WHITE PAPER

McAfee
Together is power.

Cybersecurity success requires a change of mind.

A platform approach reduces risk and speeds implementation and integration.

WHITE PAPER

Cybersecurity success requires a change of mind.

A platform approach reduces risk and speeds implementation and integration.

Cybersecurity strategy has arrived at the popular definition of insanity: do more of the same and expect a different outcome. That is exactly how the majority of organizations today attempt to protect their data, infrastructure, and other assets from cyberattacks. With each new attack, they buy the latest security widget and add layer after layer to their defenses, knowing full well they have neither the time nor the staff to deploy and configure yet another product or solution. They are using an outdated strategy–one that doesn't work in today's connected world, where the threat landscape changes overnight.

Making substantial improvements in cybersecurity requires a new way of thinking as well as a new way of doing things.

Although IT professionals spend more money every year to strengthen their defenses, things just keep getting worse. IDC predicts that spending on security solutions will accelerate over the next few years, achieving a compound annual growth rate (CAGR) of 8.7% through 2020.[1] Yet, despite increasing investments in security solutions, the number of cybersecurity threats and successful cyberattacks continues to grow.

Between 2006 and 2016, the average number of daily cyber threats grew from 25 to more than 400,000—about 300 per minute. New malware was up 60%, targeted attacks increased 30%, and cyber criminals were stealing more than a billion personal records every year. Even worse, in 2016 U.S. companies and government agencies experienced a 40% increase in data breaches over the previous year,[2] according to the Identity Theft Resource Center. And those are just the ones we know about. Many data breaches go undiscovered or underreported.

So with cyber threats growing exponentially and data breaches increasing at least 40 percent in a single year, the majority of U.S. organizations plan to invest even more money in the failed strategy that led to those unacceptable results.

Clearly, what you are doing isn't working.

At McAfee, we think the crux of the problem is an entrenched mindset that permeates the industry. In a recent McAfee research study with 500 IT and security professionals, 60 percent said they believe in purchasing best-of-breed security solutions within the security domains under their responsibility—even if it requires multiple vendors to sustain that security strategy.[3] And they cling to this belief, despite growing evidence that

their layered approach isn't making their organizations more secure. Making substantial improvements in cybersecurity requires a new way of thinking as well as a new way of doing things. You and other IT and security professionals must put aside the outdated strategy you've been using and embrace an integrated, open-platform approach that allows you to deploy security solutions faster, extend their effective life, and coordinate all aspects of security from endpoint to cloud.

The traditional approach to cybersecurity is pretty straightforward. A new threat emerges, over a new medium, and the security team discovers the organization may be vulnerable. With great urgency, the team escalates the issue to management and drives home the risk of making headlines as the latest victim of a serious data breach. To the extent the security professionals are able to convey the danger, they motivate management to fund a new cybersecurity investment to combat this new threat.

So now the security team owns a new defensive widget designed specifically for the new threat. All too often, however, the new technology sits on a shelf or ends up deployed in learning mode as the team works out how to tune and configure it. The cycle frequently gets stuck right there, with the new widget partially deployed and never optimized. This best-of-breed strategy of obtaining the latest "silver bullet" technology against the current threats, which is firmly entrenched in many organizations, succeeds only when the security team is well-staffed and has a proven method for rapidly deploying and optimizing new tools. Most don't.

This approach is similar to the defense-in-depth strategy that dates back to medieval times, when castles were built to withstand attacks at many different points. An enemy army first had to cross a moat, fight its way through a fence of sharpened stakes, and scale the steep outer walls, all under a lethal barrage of arrows. After that, enemy soldiers still had to get past another series of deadly obstacles before reaching the castle keep, where monarchs secured the kingdom's most precious assets.

> "We will bankrupt ourselves in the vain search for absolute security."
>
> — Dwight D. Eisenhower

In the early days of the internet and cybersecurity, defense in depth was a practical approach that made good sense. The strategy works well when there is a strong perimeter to reinforce and defend, one's enemy is easy to identify, the most valuable assets are located inside the perimeter, and the people who work within those cyber walls are loyal and trustworthy.

But times have changed. Defense in depth is dead.

In a mobile- and cloud-based world, the castle walls have disappeared and the only things separating authorized users from cloud-based applications and corporate assets are an internet connection and their login credentials. At the same time, the shortage of qualified cybersecurity professionals can create crippling complexity, dangerous time lapses, and additional vulnerabilities when overextended security staff must struggle to master the intricacies of a parade of new best-of-breed tools. Yet, despite the limitations of this approach in today's world, many organizations keep trying to spend their way to security by purchasing more and more security apps, all in an effort to counter each new cyberattack. It can't be done.

The answer lies not in pursuing the elusive "silver bullet" technology that will surely, this time, cure your cybersecurity woes, but in adopting a better platform—one that can deliver long-term security sustainability. The platform must allow you to swiftly onboard new cybersecurity technologies onto an architecture backed by common tools and workflows, and provide automation and orchestration capabilities to lessen the burden on your overtooled and understaffed security team.

If it's broke, then fix it.

Contrary to the rest of the tech world, in cybersecurity it rarely pays to be a late adopter. Most newly introduced technologies in the market get better over time, so many IT professionals prefer to adopt new technologies only after others have worked out the bugs and the price has come down. With cybersecurity, it's the opposite. Cyber defense capabilities actually become less effective over time as attackers develop countermeasures to evade or neutralize them, so organizations benefit most by adopting and deploying cybersecurity solutions as early as possible. Just as microbes build up resistance to antibiotics as the lifesaving drugs are widely distributed, cybercriminals quickly learn how to mutate their malevolent creations to get around cybersecurity technology that is intended to block their path.

Grobman's Curve, shown in Figure 1 below, provides a useful illustration of this concept. Grobman's Curve is named after Steve Grobman, senior vice president and chief technology officer for McAfee and lead author of the book, "The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War." Grobman developed the curve to illustrate the threat defense effectiveness of cybersecurity, which shows how cyber defenses become less effective over time.

The answer lies not in pursuing the elusive "silver bullet" technology that will . . . cure your cybersecurity woes, but in adopting a better platform—one that can deliver long-term security sustainability.

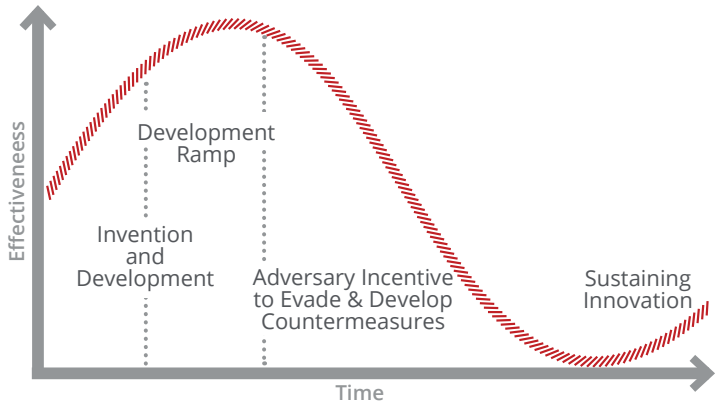


Figure 1. Grobman's Curve of Threat Defense Effectiveness

As Grobman's Curve shows, threat-specific cyber defense technologies are most effective right after they are invented. Early adopters find these tools very powerful at first, because their rapid deployment, configuration and optimization of the new widget enables them to reap the maximum security benefits. At this point (at or near the top of Grobman's Curve), the early adopter is happy, because the widget is functioning as intended and the adversary is content to exploit a large population of underdefended organizations.

Yet, as more organizations adopt the new technology farther along the curve, in an effort to inoculate themselves against the now not-so-new threat, the adversary has more and more incentive to restart their own innovation cycle. Attackers then work diligently to create countermeasures, workarounds, and new ways to evade detection and exploit vulnerabilities, rendering the once-powerful security widget increasingly ineffective. Organizations must then innovate again, to defend against the countermeasures and repel the renewed threat.

Sandboxing technology is a good example of how promising cyberdefenses can quickly become ineffective. When attackers started using malware designed to circumvent traditional antivirus defenses, many organizations deployed sandbox technology, which diverted any suspicious file or program into a contained environment. IT pros could then observe the program's operation to determine whether it was a threat. If the program proved benign it would be cleared for passage into the network. If it turned out to be a threat, the sandbox would block it. (See point A in Figure 2 below.)

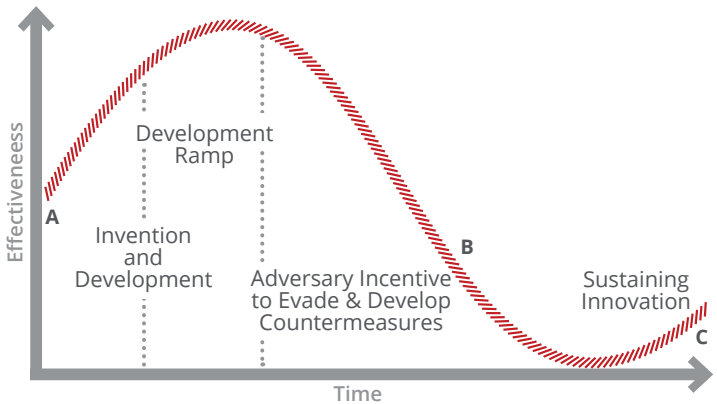


Figure 2. Example of Sandboxing Technology with Grobman's Curve

Many organizations rushed to adopt sandbox technology, believing it to be a silver bullet that would thwart cyberattacks and make the world safer. For early adopters, sandboxing was extremely effective at first, but it didn't take long for attackers to develop a number of sophisticated countermeasures that allowed malware

Early adopters of new cybersecurity solutions see immediate benefits from their investments, but as more organizations deploy the new products, cybercriminals have greater incentive to develop countermeasures.

to identify a sandbox and evade detection. (See point B in Figure 2.) As one example, attackers programmed malware to determine when it was being analyzed by a machine. Since sandboxes didn't use mouse clicks as a human operator would, attackers programmed malware to remain in stealth mode until a mouse click signaled that the malware was executing in user space and could unleash its malevolent power.

Sandbox technologies evolved by mimicking mouse clicks in later generations of their invention to confuse the upgraded malware programs, but attackers countered again. They produced malware that would wait for a certain number of mouse clicks before detonating, or that would measure the average speed of page scrolls as an indicator of human behavior. As it grew increasingly difficult to program sandboxes to mimic human behaviors, sandbox technology became the latest in a long line of best-of-breed cybersecurity solutions rendered less effective by countermeasures designed to undermine them. (See point C in Figure 2.)

With Grobman's Curve as their guide (see Figure 3 below), the goal for cybersecurity professionals is to deploy new technologies as quickly as possible, with the least amount of effort, so they can reap the benefits of threat effectiveness that come with early adoption.
And the goal for cybersecurity software vendors is to prolong product effectiveness by anticipating potential countermeasures and building resiliency into their solutions with these evasion tactics in mind.

By shifting adoption farther to the left on Grobman's Curve (as shown by the bullseye in Figure 3 below), organizations can shorten the development ramp and extend the time during which new cybersecurity solutions are effective (as shown by the red line in Figure 3).

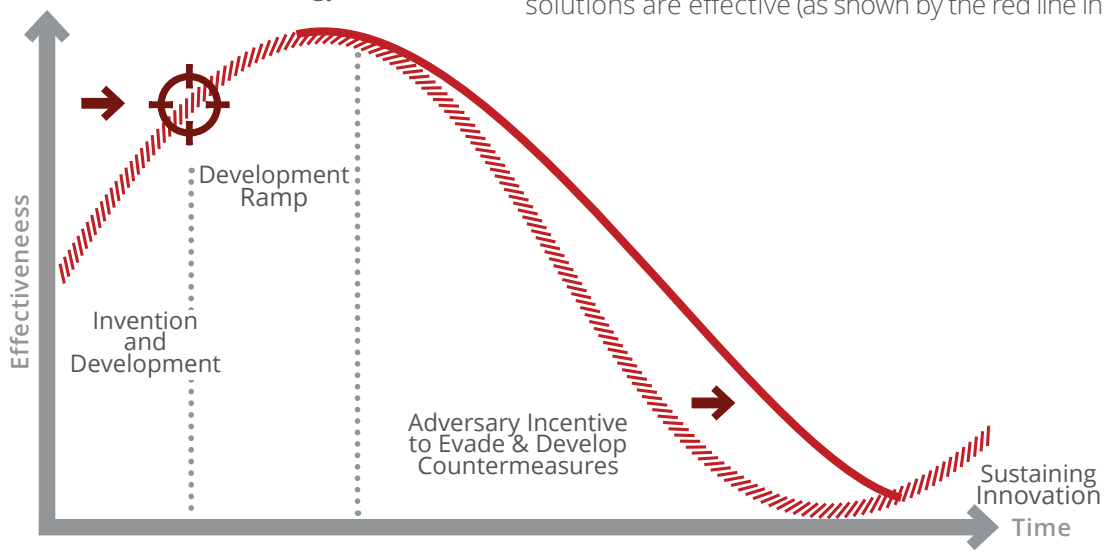


Figure 3. Extending Grobman's Curve and prolonging security solution effectiveness

"The greatest danger in times of turbulence is not the turbulence—it is to act with yesterday's logic."

—Peter Drucker

Basically, it's a matter of adding new technologies to your environment at the leading edge of the curve, at the point where they can continue to be highly effective for as long as possible before cybercriminals or other adversaries develop countermeasures that dilute their defensive power.

This is where changing the way you think about and implement cybersecurity can make a big difference in your ability to shield your organization from cyberattacks and prevent serious data breaches. By replacing the traditional best-of-breed scramble with a focused, integrated platform approach, you can strengthen your defenses while making the best use of your resources.

Open Platforms: A New Approach to an Ongoing Problem

Unlike the layered defense-in-depth approach, an integrated open platform allows you to quickly adopt the latest security products with minimal effort. In doing so, you can accelerate ROI and extend the effectiveness of your security tools in battling cyberattacks aimed at your organization.

Open platforms strengthen your defenses by allowing you to quickly add new cybersecurity solutions at an earlier point on Grobman's Curve and prolong their effectiveness in detecting and blocking threats. In addition, with an open platform, your security tools are integrated, working together and sharing threat intelligence, allowing you to reduce the time needed to detect, contain, and remediate cyberattacks. An open platform accelerates innovation by lowering development and deployment costs, makes it easier to deploy and manage a broad set of capabilities, and facilitates interoperability to ensure you can make the most of new and existing technology investments. When you use an open platform as the foundation of your cybersecurity defenses, your security products are integrated and can share information for more coordinated detection and response. You can also automate many functions to ensure faster response times and optimize your resources. In addition, automating many routine security tasks also helps you overcome some of the pitfalls of the cybersecurity labor shortage by freeing your staff to perform higher level tasks such as threat hunting that bring additional security benefits to your business.

Effective cybersecurity requires diverse approaches, technologies, and intelligence. Homogenous systems can be brought down by an attacker exploiting a single vulnerability. Open platforms ensure diversity by supporting collaboration, integration, and communication among heterogeneous solutions from multiple vendors.

Show me the money.

If you are intrigued by the power of open platforms and integrated management to strengthen cybersecurity, but still somewhat skeptical, consider the direct benefits they can offer your organization—benefits you can measure in time saved, risks mitigated, and valuable security outcomes.

> "However beautiful the strategy, you should occasionally look at the results."
>
> —Winston Churchill, Former Prime Minister of the United Kingdom

Applied Integration, Automation, and Orchestration

Figure 4. Results from the McAfee test environment.

In 2016, McAfee® engineering teams assembled a comprehensive test environment designed to simulate a large enterprise security architecture, and measured three key factors:

- Reduction in discrete agents in the endpoint image
- Time-to-resolution of a simple incident
- Increase in productivity for a typical security administrator trying to process alerts

The scores were impressive. The new approach reduced the number of agents on the desktop by nearly two-thirds, shortened time to remediation by 90%, and produced a tenfold productivity increase in alerts processing.[4] Still, the engineering team knew their findings wouldn't be taken on faith. To get the proof needed for a solid bottom line, McAfee interviewed hundreds of actual users to collect evidence and test how the integrated platform approach functions in the real world.

Consider next three examples.

Fast, Efficient Incident Management

With an open platform that facilitates real-time messages between security components from multiple vendors, you can reduce the amount of time you spend managing a security incident by more than 85%, from an average of 95 minutes to just 13 minutes.[5] Spending an average of 95 minutes on every incident weakens your organization's security, diverting attention from other threats that may be occurring simultaneously and straining your security team's resources. The kind of time savings that an open platform enables for incident response and remediation can make the difference between an isolated incident and a widescale breach.

Time Spent on Incident Management

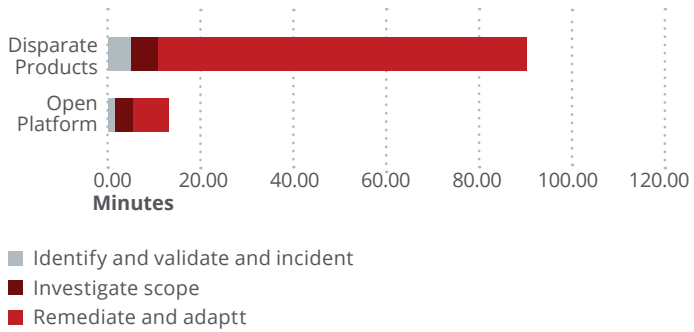


Figure 5. Open platform versus a siloed approach to security.

"Faith is an island in the setting sun, but proof is the bottom line for everyone."

—Paul Simon, Singer and Songwriter

Unified Security Management and Less Complexity

With an open platform and integrated management approach, you can unify security management across endpoints, networks, data, and compliance solutions from multiple vendors. Flexible, automated management capabilities enable you to identify, manage, and respond to security issues and threats while reducing the cost and complexity of managing security. Enterprise security organizations across many industries report that they have experienced:

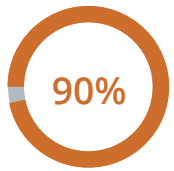
Audit preparation time

IT and end-user mpact due to misconfigured IT policies

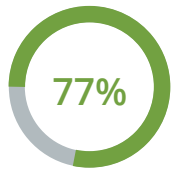
Time to develop and deploy endpoint policies.[6]

Enhanced Security and Exceptional ROI

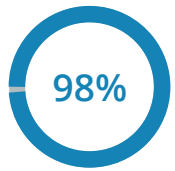
When a major US bank took an integrated platform approach to cybersecurity to ensure business continuity by minimizing the impact of network-related security incidents, the results were impressive. According to IDC, the bank realized four-year benefits worth $8.68 million and a return on investment of 208%, with a 20-month payback. Other benefits included:



Faster resolution of security events



Fewer significant security events per year



Less time lost because of security events[7]

Conclusion: Working Together

Clearly, the layered defense-in-depth approach to cybersecurity that many organizations still use is no longer an effective way to protect your assets. The threat landscape changes too quickly, and cyberattackers are too sophisticated for this traditional but outdated approach to provide the level of security that today's organizations require.

Improving security outcomes requires a new way of thinking, starting with an integrated open platform approach that ensures interoperable products, a faster response to cyber threats, and enhanced effectiveness for all security solutions. This approach enables you to deploy security solutions more quickly, with less effort and complexity, and reap the benefits of extended threat effectiveness that come with early adoption and the ability to integrate solutions from multiple vendors. Overall, an open platform and the integration and interoperability it provides can help you reduce operational costs, cut productivity losses, increase efficiency, and improve security effectiveness for your organization.

Yet, as important as it is for individual organizations to embrace a new strategy that will improve their security, there are bigger issues involved.

As organizations worldwide take advantage of the opportunities that digital transformation provides, they are also becoming more vulnerable to the growing number of cyberattacks by criminals, nation states, and hacktivists trying to breach their security and do them harm. Improving cybersecurity and making the internet safer for organizations and consumers is a challenge too big for any one company, any one industry, or any one nation. It is a mission that must be shared and embraced by everyone who has a role to play in cybersecurity.

At McAfee, we are calling on all security stakeholders—from startups and industry leaders to government policymakers and international standards bodies—to work together to achieve these goals. Step one in that process is for everyone to start thinking about cybersecurity in a new way.

Instead of thinking of cybersecurity as a series of unrelated threats that must be countered individually with the latest widget narrowly designed for that purpose, we must think of it as an ongoing challenge that requires a more comprehensive strategy than the traditional defense-in-depth approach. By making an integrated open platform the cornerstone of your cybersecurity strategy, you and your organization can achieve faster technology implementation and threat response, more effective defense capabilities, and a higher level of security overall.

> "Coming together is a beginning; keeping together is progress; working together is success."
>
> —Henry Ford, Inventor and Founder of the Ford Motor Company

Appendix: OpenDXL

Data Exchange Layer is a platform that enables security devices to share intelligence and orchestrate security operations in real time. It facilitates unprecedented collaboration in an open system, and delivers a simple path for integrating security technologies, regardless of vendor.

Data Exchange Layer is designed to shorten workflows in the threat defense lifecycle, reduce complexities across security products and vendors, and increase the value of previously deployed applications.

OpenDXL is an initiative to create adaptive systems of interconnected services that communicate and share information for real-time, accurate security decisions and actions.

Organizations and developers that participate in OpenDXL attach to a common application framework, one that will continue to gain value as more people use it and the network effect accelerates.

For more information, visit: https://www.opendxl.com.

1. "Worldwide Semiannual Security Spending Guide," IDC, March 29, 2017. (Reference: https://www.idc.com/getdoc.jsp?containerId=prUS42425417&pageType=PRINTFRIENDLY)
2. "2016 Was a Record Year for Data Breaches," Bloomberg Technology, January 19, 2017. (Reference: https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked)
3. "Customer Mindsets and Portfolio Research," McAfee, July 2017
4. The McAfee Value Management Office, 2016.
5. The McAfee Value Management Office, 2016.
6. Ibid.
7. Ibid.

Connect With Us

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

Visit us at **www.mcafee.com**.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

NOVEMBER 2017