Fortress

Rethinking Cyber Resilience for Industrial Control Systems

Speakers

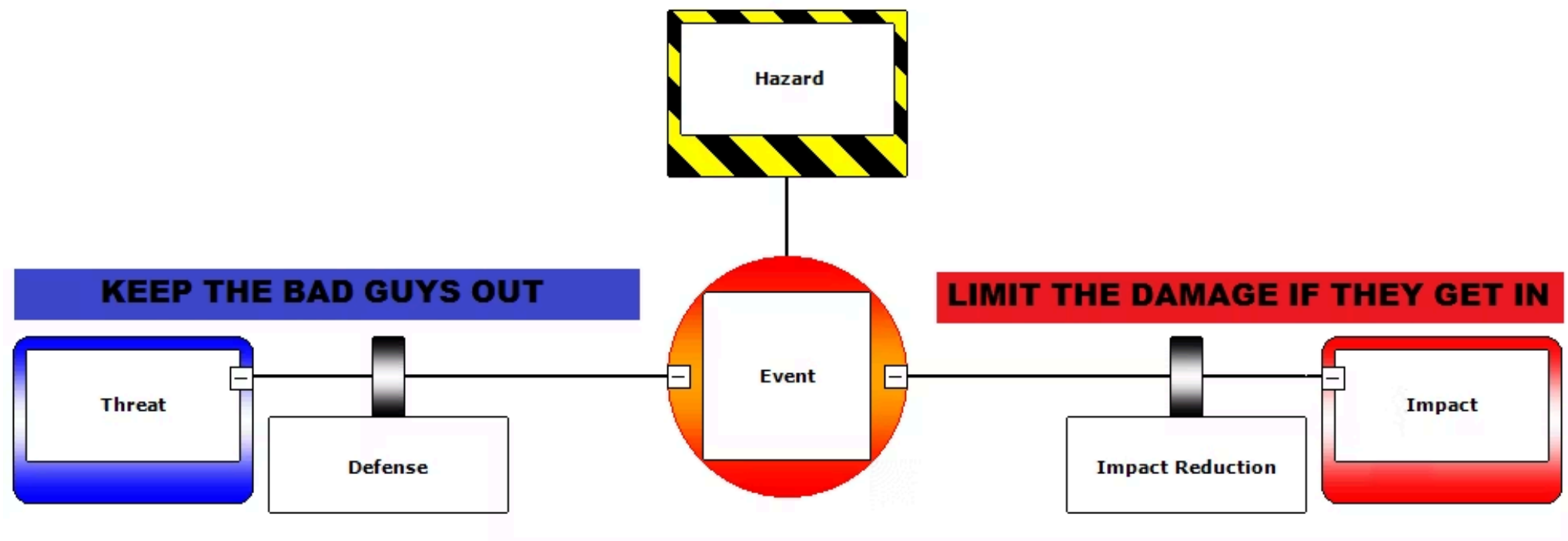
Ben Simon (CEO)

- Venture Partner at Spark Capital (2022) and Partner at Mechanism Capital (2020-2021)
- Philosophy and Computer Science at Stanford (2017-2019) and Harvard (2019-2020)

Leor Fishman (CTO)

- Senior Backend Engineer at Skiff (2021-2022) and Fractal (2020-2021), Researcher at Leidos (2016-2017)
- Computer Science at Harvard (2017-2021)

In the 1990s, Shell introduced the cyber resilience “bow tie,” which has two sides: prevention on the left, and remediation/recovery on the right



In IT vs. OT, there is a world of difference when it comes to the cyber recovery and the “right side of the bowtie”

As a generalizing statement, in IT, the overarching focus is on *data;* In OT , the focus is on *process.*

A successful cyber attack has very different ramifications if the target is a law firm versus a power generation facility

- With the former, the majority of the damage is done once the data is leaked
- With the latter, the damage is only done if critical operations cannot continue and the process must shut down

“CIA Triad” — Confidentiality, Integrity, Availability

When it comes to critical OT systems, Availability is the highest priority

In a world of growing cyber threats, existing OT cyber resilience do not provide robust availability and immediate recoverability for critical OT systems in the event of a cyber attack

More specifically:

1. Data backups are inherently restricted from a recovery time perspective

- Limited recovery flexibility
- Only available at the image level, not at the control system level

2: High Availability (HA) systems are vulnerable to cyber attacks

- Usually built using a hyper-converged architecture

The ideal OT cyber resilience solution must therefore provide both:

1. Near-Instantaneous Recovery (*a la* High Availability)
    a. Extremely rapid recovery times
    b. Recovery times must be maintained even when disparate pieces of software are simultaneously being recovered
2. Robust Integrity, Isolation, and Cyber Resilience (*a la* Immutable Data Backups)
    a. The system must not allow for lateral movement between the primary system and the secondary/backup system
    b. Ideally should only copy over a limited set of configuration data from primary to backup, rather than entire applications

Introducing Fortress

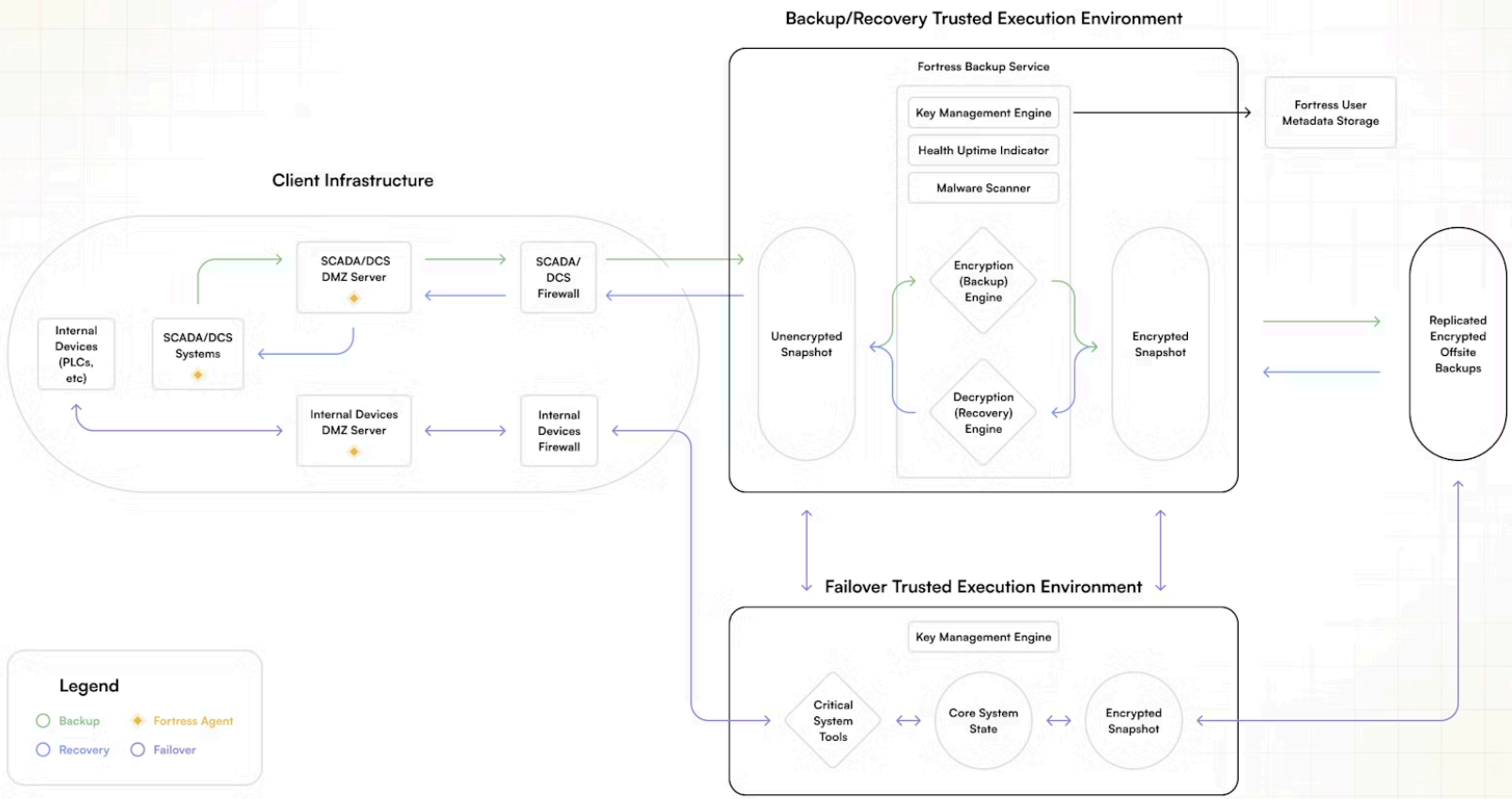
Fortress is a Cyber Resilience platform purpose-built for the needs of OT systems, which provides operational continuity and immediate recoverability within an isolated, secure-by-design availability environment

Tested with the DOE and CISA

Testing performed in November 2023 at the Pacific Northwest National Labs

"Overall, the Fortress platform successfully completed its pre-defined objectives of backing up, recovering, and failing over the water treatment skid while maintaining PLC integrity and machine activity with ***no noticeable data loss and high system availability.*** *More specifically, there was* ***only 47 seconds of downtime*** *from the initial loss of Aveva Edge functionality to the resumption of Aveva Edge control via the Fortress Failover system. Moreover, simultaneously running the onsite and Failover systems* ***did not induce PLC thrash****. On the Backup and Recovery side, all restoration tasks were completed successfully—from the project level to the full drive backup and restore—****without any noticeable data loss or interruptions in primary system data collection.****"*

System Architecture



For more information, contact:
ben@fortresslabs.com

Fortress

Appendix: Security

Fortress is designed to meet the unique architectural, networking, and security constraints of modern OT environments.

- Fortress uses Trusted Execution Environments to provide hardware-enabled security, isolation, and integrity of all resilience processes
  - Trusted Execution Environments are secure computing environments with the following properties:
    - Host isolation (physical machine access ≠ logical access)
    - No default external networking or third-party access
    - Data-in-use encryption ("Confidential Computing")
    - Cryptographic attestations of code integrity
- Fortress provides networking daemons to ensure that controllers do not need to be reconfigured to use failover
- Fortress is designed to meet the regulatory requirements of NERC CIP, IEC 62443, and other leading regulatory frameworks of cyber-physical systems.