CYBEROPS
MONITOR AND PROTECT

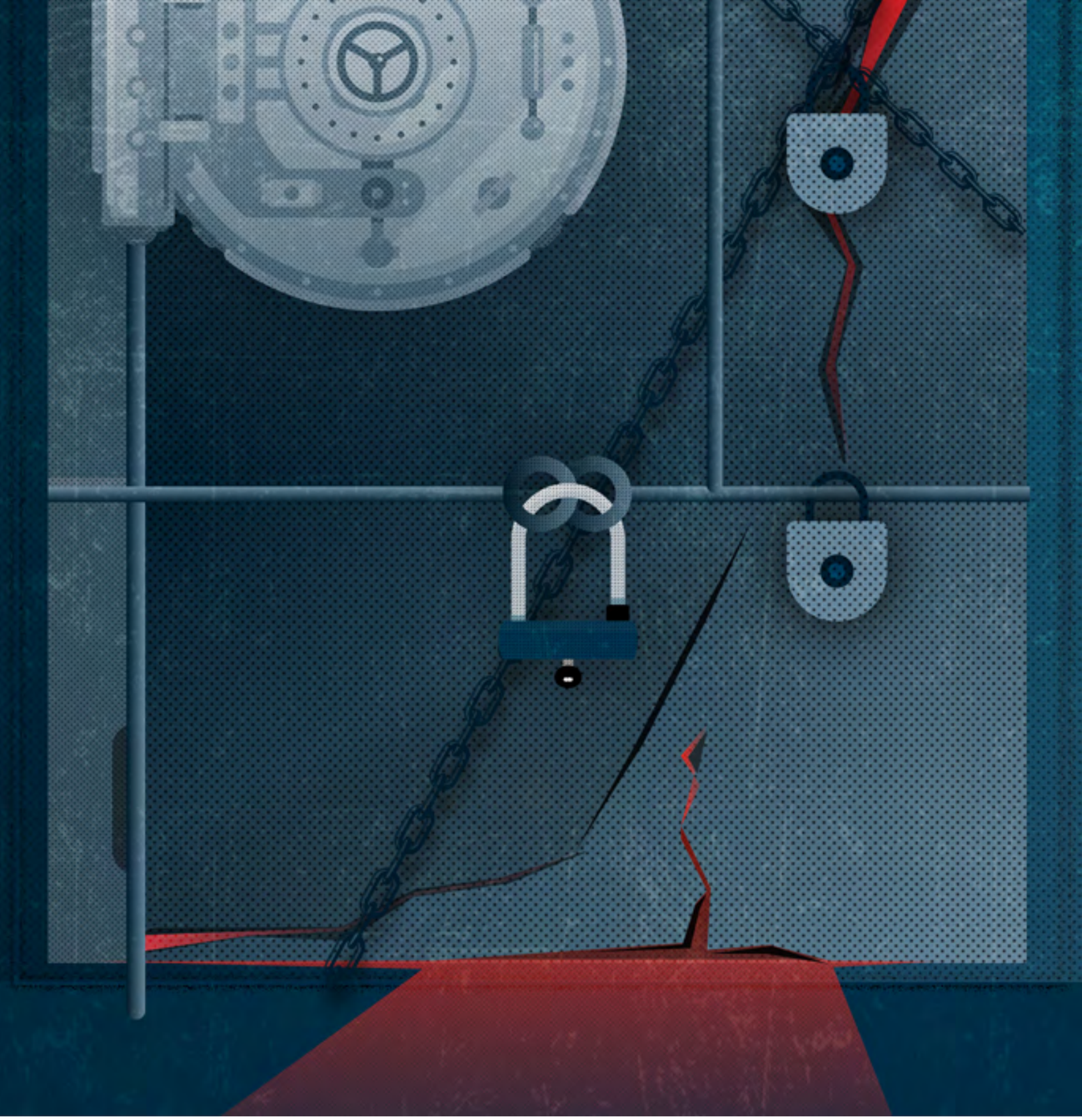
HOW TO RE-EVALUATE YOUR BREACH PROTECTION

AMERICAN TECHNOLOGY CLOUD, LLC

DO YOU DEPLOY SECURITY PRODUCTS TO PROTECT YOUR ORGANIZATION FROM BREACHES?

IF SO, IT'S IMPORTANT FOR YOU TO KNOW THERE AREN'T ANY CRITICAL GAPS IN YOUR SECURITY STACK.

For many organizations, breach protection is about placing and piecing together standard antivirus and firewall with an additional product, dedicated to addressing advanced threats. This common practice is likely to include unaddressed security risks.



IF YOU CONSIDER DATA BREACHES A CRITICAL RISK, YOU SHOULD SHIFT FROM A PRODUCT-ORIENTED TO PROTECTION-ORIENTED MINDSET.

Start with better understanding the types of attacks you face and check if you're covered.

THREE TYPES OF CYBER ATTACKS

Hit and Run

Attacker reaches its objective by one-time malware execution. Once objective is accomplished, the damage is done.

Examples: ransomware, wipeware, phishing sites.

Hit and Stay

Attacker seeks to maintain persistence on the endpoint to abuse its resources or data.

Examples: crypto-miners, banking trojans (or any other password stealing malware).

Hit and Expand

The attacker's goal is to access and exfiltrate data, or perform a supply chain attack. These attacks start with initial endpoint compromise, followed by a long lasting presence in the environment.

Examples: APT, insiders, advanced cyber crimes.

SECURITY TECHNOLOGIES VS. ATTACK TYPES

Each attack type can be detected and blocked by the anomalies it generates in either **file structure, process behavior, network traffic or user activity**. Full breach protection entails your security stack having the ability to prevent and detect threats across all of them.

	EDR\EPP		Network Analytics	UEBA
	File Structure	Process Behavior	Network Traffic	User Activity
Hit and Run	●	●	○	○
Hit and Stay	◐	◐	◐	○
Hit and Expand	◐	◐	◐	◐

● Full Protection ◐ Partial Protection ○ No Protection

THREE APPROACHES TO CONSIDER

Single Product

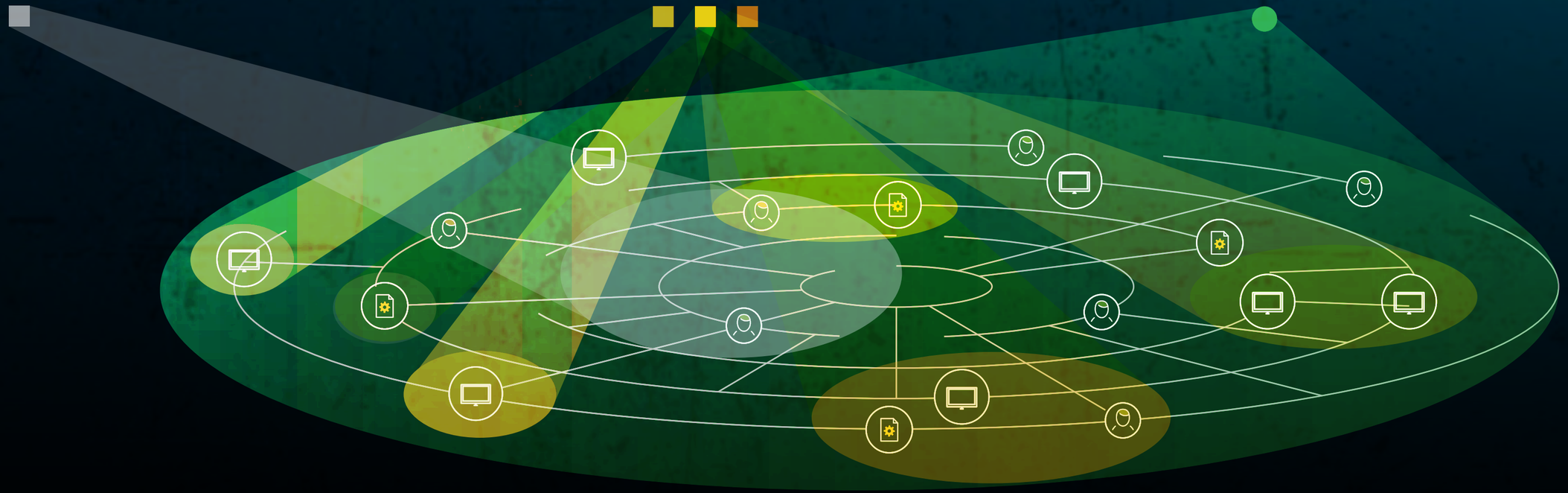
Choose a single advanced security product (EDR, network analytics or UEBA). It makes sense from a budget perspective but leaves you exposed to at least one attack type.

Multi Product

Deploy multiple products and manually integrate them to protect from all attack types. This is a costly path that will require a highly skilled workforce to deploy and operate.

Integrated Platform

Use a platform that natively integrates all breach protection functionalities either alongside or as a replacement to your AV. You gain protection from all three attack types with easy deployment and simple operation.



KEY BREACH PROTECTION CONSIDERATIONS

1 | Deployment

The most essential requirement from a security product is to be in place. Practice shows that installation issues result in partial deployment leaving parts of your environment exposed.

This applies equally both to evaluating existing products, as well as to purchasing a new one. If you have endpoint protection, are there agents installed on all your endpoints? If it's a network analytic tool, does it cover all portions of your network?

2 | Attack Coverage

The purpose of security products is to protect from attacks, which vary in means and ends. Attackers seek weak points in your protection stack and it's up to you to reduce them as much as possible.

Check the protection level your current products provide from each of the three attack types. They might score high against one, but fail against the other. For example, a first class NGAV would dramatically decrease your exposure to Hit and Run\Stay attacks, but would offer little to zero protection against Hit and Expand scenarios.

KEY BREACH PROTECTION CONSIDERATIONS

3 | Management

Breach protection involves multiple workflows: proactive IT hygiene and vulnerability management, triage and prioritize alerts, respond to active attacks and orchestrate the recovery process.

Easy and intuitive management of all these functionalities is a must. The competency bar is straightforward – if efficient day-to-day operation of these workflows is beyond the skill of your in-house team, then you're not secured.

4 | Expertise

At the end of the day, advanced attacks call for advanced skills. You don't need – and typically can't afford – employing such skills as part of your team.

This need arises regardless of the products you have in place and is especially required when facing a Hit and Expand attack. Skilled analysts are a must to unveil defense-evading malicious presences.

THE ULTIMATE BREACH PROTECTION CHECKLIST

		Considerations
DEPLOYMENT	Time to deploy	How long does it take for your protection to be up and running?
	Ease of deployment	Are there any issues, such as network configurations or software on the endpoints that act as deployment blockers?
	Full invironment coverage	Is your entire environment covered across all operating systems and network portions?
	Infrastructure flexibility	Can you deploy across both on-prem and cloud workloads?
THREAT COVERAGE	Hit and Run	Are you protected against zero-day malware, exploits and fileless attacks?
	Hit & Stay	Do you have the ability to detect C2C communication and connection to malicious site?
	Hit & Expand	Can you disclose malicious presence and activity such as reconnaissance, credential theft, lateral movement, data access and data exfiltration?
MANAGEMENT	Integrated interface	Can you manage all breach protection workflows from a single interface?
	Operational simplicity	Can your current IT/security team efficiently manage daily breach protection operations?
EXPERTISE	Manual protection	Do you have the required skills at your disposal for response to active, advanced threats in your environment?

THE NEW, INTEGRATED SECURITY PLATFORM

When we think of breach protection, we tend to think about a complicated stack of multiple products pieced together, operated by a team of highly skilled analysts. Nowadays, it's the time for breach protection to become a commodity within reach for all organizations.

IMMEDIATE IMPACT

Organizations need the ability to instantly move from exposure to protection and totally remove deployment issues from the equation. The infrastructure level must become a transparent operational layer that requires zero maintenance efforts to enable all protection capabilities to operate.

AIRTIGHT PROTECTION

Multilayered protection across all attack surfaces is a must, regardless of the attack's type and vector. The protection functionalities must span all aspects of breach protection, from proactive IT hygiene, through active threat prevention and detection, to full response orchestration.

ABSOLUTE SIMPLICITY

The required skill to efficiently manage the day-to-day operations must be within reach of the common IT/security workforce, overcoming the infamous 'security skills shortage.' Only what is simple can provide sustainable protection.

ABOUT CYBEROPS

CyberOps provides organizations with the ability to protect themselves from breaches with an integrated platform that brings together environment visibility, attack protection and response orchestration in single interface, instant to deploy and simple to manage, regardless of security team size and skills. To learn more visit **www.transmosis.com/cyberops**