
Clarium

*Why breaches occur and how Clarium Managed Services prevents them*

# Cybersecurity

www.clarium.tech

# TOP (5) REASONS BREACHES OCCUR?

Conventional cybersecurity products are designed to detect and remediate an attack, not prevent them.

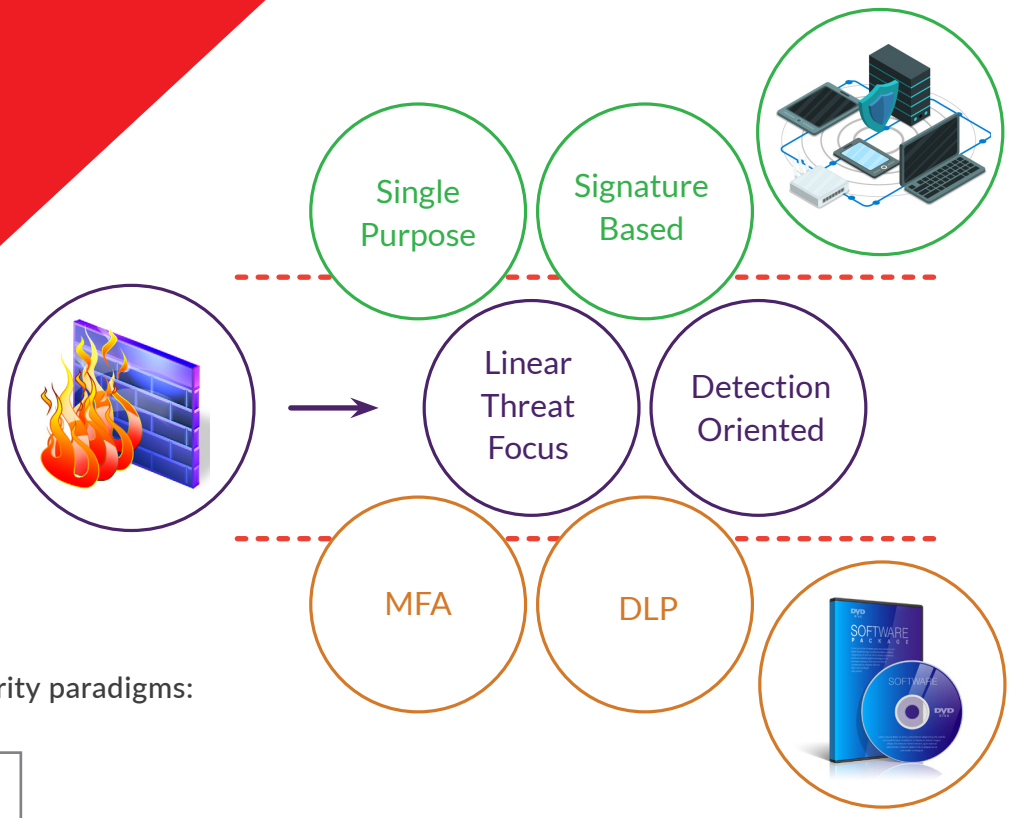
Conventional vs. layered defense strategy. Lack of understanding on how modern threats actually evolve during an attack.

Insufficient assessments, testing, and patching.

Disjointed Solutions – Security products that do not communicate threat to another area of the eco-system. For example, Advanced Endpoint Protection alerts to the Firewall.

Human error such as improper configuration.

# WHAT IS A CONVENTIONAL APPROACH TO CYBERSECURITY?




**Products are oriented around (3) primary security paradigms:**

1. Endpoint Protection
2. Firewalls
3. Security Software

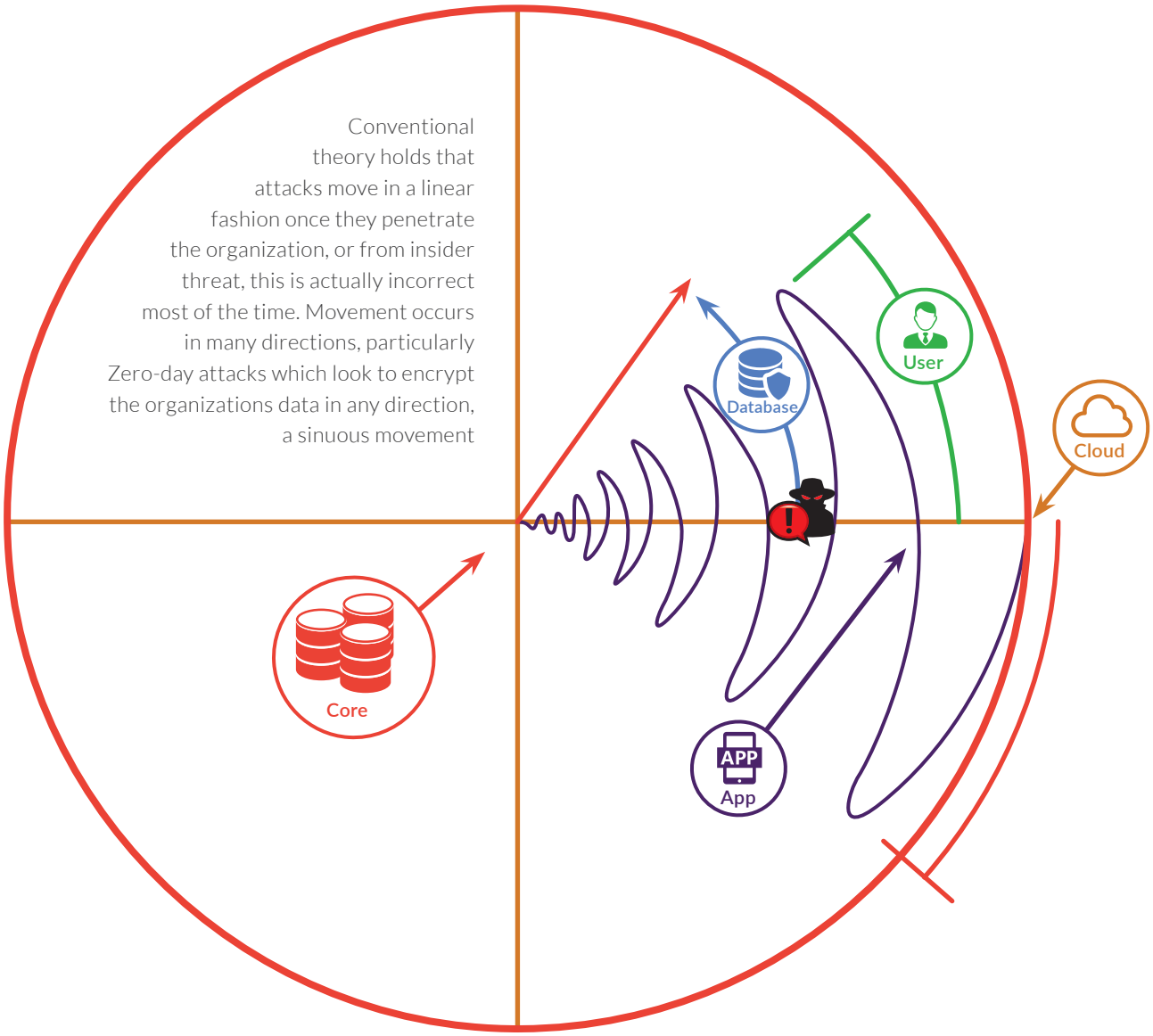
Focus is primarily on outsider threat and/or linear attack orientation.

Entirely focused on the efficacy of a product to protect a portion of the security eco-system instead of taking a data first approach to defending data.

An event in one part of the eco-system does not alert and prevent the attack from progressing to the rest of the entity since they are not integrated. This leaves a clear path to whatever goal the bad actor is seeking.

Monitoring and logging this model is complex for security firms, much less internal security resources

# THE SINUOUS THREAT VECTOR




## SIN·U·OUS DEFINED

/ˈsinyo͞o͞əs/

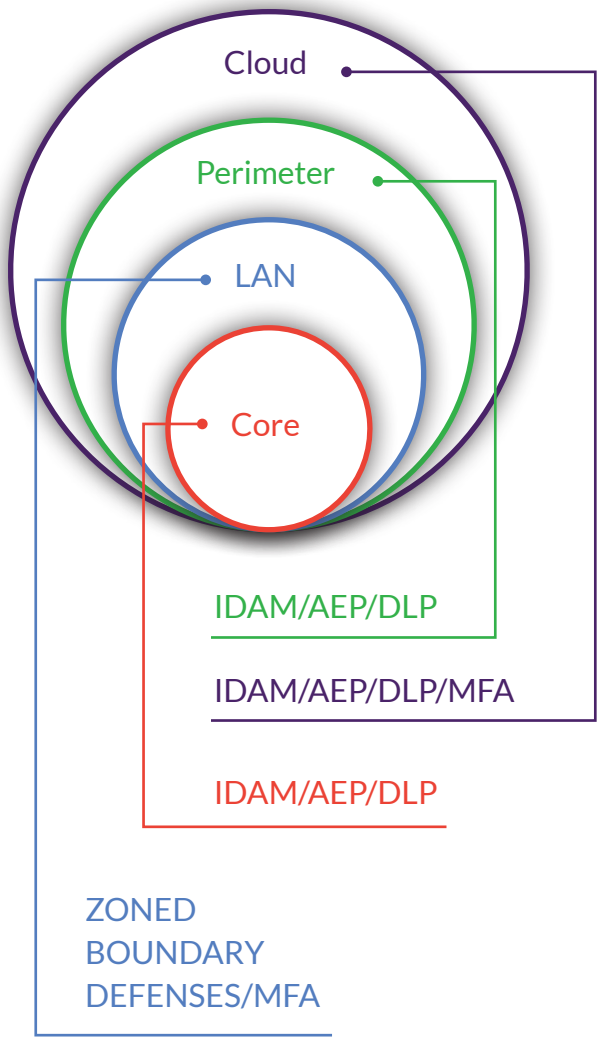
having many curves and turns.
"the river follows a sinuous trail through the forest"
synonyms: winding, windy, serpentine, curving, twisting, meandering, snaking, snaky, zigzag, zigzagging, turning, bending, curling, coiling, undulating

**Modern cyber attacks penetrate and move throughout your organization following any clear path including an insider, in most cases these paths are not linear.**

**This requires a new security approach to how we prevent and disrupt the attack.**

# WHAT IS A LAYERED CYBERSECURITY DEFENSE?

Each layer of the eco-system has multi-method defense




## The Security Eco-System

- MFA = MULTI-FACTOR AUTHENTICATION
- AEP = ADVANCED ENDPOINT PROTECTION
- DLP = DATA LOSS PREVENTION
- IDAM = IDENTITY MANAGEMENT

Focused on preventing attacks from any direction or dimension, sinuous attack prevention orientation Products must utilize multiple methods to prevent an attack, such as: behaviors, anomalies, and artificial intelligence (AI).

Not one product is more important than another, only deployed in a sequence based on prevention priority.

A breach in one part of the eco-system alerts and remediates the entire eco-system.

A layered approach allows machine learning and artificial intelligence tools to provide greater prevention of threats across the entire entity.

Each area is a ZONE and provides multi-method defenses that disallows any unauthorized or unencrypted traffic that doesn't fit an acceptable use. Once all the defenses are orchestrated, a monitoring SOC, or SEIM is overlaid providing oversight of the entire security eco-system.

# 10 CLARIUM PRACTICE AREAS

## Data Protection, Encryption and Privacy

## Mobile Security

## Network Security

Prevention of APT, visibility solutions, isolation and deception for the enterprise network.

## Applications and Website Security

Security measures for software and web applications, including code review, bot detection, DevSecOps, web application firewall (WAF) and DDOS prevention.

## Endpoint Security

Anti-malware and anti-ransomware solutions, and Endpoint Detection and Response (EDR).

## Connected Devices, IOT and Control Systems

Solutions for security challenges when usng connected devices, from IOT network and mobile device management, to connected cars, industrial control systems, and medical devices.

## Cloud and Infrastructure Security

Solutions for securing cloud services, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), container-based virtualization and serverless computing.

## GRC and Vulnerability Management

Cyber-risk and vulnerability management, solutions for cyber insurance, supply-chain monitoring, and compliance audit.

## Anti-fraud, Authentication and IAM

(Identity and Access Management)

## Security Operations and Orchestration

All operational measures required to protect an enterprise network, including Security Orchestration, Automation and Response (SOAR), forensics, SIEM, alert management, threat intelligence, security analytics, and penetration tests.

Clarium is a market-leading provider of end-to-end cyber security solutions.

We help clients assess, plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities in cyber security strategy and managed security services, incident response, risk and compliance, security consulting, training and support, integration, and security technology.

Through our highly specialized 10 practice areas we cover the entire spectrum of cyber defense from assessment to monitoring.

# CLARIUM'S FIRST 5 STEPS TO PREVENT A CYBER EVENT..

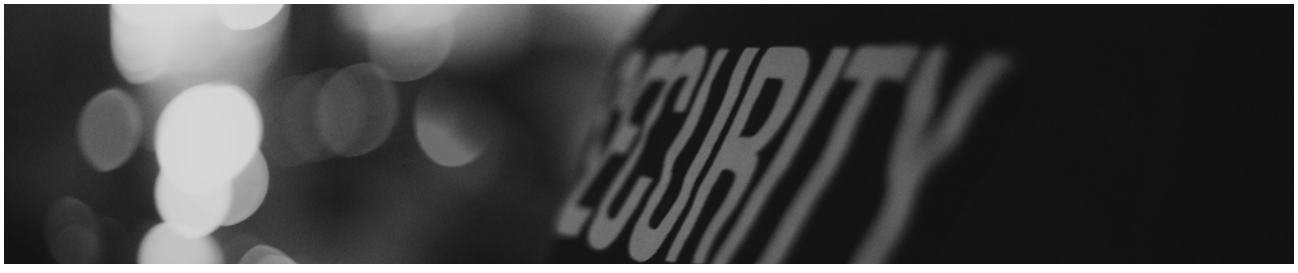
Conducts an assessment using our Assessor+TM platform which:
- Give you a baseline starting point of your current cyber defense health
- Provides a simple roadmap to a sinuous threat defense

Work together to develop a simple, no nonsense path to implementing a cost effective security infrastructure that is 100% prevention focused.

Acts as your trusted advisor Clarium represents your firm to the (30) different technology suppliers we have alliances with, such as Palo Alto Networks, Check Point, Fortinet and others.

Apply additional relevant solutions from among Clarium's practice areas as needed to achieve cyber health and regulatory compliance.

Upon achieving a healthy score in Assessor+TM , we will provide you with a monitoring solution from our redundant Security Operations Center (SOC) where you can have piece of mind that your operation is being closely guarded.



# ABOUT CLARIUM

Clarium helps customers run and reinvent their cybersecurity with scalable, and effective solutions to complex security problems. Agile, Cyber security practice with a track record encircling the globe executing on all levels of information security including guidance, design, implementation, and delivery of a secure eco-system. www.clarium.tech



## CONTACT US

Address:
2244 NW 114th Avenue, Miami
33172 United States

Fax: +1 954 272 7766
Security Center: + 1 877 THREAT 0
Email: contactus@clarium.tech