superna

Thought Leadership paper - Securing data means evolving the problem statement

Overview

The security industry spends a lot of time building eggs, hard outer shells to keep the bad actors out. What’s on the inside of an egg? A soft easy target. The entire security industry evolved from the early Word macro viruses and other annoying malware that plagued the early days of computing.

The evolution of the security industry has been to collect more data, analyze this data and automate responses while reducing false positives for Infosec teams to action and respond to.

Many buzzwords are thrown around XDR, EDR etc.. are all forms of the evolution above but all have an obvious flaw.   They all look like a boil the ocean approach to security with AI/ML applied against a massive pool of log data.

A personal pet peeve is the assumption that AI/ML will save us all from “fill in the blank” problem statement.   All AI/ML is not created equally and it’s only as good as the team that wrote it. It’s just more software, it did not change the approach to the problem, it is simply accelerating analysis from an old way to a new way.

What’s the new problem statement?

Ransomware changed the problem statement but the approach to security did not change.   New problem statement for data security: The fact is ransoming data or theft of data for public release are the 2 primary objectives of cyber attacks. A 3rd objective is complete destruction to harm a business to the point that it cannot recover. This last point is overlooked by many Infosec teams that focus entirely on the financial motives of bad actors. We have not yet seen this last objective executed but it’s coming.

The problem statement above makes no mention of protecting laptops, servers, network switches and Cloud virtual machines.   It only mentions data, the target of all cyber attacks.

In the section below we will take a look at the mainstream vendors statements regarding next generation security products.

Let's review the XDR, EDR definitions of cyber security.

EDR is endpoint detect and respond and is narrowly focussed only on endpoint security. XDR is extended to detect and respond and this is positioned as the evolution of EDR based solutions that encompass more data inputs from other security domains in order to correlate and make decisions on the threat level.

This evolution comes from the ability to collect data and correlate it from more sources than endpoints alone. Multiple mainstream security vendors list the following areas as all encompassing: endpoints , servers , Cloud security, email, network and mobile.

One gaping hole in the above definition is the storage devices themselves that store the data that is the target of the attack.

What could the storage device offer in terms of input to threat detection?, let's review that below.

Storage Device Security Features

Storage devices can be anything that stores data and allows access over various protocols such as SMB, NFS, S3, HDFS and many others.

1. Snapshots (point in time immutable) or automatic data versioning (i.e. S3)
2. Replication (sync or async)
3. APIs to control the security of user and application access
4. Audit log of any data manipulation (common to all storage devices)

Audit log data has something in common across all storage vendors in that the operations against the data are the same.

1. Read
2. Write
3. Delete
4. Rename
5. Modify
6. Create
7. Access control change

It certainly looks like we have a common method to track threats against data regardless of the vendor that stores the data.

Let's test this out against Cloud storage, are the above operations common in the Cloud when data is manipulated? yes they are.

Does that mean we now have a standard that would allow protecting data on premise and in the Cloud? Yes, it does.   Why has no security framework been presented to use a data centric approach.   Likely due to cyclical innovation on old frameworks and no new eyes on the problem.

What needs to change? Re-thinking how security is applied to infrastructure.

Who is doing this? Superna's long history of innovation and data centric product solutions offer a data first approach to security, orchestration, management, and analysis.

What should the next generation security architecture look like if based on today's security problem statement?

A data first ring based security approach that is designed to prioritize analysis and the weight of alerts from devices that are nearest to the data itself. Note this architecture is generic and applies to Cloud and on premise IT resources.

Ring 0 - Offline copy of data Cyber vault or backup solution with offline capabilities

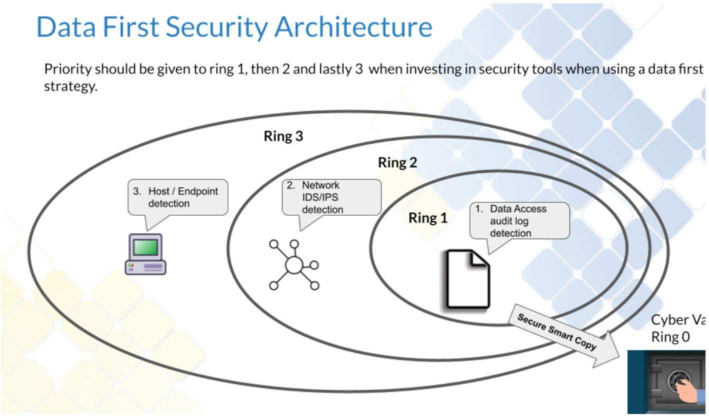
Ring 1 - Storage devices that store data file, object and block storage

Ring 2 - Network devices that connect hosts to storage devices, that have visibility to users, applications and storage devices.

Ring 3 - endpoints, hosts with applications

Ring's greater than 3 - These are areas that create a hard outer shell of security but once penetrated offer little value to an attack that is occuring inside ring 0 to 3. Examples would be security products for email, spam gateway, Internet facing firewall, mobile phone, configuration management, OS patching solutions.

This diagram visualizes the Data First Security architecture.



Data First Security Architecture

Priority should be given to ring 1, then 2 and lastly 3 when investing in security tools when using a data first strategy.

Ring 3
Ring 2
Ring 1
3. Host / Endpoint detection
2. Network IDS/IPS detection
1. Data Access audit log detection
Secure Smart Copy
Cyber Va
Ring 0

What are the factors when designing a Data First Security Architecture?

1. Build your security architecture from Ring 0 outward and ensure the vendor's approach can support storage devices natively.
2. Ensure products selected can analyze user behaviors of data manipulation in real time
3. Don't assume AI matters, look for proof points with independent 3rd party testing of the solution actually doing what they claim they can do.
4. Automation api's to hook into existing security tools is vital, without this in place no cross domain detect and respond can occur. The ring 0 devices solution must support automation API's to empower tools protecting Ring 2 and 3 to request data protection services, or user lockout or forensics logging.
5. Products with external script trigger capabilities
6. Forensics for post incident precision recovery , root cause of ground zero of the attack

What Considerations do Hybrid Cloud architectures introduce?

1. Security architectures should not be applied differently from on premise to the Cloud. The problem statement of protecting data is the same.
2. Data Orchestration is fundamental to a hybrid Cloud architecture with data moving in both directions. This requires a solution that understands data moves and needs to accommodate this requirement.
3. What if the data orchestration

layer was security aware and used inputs from the security systems to apply protection policies to data inflight in either direction (north south, and east west data movement).

   a. This requirement fits perfectly with the data first hybrid Cloud approach defined in the paper here. The concept is data that is moving from on premise to the Cloud or Cloud to on premise or Cloud to Cloud should have consistent security protection and policies that limit data movement under threat scenarios.
   b. In Superna’s case, Golden Copy is the cornerstone to a secure data orchestration layer that is fully integrated with our Ransomware, Auditing and cyber security solutions.

4. A solution that is common to both on premise and Cloud the Cloud makes obvious sense to protect data with the same capabilities and visibility, monitoring where ever the data lives

About the Author
Andrew MacKay - President & CTO of Superna