Turning Cyberattack PREVENTION into a SecOps Advantage

How To Stop Wasting Resources and Return Focus To Critical IT Projects
Introduction

“Nearly half of the IT team’s resources were being deployed to chase alerts. At the same time, their AV solution provider’s reaction time to zero-day and polymorphic threats continued to lag due to their signature-based model.” —From a Cylance Case Study on the challenges faced by a nationwide healthcare provider

Blind spots. Whether driving or managing an organization, we all have them. When considered in a business context, the existence of a blind spot can be a costly price to pay for the lack of visibility into the right way to deal with IT security problems and cyberthreats. Fixing the problem seems like the biggest obstacle, but sometimes embracing a new, more effective way to solve the problem can be the biggest challenge.

One such problem identified by both government and commercial organizations is the lack of qualified SecOps human resources and its impact on an IT organization’s ability to effectively combat the advanced landscape of cyberthreats while still delivering the IT support and critical projects the organization truly needs.

Another problem identified by government and commercial organizations was cited in a February 2016 Boston Globe article, which stated, “Cyberattacks increased by 48% in 2014, according to the accounting and consulting firm PwC, and are expected to increase further as devices from phones to appliances to cars become connected to the Internet.”

When you take both of these problems into consideration with an understanding that an overwhelming number of government and commercial organizations still rely on outdated, signature-based antivirus solutions that rely on manually intensive detect and response approaches, it is easy to see why so many organizations suffer from a shortage of IT resources.

Unfortunately, these organizations have not yet realized that these problems have already been solved using technology. Through advanced malware and virus prevention based on artificial intelligence and machine learning, organizations around the globe have the ability to free up these IT resources and refocus them back on critical IT projects.

A Congressional blog stated in April 2015 that “conventional approaches to cybersecurity training and certification are not keeping pace with the reality of today’s fast-changing and complex technology landscape.” What happens when organizations rethink the problem? Is it a talent problem or a technology problem? And what happens to your SecOps strategy when you realize you’re fighting the wrong battle?

What Happens When Organizations PREVENT Instead of Detect?

In a study by KPMG, “Cybersecurity: a failure of imagination “by CEOs,” researchers found that “organizations need to invest in the right tools… They need visibility first and foremost, to know if they are being attacked. Without visibility it’s impossible to identify holes in the security arsenal and weaknesses in infrastructure. There are organizations that have been compromised for years before they discover the damage.”

A select number of IT organizations and CISOs have embraced these tools in the form of advanced malware prevention solutions. As a result, their conversations about tech talent shortages and incident response have transformed into strategic discussions about increased visibility, efficient...
incident qualification, and the improved performance of their teams. The paradigm shift occurred when they began to focus on one critical factor:

**Behavioral, Anomaly-Based Threat PREVENTION**

In February 2016, Fortune Magazine featured an article titled, “Why Cybersecurity Isn’t So Complicated”. The writer’s recommendation was part of a postmortem of the 2015 breaches at the U.S. Government’s Office of Personnel Management: “Instead of waiting until there’s been an attack and then cleaning it up, we need to shift our angle of vision and our attention to the source of the attacks. This requires that we shift our focus from breach discovery and incident response, to anticipation and prevention. In other words, our security efforts need to work more like a bodyguard and less like a police force. If we can catch threats while they’re still just threats, we’ll have far fewer incidents to explain and apologize for.”

These acclaimed ‘bodyguard’ systems are available today and harness the power of mathematical algorithms to learn the behaviors and tendencies of cybercriminals. Based on that learning, they detect and prevent malware in a way that proactively quarantines potential threats BEFORE they execute and alerts SecOps teams to only those incidents that pose a real threat such as zero-day attacks.

**The Payoff: A SecOps Advantage**

**What if there was a way to double the productivity of your IT resources?**

By deploying a product that stops malware and advanced persistent threats BEFORE they execute, your IT resources will be free from re-imaging computers that have fallen prey to cybercriminals as well as the devastating impact on your systems caused by users clicking on things they shouldn’t. Your IT resources will be free from a continual reactionary posture and having to run from user to user, trying to stop breaches after they have already occurred.

1. **Deprioritization of False Positives** Rather than concentrating on detection and response and accepting the premise that data breaches are inevitable, SecOps teams now have the ability to focus on developing a prevention paradigm. This is a significant shift for those organizations mired in the day-to-day reactionary model that drains resources and reduces talent to nothing more than guardians of a broken system.

2. **Prioritization on Strategic Threat Assessments** The transformation from a reactive to a preventive approach gives SecOps teams the capability to proactively identify threat vectors and new threat actors, dramatically minimizing the impact of what would, in many IT organizations, be a talent shortfall.

3. **Increased HR Efficiency** The recruiting and hiring of high-performance and skilled SecOps resources is important to any organization. However, the need for on-demand cybersecurity specialists is significantly reduced through a solution that is not dependent upon round-the-clock monitoring.

4. **Cost Savings and Increased Profitability** Efficiencies in HR operations and SecOps teams create a leaner organization driven by improvements in productivity and initiatives that support strategic growth. With a solution that is transparent to the end-user, departments enterprise-wide face fewer incident-related disruptions.

5. **Metrics That Matter** An IT organization that was once focused on transactional performance (e.g., How many viruses were quarantined?) is now equipped to quantify the impact of cyberthreat prevention on the overall security, efficiency, and profitability of the company.

---

**The Anatomy of a SecOps Organization**

**Signature-Based Cyberthreat Prevention**

- 50% of resources chasing all alerts and responding to incidents.
- 50% of resources managing all other initiatives.

**Anomaly-Based Cyberthreat Prevention**

With a solution in place that qualifies alerts and reduces the need for 24/7 monitoring, resources are doubled to handle other initiatives.

* % improvement based on Cylance client testimonials
The Burden on IT and HR Is Growing
By continuing to rely on outdated detect and respond antivirus technology, organizations are putting unnecessary strain on their IT and HR departments as they fight a battle that simply CANNOT be won without the introduction of advanced antivirus and anti-malware technology that eliminates threats BEFORE they ever occur.

The Cost of Traditional Antivirus to IT and HR

Specialists
- The job description is different for each company
- Educational requirements and standards differ
- Salaries for specialists can drain resources
- Specialists may be so specialized that they are unable to contribute to other initiatives within an IT organization

Human Resources
- The hiring of cybersecurity specialists has become an HR and recruiting burden
- HR resources are not always fully educated about the skillset required to resolve critical cybersecurity problems
- Competition is fierce
- Corporate HR procedures, based on educational qualifications and other restrictions, often rule out those who could contribute

Retention
- Within this highly competitive recruiting environment, the loss of a cybersecurity specialist to another opportunity puts a traditional IT organization at significant risk
- HR teams are forced to interact with cybersecurity communities and teams on their terms to ensure full engagement

Resources
- When SecOps are focused on 24/7 detection and response of every cyberthreat, significant resources are required to track and monitor incidents
- When SecOps resources are deployed only for tracking, monitoring and response purposes, other strategic IT initiatives take a back seat
- The current strategy of most IT organizations is to deploy additional resources to track and respond to the growing number of cyberattacks
- Existing IT resources assigned to more strategic IT initiatives are often migrated into the SecOps team to address urgent malware threat detection and response needs

Cylance: Solutions for Every Step in the Kill Chain
All cyberattacks are planned and delivered in nearly the same manner, seldom straying from a high-level process map known as the ‘Cyber Kill Chain’. The only variable is the amount of resources cybercriminals spend on the different stages of an attack. No matter where your problem lies on the cyberattack spectrum, Cylance stops malicious files BEFORE they can ever execute.

What Makes Cylance Different?
Most endpoint protection platform (EPP) providers are seeking to do one thing: remediate a threat. The concept of remediation implies one important consideration — the reality that a threat has already taken place. Certainly, there are impressive dashboards designed to help IT organizations and CISOs control active cybersecurity events. However, they do not take into consideration several critical dynamics within most industries:

- A remediation-dependent system relies upon the management of highly trained IT professionals who can monitor and respond on a 24/7 basis. This can be a challenge for resource-constrained support organizations.
- Valuable time is lost and financial resources consumed while system analysts research events and follow protocols to remediate.
- Zero-day vulnerabilities often go unaddressed.

In February 2016, Gartner, Inc. reported that by 2018, 60% of EPPs will restrict executables that have not been preinspected for security and privacy risks, up from 22%. The stage has been set for those providers innovating with disruptive solutions that can detect a growing number of variant threats before they happen while minimizing the endpoint and network IT management requirement. Utilizing a revolutionary artificial intelligence agent, Cylance’s solutions and services are designed to proactively prevent the execution of advanced persistent threats and malware.

Key Product and Service Strengths
- Proactively detects new variants and repacked versions of existing malware
- Delivers a minimal impact on networks and endpoints (continues to work with less than 1% of CPU memory and loss of Internet connectivity)
- Offers a cloud-based management console without requiring cloud-based detection
- Generates static file assessment reporting for learning across customers and quarantines
- Reach expands to OEMs who can utilize our solutions to secure embedded systems
- Supports Microsoft Windows® and Mac® devices; Linux® available soon
Industry Response

Gartner recognized Cylance as a Visionary in its 2017 EPP Magic Quadrant. Cylance believes this is because we are one of the fastest-growing companies in the history of cybersecurity and provide an innovative new approach that replaces traditional signatures found in traditional antivirus products.

Cylance technology is currently deployed on over six million endpoints and protects over 1,000 enterprise clients worldwide, including Fortune 100 organizations and government institutions.

Take the Next Step: Prevention

To begin a discussion or for further information on applying artificial intelligence, algorithmic science and machine learning to cybersecurity, please contact:

Chris Coulter
Email: ccoulter@cylance.com
Phone: +1-877-973-3336

Contact Information

To learn more about Cylance, its projects and events, please visit www.cylance.com.

Cylance
+1-877-973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700
Irvine, CA 92612

https://www.youtube.com/user/CylanceInc
https://www.linkedin.com/company/cylanceinc
https://www.facebook.com/CylanceInc
https://twitter.com/cylanceinc