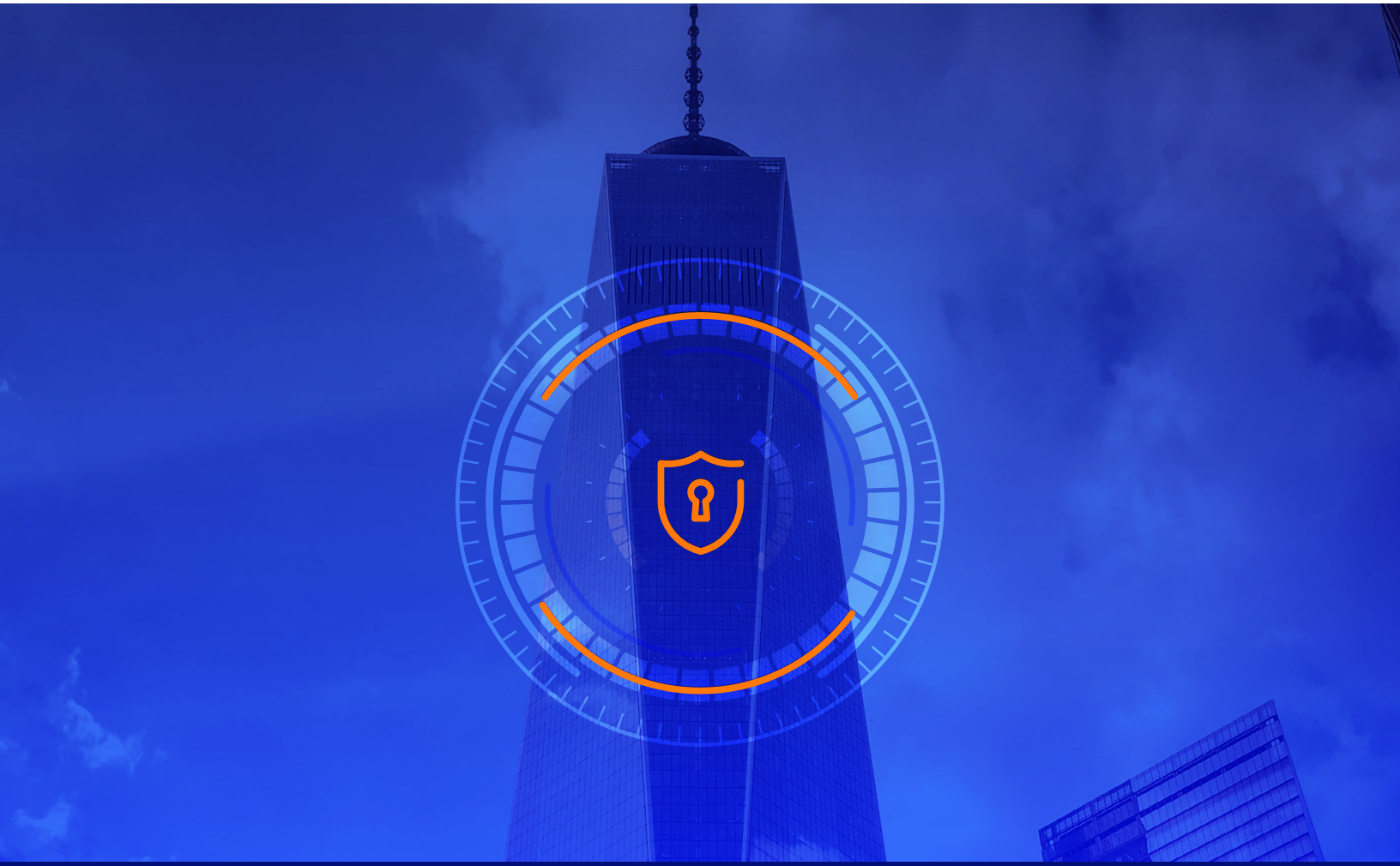
affirmlogic

CYBER

Deploy next generation defense, now.

How Hyperion is a force multiplier for cyber defense.

New vulnerabilities, threats, and actors require next-gen defenses by companies in top-targeted industries. The stakes are too high to only defend against known attacks.



1660 International Drive | Suite 600 | McLean VA 22102

www.affirmlogic.com

Every thirty-nine seconds an American computer system is attacked.[1] Corporations spend billions every year to defend themselves from these aggressions. Governments race to promote cyber as a risk-agenda topic; the White House even established a "President's Cup" challenge to spur competition among top cyber personnel.[2] Yet, as Verizon reports, cybercriminal attacks are growing more regular, organized, and systemic.[3]

To keep up, public and private institutions deploy a range of security products, including firewalls; SIEM; user behavior analytics; security orchestration, automation, and response (SOAR); endpoint detection; data loss prevention (DLP); and email and web filters.[4]

Despite these measures, attackers are gaining the advantage.

According to one report, eight critical US government agencies, including the Department of Homeland Security and the Social Security Administration, are unprepared for cyber attacks.[5] Nation-state hackers from Russia, China, and Iran were recently implicated in attacks on targets ranging from the Democratic National Committee to the Ukrainian electrical grid.

By 2021, By 2021, the annual global cost of cyber crime is expected to reach $6 trillion.[6] IBM estimates the average cost of a breach to be $3.86 million. The average time to identify and contain a breach: six months. (See Figure 1)

Global	2020	2019
Average cost of a breach	$3.86M	$3.92M
Average time to identify & contain	280 days	279 days
Security automation deployed	59% of orgs.	52% of orgs.
Highest average cost industry	Healthcare	Healthcare

Cost of a Data Breach Report 2020 IBM Security

FIGURE 1

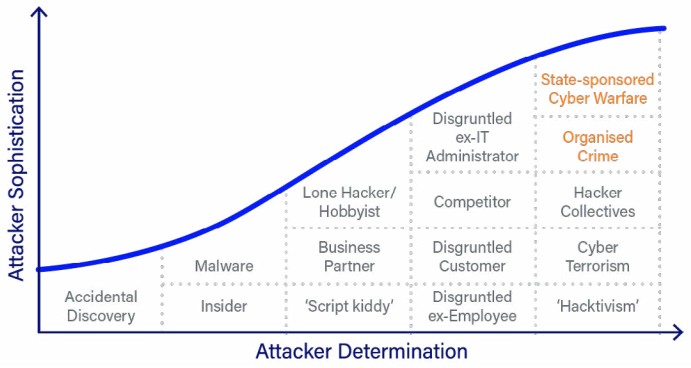
For public companies, the effects are more severe. An *Audit Analytics* survey of 639 public companies from 2011 to 2020 finds the cost of a breach to be $116 million.[7] Ransomware was responsible for nearly $12 billion in losses last year. In 2018, 1.2 billion consumers were victimized by cyber crime, making it the most pervasive illegal activity on the planet.[8]

The evolution of cyber attacks.

The increasing sophistication and devastation of attacks are byproducts of the cyber arms race. Over the years, as malicious attacks increased, defenses improved. As defenses tightened, attacks advanced.

This evolution is a function of global mega-trends. Rapid innovation and easy access to cyber attack toolkits means even criminals with limited technical sophistication have tools for their ambitions. Emerging IoT–with billions of connected devices and systems–expands the cyber playbook. Weaponized artificial intelligence and machine learning invite attacks at a never-before-seen scale.[9] The velocity of data sharing gives malicious parties easy access to the data they need to steal, manipulate, or destroy.

Check Point Software highlights how resourceful the cyber crime market has become. They observe:[10]



- Cyber crime has its own social networks with escrow services.
- Malware can now be licensed (and includes tech support).
- Botnets are available for per hour rental.
- Pay-for-play malware infection services to easily create botnets are flourishing.
- A lively market for zero-day exploits (unknown vulnerabilities) exists.

Bad actors focus where it's most profitable. Consider the rise of social engineering attacks surrounding the coronavirus crisis and remote workers who possess valuable assets like personal, financial, and corporate data. In a recent PwC simulated phishing attack on mid- to large-size financial institutions, 70% of phishing emails were delivered to their targets, and 7% of recipients clicked on the malicious link.[11]

Nation-states and the cyber arms race.

No groups play a more significant role in the growth of cyber crime than hostile nation-states. The evolution of attacks originating from state actors–including all varieties of API abuse, application DDoS, ransomware, and platform misuse to steal, radicalize, disrupt, and project national power–make prior forms of pranks and low-tech phishing the least of an enterprise's concerns. In 2018, the US issued public warnings about Russian attempts to target suppliers of electric grid operators, resurrecting references to a new cold war.[12]

Forbes notes how a cyber attack is "[…] best understood not as an end in itself, but as a potentially powerful means to a wide variety of political, military, and economic goals." [13]

"Serious cyber attacks are unlikely to be motiveless," shares Martin Libicki, Senior Scientist at RAND Corp. "Countries carry them out to achieve certain ends, which tend to reflect their broader strategic goals […]" Reports of a retaliatory digital strike to

disable maritime operations in Iran by the United States, if true, reinforce this.[14]

The theater of battle is now digital, and covert assaults are the way forward. Although largely unseen by the public, the list of casualties from cyber attacks–including some of the biggest names in technology, financial services, media, healthcare, defense, and government–is lengthy.

Moving beyond standard defenses.

Enterprises commonly deploy a layered approach to security. This architecture, dubbed "defense-in-depth" (DiD), involves layering a variety of defensive mechanisms to protect data and thwart intrusion.

Like a medieval castle, where drawbridges, moats, and ramparts foiled unwanted visitors, DiD applies a concentric series of security elements.[15]
These include:

- Network security controls (e.g., firewalls and intrusion protection systems)
- Antivirus software
- Data integrity solutions
- Intrusion detection

Companies that inventory their endpoints and connected applications, identify weaknesses in traditional signature-based tools, and scan for compromises are likely to stay buttoned-up against most threats.

When generic attacks do occur, companies can use their human resources and commercial technology to identify and rebuff them.

But entities that operate critical infrastructure or possess data and intelligence most attractive to cyber criminals, need better protection.
Protecting only against common breaches and taking days or weeks to understand the intent of an attack or the nature of exposure, isn't enough.

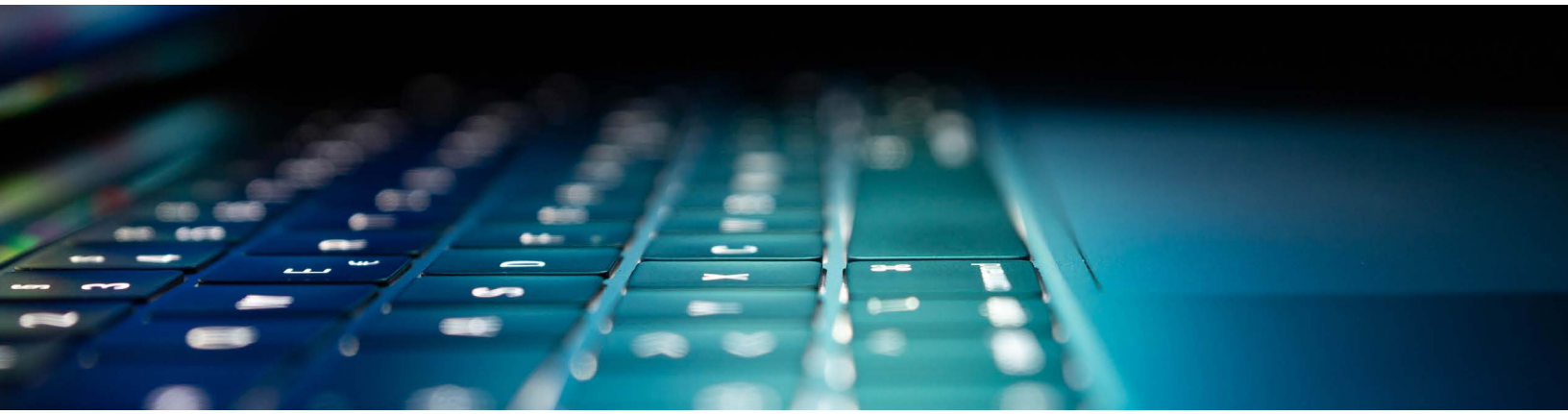
These organizations are targeted with sophisticated and purpose-built software originating from well-resourced criminal groups or sovereigns–true enterprise grade cybercrime.

Key industries in the crosshairs.

IBM's Cyber Security Intelligence Index highlights health care and financial services as top targets for cyber attacks.[16] Boston Consulting Group finds that financial institutions are 300 times more likely to be attacked than companies in other sectors.[17] Mastercard reports nearly 500,000 intrusion attempts per day–up 70% from a year ago.[18]

Further, 75% of all healthcare organizations will report a cyber attack in their lifetime.[19] CDNetworks finds that government agencies are also under siege; ransomware affecting 911 systems, utility management, and Click2Gov–a public sector web payment portal– emerged in the last year alone.[20]

Local, state, and federal agencies saw a 1,300% increase in information security incidents from 2006 to 2015.



These sectors are most susceptible for three distinct reasons –

- They own or operate something that cybercriminals can steal and monetize. Examples: bank or financial records, personal information, national security intelligence, and IP or other trade data.
- They have patchwork deployments of cybersecurity tools and applications that are sometimes outdated leaving them vulnerable to the latest attack vectors.
- They employ unsuspecting white collar workers representing millions of desktop computers with network access points.

The particular financial, regulatory, reputational, and security risks faced by organizations in these markets require a new defensive mindset.

"Companies that are victims of random attacks have one set of concerns. But organizations in these highly-targeted industries must think beyond the basics," guides Larry Roshfeld, CEO at AffirmLogic. "If your organization is specifically targeted there are new worries: *who's the attacker, what are they after, are they already in my system, and are there existing damages from a previous attack?* Understanding whether a suspicious file is good or bad, or simply detecting intrusion, isn't enough. Timely analysis enables action."
Because attack specifics vary based on threat actors' motivations, cyberdefense and risk management must be tuned specifically for high-potential targets.

Reimagining cyber defense.

For AffirmLogic's Roshfeld, modernizing defenses must be a priority, but not at the expense of operating effectively. "Security accommodations that sub-optimize for connectivity, for example, may not be worth the trade-off. If you're protected, but your stakeholders can't communicate, are you better off?"

Enter HYPERION

Market leaders in critical, highly-targeted industries need improved insight and faster visibility. They need to achieve this cost-effectively, without slowing internal operations – especially as they contend with well-resourced nation-state actors and cyber crime syndicates.

Hyperion, advanced malware detection software born out of Carnegie Mellon University research, delivers this.[21]

"Malware was becoming more sophisticated at hiding. We realized we had to go beyond traditional read-or-run solutions and instead, perform our analysis at the chip level, using advanced mathematical methods to compute software behavior," shares Rick Linger, AffirmLogic CTO and original Hyperion development team founder.

Hyperion's patented computational analysis engine is based on peer-reviewed research on mathematical

theory to ensure high levels of data precision. It provides visibility into malware by creating a computed representation of a sample's behavior and merging it with a structured version of its associated, disassembled code.

The approach works because it operates under a simple premise: malware must actually run to achieve its objectives. To Hyperion, it's simply more upon which to perform behavior computation – even if it's hidden, distributed, or obscured.[22]

Pillars of modern defense.

Hyperion's next-generation defense builds on three pillars: detecting, reverse engineering, and defending.

- **Detection**: Software with unknown behavior and security is most often behind major attacks. Classic syntactic scanning and dynamic execution are useful but insufficient to determine whether a coded behavior is malicious. Whether with zero-day or sleeper code, behavior computation can be used to detect malicious code, even if scattered across multiple functions.
- **Reverse Engineering**: Hyperion's automated reverse engineering is an essential part of a defense-in-depth strategy. Behavior computation pinpoints malicious content allowing cyber analysts to skip time-consuming investigations. In addition, it boosts levels of actionable intelligence.
- **Defense**: Old approaches can't sufficiently protect against new threat vectors. Even AI/ML based countermeasures (like cybersecurity correlation automation, or CSCA) fail to consistently identify new attacks because there is no pattern from which to learn . The generation and dissemination of Hyperion's unique, behavior-based signatures strengthen existing AV security suites and intrusion detection systems.

"Cost and time savings are pillars of a defense-in-depth strategy. Our approach automates the process of reverse engineering malicious software and documenting behaviors," guides Roshfeld.

> "Hyperion can do in four hours what takes a highly trained cybersecurity analyst about two weeks. The value isn't just in improved staff efficiency, it's in reducing exposure time prior to mounting their defense.

As consultancy Oliver Wyman reminds, antagonists will remain ahead unless more sophisticated cyber defense methods are implemented.[23] For widely targeted companies, these include solutions with comprehensive detection, response, reverse engineering, and countermeasure capabilities.

"There's nothing wrong with being protected 90% of the time," warns Roshfeld. "It's the other 10% you have to worry about."