White Paper

A New Approach to Cybersecurity –

The Cyemptive Approach

May 8, 2021

The Current Cybersecurity Challenge

The technology industry is evolving very rapidly. New vulnerabilities are continually created as part of constant change. While companies are identifying and protecting against these vulnerabilities as fast as they can, there is always some level of "found but not yet solved" vulnerabilities. Also, as the industry has evolved to higher and higher levels of operational automation, hardware, operating systems and all processes running on them have needed hooks to allow the automation. This has also created new attack vectors at all levels in the stack.

The industry does not believe that anyone can be completely secure. While many cyber solutions claim they have solved a piece of security, no one is claiming that they can solve everything. Rather than closing the gap, offensive attacks have exponentially increased while defensive abilities have not evolved as quickly. The largest investments in the past few years have been in using Artificial Intelligence and Machine Learning to process through the complexity that is beyond human capability. These improvements are finding attacks that were impossible to stop historically, but the ability to detect something outside the norm requires data from an attack that is already happening or has not yet happened.

The Hardware Environment Is Enormous

There are hundreds of thousands of devices in the world: laptops, desktops, servers, cameras, sensors, phones, and more. Each device can expose itself to the network and the internet in many ways. The result is that our systems present countless potential attack surfaces. Each of those is exposed to millions of attacks a year. The odds are increasingly stacked against us.

To combat this challenge, we employ dozens of different security solutions, each of which requires separate management, and none of which understands how to talk to the others.

The Software Environment Is Even Bigger

The major operating systems and office applications have well over 50 million lines of code. Even devices like phones and firewalls can have millions of lines of code, all compromised in minutes by targeted hackers.

Each line of code represents a potential security vulnerability. There was a time when these vulnerabilities were found by knowledgeable hackers with skill and talent to seek them out. Today's hackers simply use brute force. They employ machine-driven attacks that can attempt thousands of exploits per second, essentially testing each line of code. New hacks are found and exploited thousands of times a day, leaving static scanning companies behind. The software vendors are left even further behind, with mountains of holes to fill.

Human Expertise Can't Keep Up

Security experts are hard to find, and they are expensive when we can find them. Even if we could recruit, retain, and afford all the security experts we require, it won't be enough.

The most experienced humans can only identify, isolate, and repair a few attacks a day. Machine-driven attacks are coming thousands of times a second. Human interaction cannot scale to the level of machine-driven attacks happening every day. The automation required to keep up with machine-driven attacks also creates new vulnerabilities to be exploited.

Attackers Have Time on Their Side

According to Verizon's Data Breach Investigation Report in 2019, in over 60% of breaches data is stolen in minutes or hours; however, 56% of breaches aren't discovered for months or longer. Bad actors can have many months of dwell time within a network to exfiltrate data, embed malware, or plan their attacks. **Attackers have a distinct time advantage.**

They use the scale of the environment, the complexity of the software, and the ineffectiveness of the defense to their advantage. They know they can operate with impunity and take their time. They find and steal information, trade secrets, and intellectual property at their leisure. Or worse, implant viruses to live in networks for months or years without detection.

All of this leaves us vulnerable to a wide range of security threat scenarios.

Cyemptive's Different Approach

Cyemptive has patented an innovative approach but it starts with a completely new mindset. The cyber industry historically has relied on preventing known attacks, scanning infrastructure and applications for signatures of these exploits, and knowing how to stop them. There has been a huge investment in threat intelligence to understand these known exploits and to close the gap in the time it takes between when they are first found, the time when there is a solution developed to block the new exploit, and the time that it takes to deploy this new solution so the new exploit can be stopped. More recently companies have leveraged the branch of Artificial Intelligence called Machine Learning to close these gaps faster and with more efficiency than having humans close the gaps. Significant progress has been made, but the mindset hasn't materially changed from one where we need to protect against known exploits.

Cyemptive's approach utilizes a unique combination of technologies that does not seek to identify and stay ahead of known threats, but rather uses our patented technology to "Preemptively" stop all attacks regardless of being known or unknown.

Cyemptive has built protections leveraging multiple automated defensive technologies working together. The combination of Cyemptive solutions; CyberSlice, CyberScan, and CyberSensor, makes environments nearly impenetrable.

Cyemptive's Preemptive Protection

Traditional approaches to cyber security involve evaluating where a company has the most risk since they can't protect everything, putting protections in place to mitigate that risk, and then investing in the ability to detect where the protections are bypassed. They also invest in the ability to respond and recover after they are compromised to minimize the risk.

A successful attack starts with finding a vulnerability and then exploiting that vulnerability. Cyemptive assumes that attacks could be happening at any moment, and our zero-trust patented technology preempts any attempted attack before they can succeed by combining the entire Cyemptive solution stack end-to-end, and following Zero Trust blueprints, to enable the preemptive protection.

Cyemptive's Technology

The four fundamental technologies are;

1. **CyberSlice**© : rapidly and automatically isolates cyberattacks, providing protection that is faster and far more effective than currently existing systems.
2. **CyberScan:** Cyemptive's CyberScan technology is a revolutionary scanning capability that detects tampering of data based on the state of files in your environment. This along with other Cyemptive products allows us to make claims that no other security provider will do.
3. **CyberSensor**: Cyemptive's sensor technology introduces a new wave of technologies based on its "Cyemptive State" where it intelligently enables awareness faster than other technologies found in the marketplace today. These unique sensors help the rest of the Cyemptive technologies amplify the effectiveness of providing a robust results-driven response to cyber. CyberSensor is foundational to assisting triggers within the stack and shortening the detection time and improving problematic accuracy.
4. **CyberSLA:** We are the only cybersecurity company that stands behind the security we provide with financial guarantees. Cyemptive service level agreement performance measures provide new, revolutionary seconds-based performance guarantees for our customers.

Summary

Cyemptive brings a different approach to solving the many cybersecurity threats we face today. The solutions are results-driven and are extremely disruptive and innovative by offering SLAs in seconds or minutes against Zero Day attacks and other bad actors. We employ world-leading security architects, top ethical hackers, and many other employees with expertise other companies do not have.

Corporations and organizations will require solutions that can grow as the attacks gain sophistication. Cyemptive has built protections leveraging multiple automated defense techniques, deep zero-day intelligence, revolutionary honeypot sensors, and revolutionary Cyemptive State technologies working together. The combination of Cyemptive solution technologies, CyberSlice, CyberScan, CyberSLA and CyberSensor, makes environments nearly impenetrable.