CyberadAPT

RETHINKING CYBER SECURITY

Introduction

Advanced Persistent Threats (APTs) and advanced malware have been plaguing IT professionals for over a decade. During that time, the traditional cyber security vendor community has attempted to repurpose their legacy products and solutions, hoping to effectively eradicate the new attack tools and tactics. Unfortunately, their failure is front-page news almost daily around the world.

Meanwhile, governing bodies and boards have increasingly held C-Level staff accountable for failures to protect their investments. Knowledgeable and experienced people lost their jobs, even though they had faithfully deployed millions of dollars in the latest "best practice" technologies, tools, and processes.

As CIOs & CISOs struggle daily to fortify their multi-million dollar defenses, sophisticated attackers quietly continue to steal billions of dollars worth of intellectual property and other critical business information. The solutions in place are clearly not meeting the level of skill of the adversary. But who should be held responsible in the event of a breach? Those who miss the attack due to inadequate tools or those who decided which tools to use? Clearly, there is a gap.

IT IS TIME TO CHANGE THE CONVERSATION.

THE CHANGING ECO-SYSTEM

"As global threats evolve, so must cyber security solutions."

-Kirsten Bay, CEO Cyber adAPT®

According to a June 2014 report by the Center for Strategic and International Studies, crime involving computers and networks has cost the world economy more than $445 billion annually.

RETHINKING CYBER SECURITY

CHANGING THE BUSINESS CONVERSATION

As cyber security breaches continue to make headlines, an increasing amount of APTs, zero-day attacks and other advanced malware are born, raised, and launched on the Internet. Attacks on corporations, governments, and universities are increasing in quantity and quality. Some, such as those aimed at Target, Office Depot and JP Morgan Chase have become very public. As developers become more sophisticated in the methods they use to break into corporate networks, current security solutions struggle to keep up.

For over 25 years, the cyber product industry and, by extension, the commercial and government enterprise markets have been almost exclusively focused on cyber attack prevention. The perimeter form of defense has its roots in the military strategy of the 4th century A.D. Roman Army. It is based on the premise that putting up enough defenses on the border will discourage or prevent the enemy from attacking.

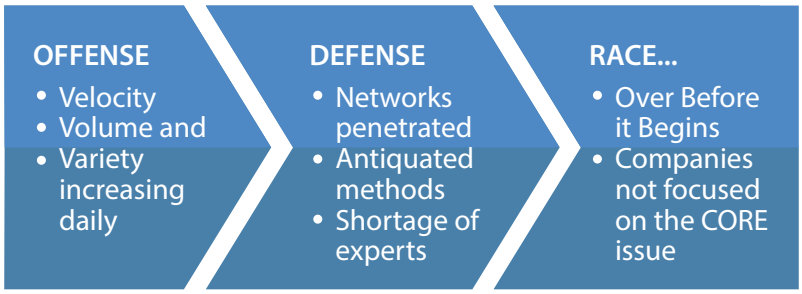
Vendors and customers alike have concluded in the last 12-18 months that prevention alone is not enough. Even with the latest technological evolution in the prevention playbook (such as payload analysis via sandboxing), it has become easy to circumvent this technology often by just reading the vendor instruction booklet.

The open market for the production, distribution, and maintenance of advanced malware is highly profitable and global. Developers are extremely proficient at developing new and innovative 'on ramps,' allowing them to get inside the network and to extricate confidential and private data. Once inside the network, they take their time and hide, ensuring that their malware movement remains untraceable. In the rare cases when malware is found and purged from the network, it has often already replicated and hidden itself in other areas of the network to continue its mission.

Typically, security analysts don't learn about a cyber attack for almost a year after the breach occurred.

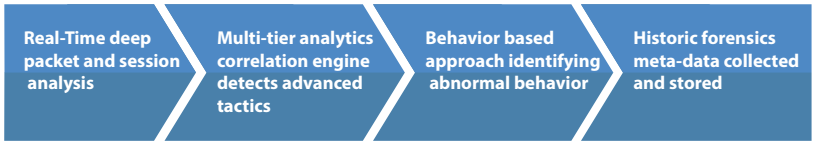
Shedding Light Where There Was Darkness Before

Attackers hide inside enterprise networks for months or even years before being discovered. There is universal acknowledgement that all major networks are already compromised in some way. The cyber security industry's current hardware and software platforms work exceptionally well against known threats. They are necessary but not sufficient in today's security threat landscape where attackers conceal themselves in dark places. The hacker or malware tactic stealthily crosses the perimeter, infiltrates a network, and hides. According to the 2014 Threat Report by Mandiant, the median number of days that threat groups are present on a victim's network before detection is 229 days. What those businesses are lacking is real-time detection and live analysis on the wire.



Most "behavior" based detection technologies today pertain to sandboxing the perimeter, rather than live behavior analysis of the traffic, which takes a long time and a lot of meta data to establish and properly evaluate. Cyber adAPT® observes and records typical host behaviors on the network first, in order to evaluate baseline behaviors so that it can detect substantive changes and spot abnormalities. This process can be effective only if it takes place over a long period of time.

Cyber adAPT® Breach Discovery Process:

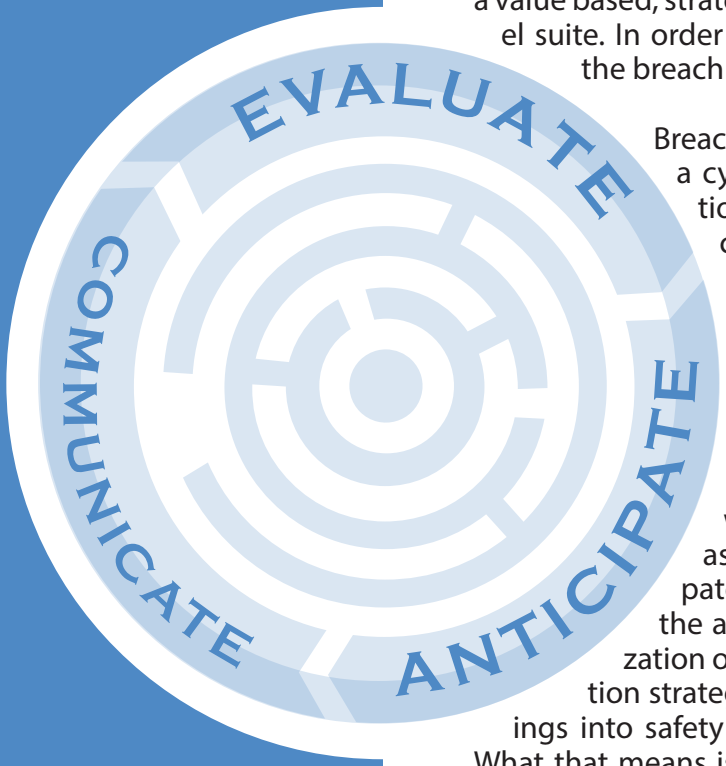


Prevention must be augmented with sophisticated signature-less detection technologies, tools, and processes that can find attacks in progress on an enterprise's networks. These detection methods must be able to "see" attacks developing over very long periods of time.

Completing an enterprise's cyber security portfolio by augmenting the perimeter protection with live detection cannot happen until a breach life cycle is properly understood by those in charge of securing the company's critical assets and communicated to the upper management. It will take the right tools and the right people to set policies and to guide strategic planning in order to make a real change.

Where Security Drives Business Value

Besides shifting from prevention to detection, building an effective corporate strategy to prevent a business from suffering major losses from an undetected attack asks for a different organizational approach. The CIOs and CISOs are no longer merely responsible for managing the network structure. Their engagement is vital on all levels, and they must be included in a value based, strategically oriented discussion with the C-Level suite. In order to achieve that, a deep understanding of the breach life cycle becomes critical.



Breaches can and do occur at multiple stages of a cyber security life cycle. Adequate preparation will require a balance of technology and corporate policy. It is a highly dynamic process that requires continuous risk evaluation of the business infrastructure, in order to determine the gaps that leave both the perimeter and the network vulnerable to penetration and exploitation. Knowing their level of corporate security is not enough. Those entrusted with protecting their company's critical assets must think ahead and learn to anticipate threats in order to remain a step ahead of the attacker. In order to achieve that, a prioritization of risk needs to be balanced with a remediation strategy, turning post- breach investigative findings into safety protocols in the event of a compromise. What that means is that security professionals must learn to create, emphasize, and communicate the context of the security's impact on the totality of the enterprise - a context that is bound to change and evolve. The process becomes a feedback loop of evaluating security risk profiles, anticipating threats, and communicating the impact so that effective prioritization can take place.

Even after security policy measures have been incorporated into the company's general plan, it will not ensure that its security risk profile has been maximally fortified until infrastructure gaps have been identified and proper solutions installed. Policy must match technology. This is where the conversation becomes a business continuity discussion that will ideally impact the company's corporate strategy not in part but as a whole.

Know Your Risks & Vulnerabilities

Plan Ahead

Remediate & Integrate

Security's Growing Impact

In light of devastating breaches in the financial sector over the recent months, particularly the JP Morgan Chase & Co. attack this summer, hundreds of financial firms are ramping up their cyber security spending. According to a survey conducted by the accounting and consulting firm Pricewaterhouse Coopers, the budgets will go up by approximately $2 billion over the next two years, representing a 10%-20% increase over the previous year. The Wall Street Journal reports, "The spending increases represent accelerated efforts to keep hackers out and a realization that previous efforts haven't been sufficient."

ADAPTING to Rapidly Changing Cyber Security Environment

The dynamically shifting threat landscape has required cyber security professionals to frequently adjust their methods to fortify their company risk profiles. For too long CIOs & CISOs have been stalled by thegranular IT aspect of security, which has prevented them from engaging in a value discussion with C-level executives. The potential impact cyber security level has on critical business assets needs to be reconsidered and re-evaluated. It often becomes evident, but only after it is already too late - either during or after a breach. Only by shifting from reactive to proactive planning can an enterprise's assets be saved.

Understanding the company's attack surface and the security's impact on the business can help prevent significant losses during and after a breach. This approach sets the stage for a pivotal discussion that sheds light on the significance of cyber security on the entirety of the business.

With new tools and levels of support to assess security risks that were not previously considered with antiquated tools, blind spots can be identified and removed, allowing corporate leaders to focus on building a holistic business strategy.

This can be achieved by:

- Identifying security components to ensure adequate protection,
- Pinpointing areas of breach's impact on the business, and
- Articulating security life cycles and their impact to business owners.

It will take the right tools and the right people to set policies and guide strategic planning to make a real change.

PUTTING IT ALL TOGETHER

In spite of the billions of dollars spent annually on security infrastructure, tools, systems and the professionals to manage them, sophisticated attackers continue to penetrate our networks, exfiltrate our most valuable assets, and cause substantial damage. If we continue down the path of investing time, money, and effort solely in our prevention strategies, the opponents will continue to defeat them, steal and damage our assets, resulting in the destruction of immense value across an enterprise's networks.

Savvy company C-Level executives know that security is not a stand-alone issue, but one that must be fully integrated into a company's long-term business strategy. Success depends on constantly adapting to the changing environment and embracing a full spectrum of cyber security solutions aimed at preventing attacks, detecting successful attacks, and responding quickly and effectively to prevent future attacks.

Kirsten Bay
President & CEO
Cyber adAPT®

Headquarters
337 Mirada Road, Second Floor
Half Moon Bay, CA 94019

Dallas Location
14755 Preston Road, Suite 405
Dallas, TX 75254

Chicago Location
135 Park Avenue, Suite 201A
Barrington, IL 60010

Email
info@cyberadapt.com