attacks can result in real-world physical damage

# Moving Target Defense



- ✓ Reduces the attacker's window of opportunity
- ✓ Increases the cost of the attacker's probing efforts

## **MOVING TARGET DEFENSE**

# Storage Threat Layering

Multiple attack vectors are available

Multiple vendors protect most layers

NexiTech stands alone  
with comprehensive  
**Moving Target Defense**  
at the Data Storage Layer

Identity Management  
VPN, SSO, Authentication

Web Application Security/  
Content Filtering

Application Memory

Operating System

Server Hardware



reads



writes

## DATA STORAGE SYSTEMS

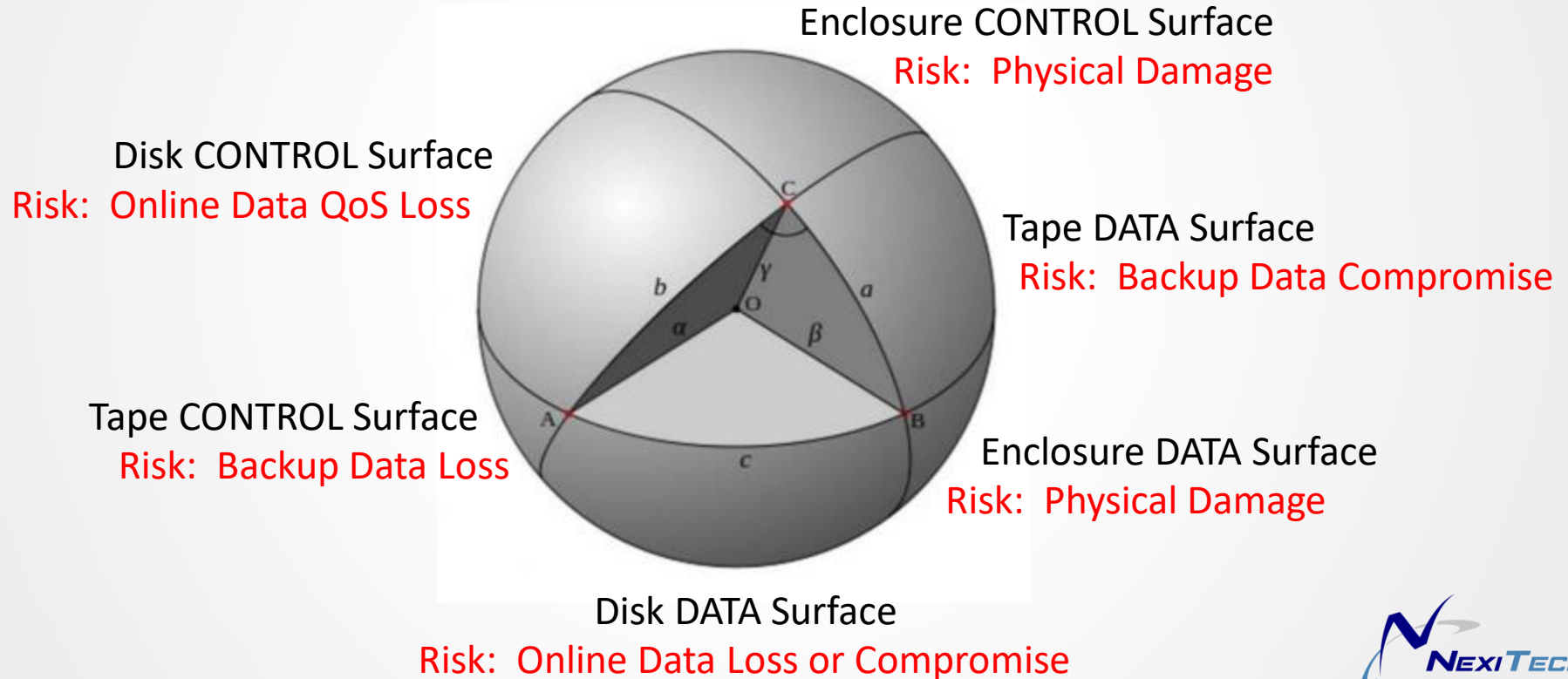
Enclosures  
power, cooling

Data in Motion

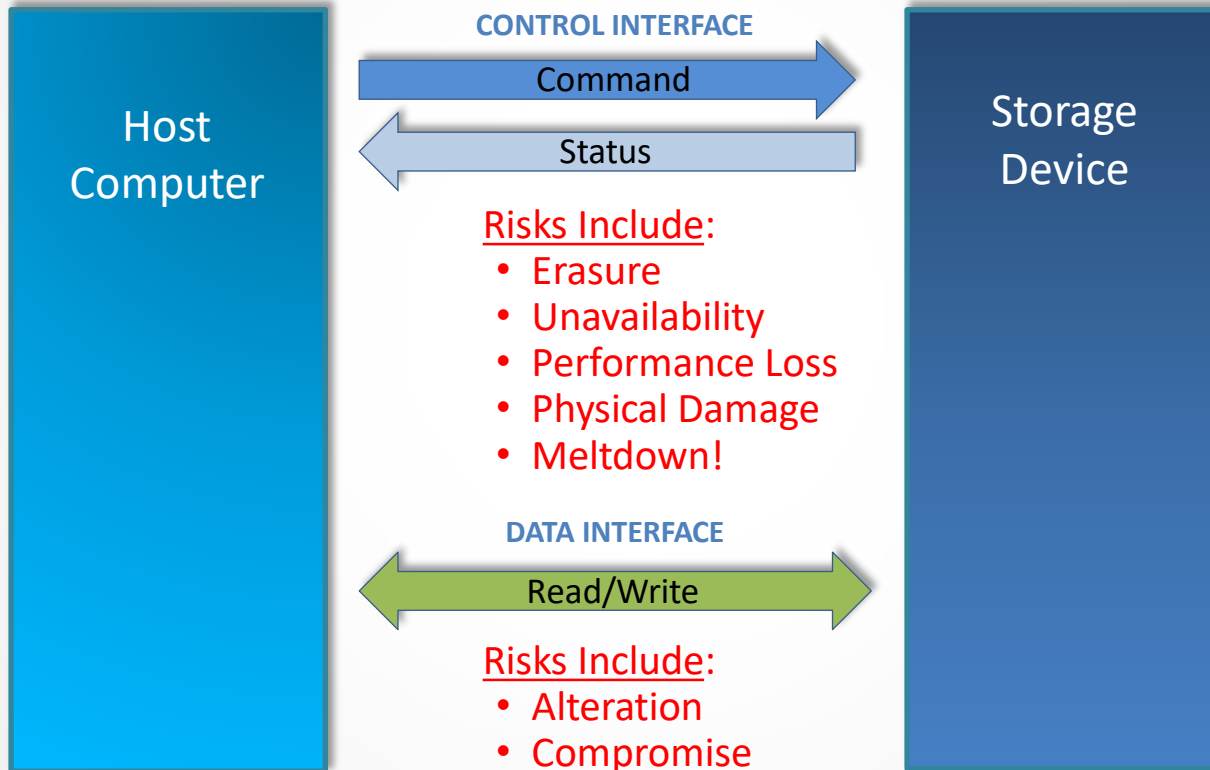
Solid State Drives

Data at Rest

# Storage Attack Surfaces



# Storage Attack Surfaces



# Our Place In The World

Cyber Security  
Domain

Data Storage  
Domain





# Successful Customer Engagements

Mission  
Planning  
Environments



2012



Silicon Valley  
Innovation Program

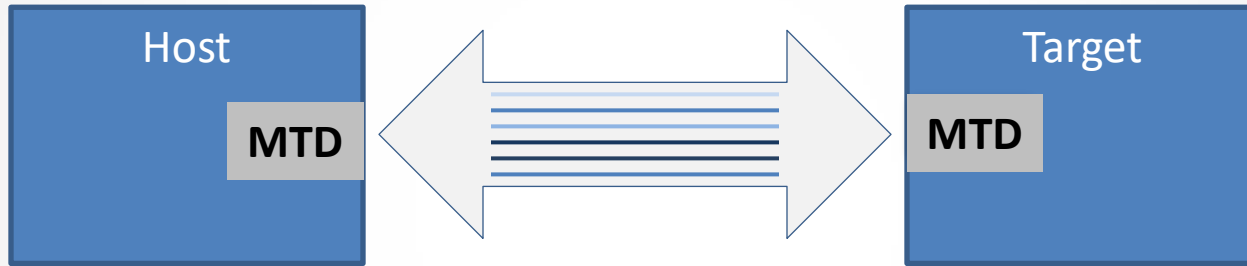


2017

# Our Technical Solution

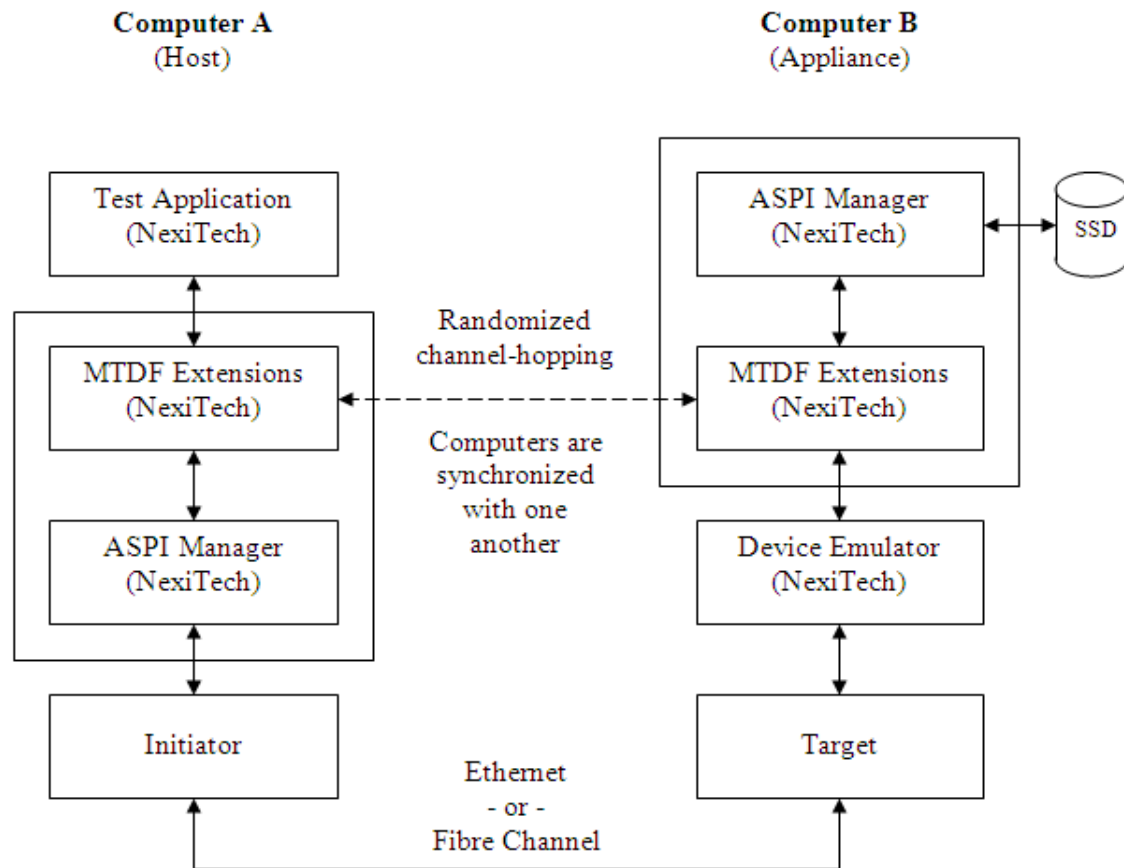
- **Isolate the device**
  - Change the device type from "disk" to "unknown" inside a storage appliance.
  - Create multiple abstractions of the device using storage virtualization.
- **Obfuscate the command set**
  - Change the command set for the device inside the appliance.
  - Makes it more difficult for an attacker to access the device, but not impossible.
- **Now introduce a Moving Target Defense (MTD)**
  - Change the communications channel from one command to the next.
  - Change the command set itself from one command to the next.
- **Statically link the interface library (optional)**
  - Only specific applications can access the device.

# How It Works



An autonomous system that randomly changes multiple dimensions of the attack surface, making it unpredictable to adversaries.

# MTD Framework (MTDF) Reference Architecture

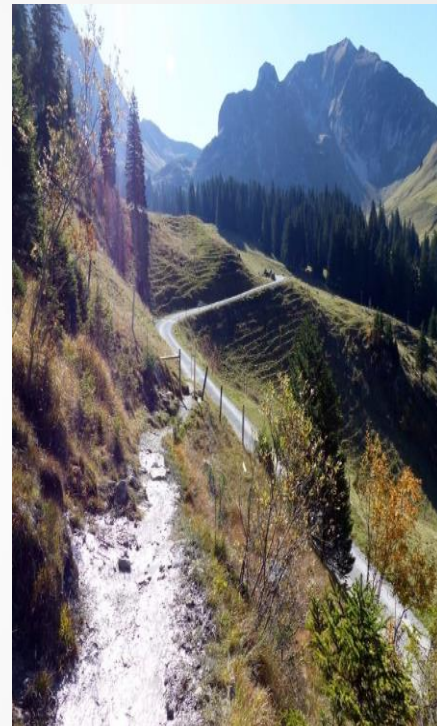


# Technical Attributes

- Autonomous
- Multi-dimensional
- Uses randomization
- Unpredictable by adversaries
- Dynamic network configuration
- Gathers metrics and reports breaches
- Optionally may use a Honeypot (i.e. Decoy)
- Address Space Layout Randomization (ASLR) for DATA STORAGE

# Why Should You Work With Us?

- Evolving the technology
- Expanding market opportunities
- Forming a network of partnerships
- Exploring a broad range of additional use cases
- Subject Matter Expertise in NVMe
- Subject Matter Expertise in Kernel Drivers



# Summary

- The core technology is adaptable
- It uniquely protects data-in-flight for the storage DATA surface and also the storage CONTROL surface
- Can exist in an appliance ...
- ... or can be embedded in the device itself
- This is one more tool in the toolkit when it comes to fighting ransomware and stopping cyber attacks!

# MTD – The Last Line Of Defense





# Call To Action

- Review our Virtual Expo page
- Download our slide deck for additional bonus slides
- Reach out to learn more about Moving Target Defense

# Let's Start a Conversation!

## Questions?

NexiTech, Inc.  
Don Matthews  
President & CEO  
970-702-2388  
[matthews@nexitech.com](mailto:matthews@nexitech.com)  
[www.nexitech.com](http://www.nexitech.com)

# DHS Silicon Valley Innovation Program

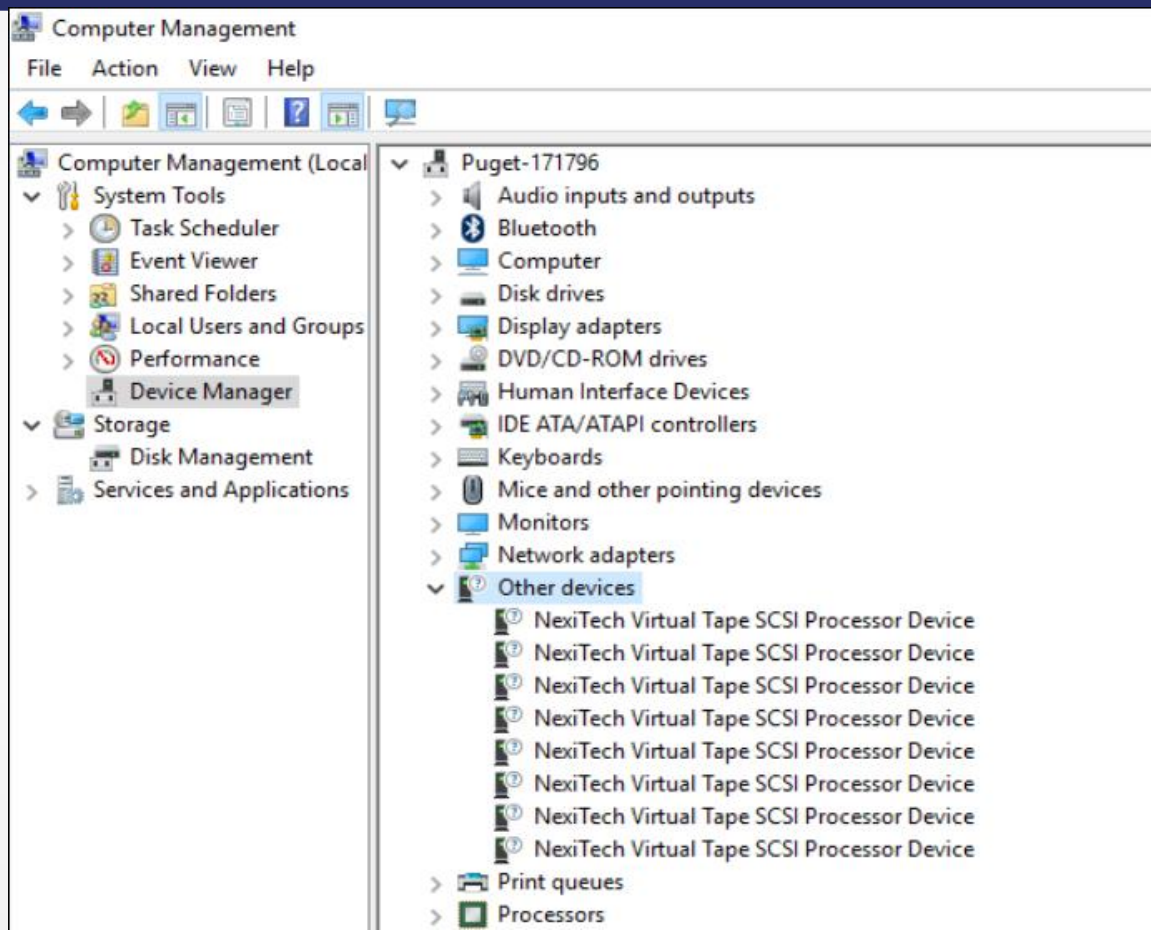
Latest News - Moving Target Defense | SVIP | Homeland Security

dhs.gov/science-and-technology/svip#

## Financial Services Cyber Security Active Defense

- [Cyber 20/20 \(Newark, Delaware\)](#) will build TURACO, a next-generation sandbox, which uses machine learning to significantly extend Cuckoo, an open-source sandbox environment, and defend against anti-anti-sandbox malware. (Initial award June 2018) – **Currently in Phase 1**
- [Def-Logix Inc. \(San Antonio, Texas\)](#) will enhance its Entrap capability that provides malware detection, characterization and enhancement capabilities to enable the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. (Initial award December 2017) – **Currently in Phase 1**
- [Heilig Defense, LLC \(Arlington, Virginia\)](#) will develop the Memory Sentry solution, which provides runtime application protection against specific memory-safety vulnerabilities. Memory Sentry is a “pre-exploitation” protection tool that can disrupt an attacker’s ability to successfully exploit software vulnerabilities. (Initial award October 2017) – **Currently in Phase 3**
- [Intafel \(Cambridge, MA\)](#) will enhance their product Solitare, a slimmed-down virtual machine capability, to create a Moving Target Defense system that uses randomized isolation to increase the cost and complexity of attacking financial institutions. (Initial award September 2018) – **Currently in Phase 1**
- [Morphisec \(Beer-Sheva, Israel\)](#) will develop a Moving Target Defense-based cybersecurity solution for virtual desktop infrastructure (VDI) environments to prevent cyber attacks to financial institutions without reducing the overall performance of an enterprise-level VDI environment. (Initial award September 2018) – **Currently in Phase 1**
- [NexiTech, Inc. \(Woodland Park, Colorado\)](#) will develop an innovative Moving Target Defense approach to providing critical protection for storage devices and networks. It aims to protect storage management and data interfaces by creating multiple abstractions of devices—similar to frequency-hopping previously used in radio communication—to confuse potential cyber attackers. (Initial award October 2017) – **Currently in Phase 1**
- [StackRox, Inc. \(Mountain View, California\)](#) proposes a software solution that runs as a collection of integrated, container-based micro services within a computing environment that identifies cyber attacks and uses container-native software to automatically stop malicious activity on affected applications. (Initial award May 2017) – **Currently in Phase 3**
- [Veramine \(Bothell, Washington\)](#) seeks to harden financial institutions’ cyber defense by adding cyber intrusion deception, moving target defense and isolation and containment capabilities to its current Endpoint Detection & Response platform with the aim to significantly increase the economic costs for potential attackers. (Initial award June 2017) – **Currently in Phase 1**

# Device Manager View of Multiple Abstractions



# Cyber Defense Matrix

NIST Operational Functions					
Assets	Identify	Protect	Detect	Respond	Recover
Devices	YES	YES	YES	NO	NO
Applications	YES	YES	YES	NO	NO
Network	YES	YES	YES	NO	NO
Data	YES	YES	YES	NO	NO
People	NO	NO	NO	NO	NO

# Inspirational Machines

