EXECUTIVE BRIEF

McAfee
Together is power.

What's the Best Way to Protect Your Organization?

Start By Separating Security Myth from Reality.

When it comes to protecting a business, organizations typically won't go wrong following industry best practices for security and threat defense. But what do you do when there is no consensus around which practices really are best? Unfortunately, this is not just a hypothetical. IT and security professionals all over the world are largely united in assessing the scope of the threat they now face. But when it comes to identifying the best way to address the problem, there is still wide disagreement.

Figure 1. Security professionals see the same set of challenges.

Here is what the people in the trenches can agree on:

- **Threats are increasing in volume and sophistication:** Ten years ago, enterprises typically saw 25 new threats per day, according to McAfee® Labs.[1] Today, it's 500,000 daily. Even more alarming is the fact that attackers have become far more sophisticated, crafting advanced attacks that target a specific organization. According to Verizon security research, 70% to 90% of malware samples collected are unique.[2]
- **The traditional network perimeter no longer exists:** In the old days, there was a clear demarcation between activity inside and outside the enterprise. But with an increasingly mobile workforce, paired with growing use of cloud applications and services, those lines are blurring. McAfee forecasts 200 billion connected devices by 2020.[3] And based on an McAfee survey of 1,200 cloud decision-makers in eight countries, 80% of IT budgets are moving to cloud computing services, with 43 different services used, on average.[4] In this environment, notions of on premises or off premises no longer apply. Much of a business's data traffic now lives in a blended world. Which means that just maintaining visibility across the environment, much less protecting it, has become a lot harder.
- **The clock is ticking:** According to the Verizon study, in 60% of cases, attackers were able to compromise an organization within minutes.[5] But detecting that a breach had occurred took a lot longer. According to the Ponemon Institute, it takes organizations, on average, 229 days to detect a malicious attack and 82 days on average to contain it.[6] Every day that goes by, the threat to the business increases—as does the price tag for cleaning it up. According to the same study, for attacks that took more than 100 days to identify, the average total cost to the organization was $4.38 million—about 36% higher than threats that were detected sooner.
- **There are not enough people or resources to throw at the problem:** While the threat continues to grow, IT budgets are expected to remain relatively flat, according to a 2015 Spiceworks survey of more than 800 IT professionals.[7] And even when organizations have budget to hire new security staff, there simply isn't enough IT security talent in the pipeline. According to Frost & Sullivan, there is an acute cybersecurity labor shortage across the industry, with nearly 2 million positions expected to go unfilled in the next few years.[8]

Security professionals can agree on all of this. The question, then, is what to do about it. And here, they are sharply divided. Research firm Penn Schoen Berland (PSB) conducted a survey of more than 2,100 security professionals across five countries in 2016,[9] and found the industry split down the middle between two schools of thought:

- **Best-in-breed:** This view, held by 50% of respondents in the PSB survey, holds that organizations are better off relying on expert security talent than on automated systems. The best way to protect an organization, the thinking goes, is to choose proven proprietary point solutions for each of the various security domains (threat prevention, reputation intelligence, sandboxing, and others), integrate them internally, and rely on in-house experts to use them effectively.
- **Integrated platform:** Professionals in this camp believe that speed and automation are the only way to stay ahead of threats. They believe the answer lies in automating systems to address the exponential volume of low-level threats, thereby freeing their limited IT security talent to focus on rarer, more complex threats that require human intervention. And they're seeking to consolidate the number of disparate point products in the environment, and embracing a platform approach enabled by an open ecosystem of integrated solutions.

These are two very diametrically opposed diagnoses of how best to combat the growing threat. Both can't be correct. The inevitable conclusion: half the market is wrong.

Let's explore some of the myths and misperceptions pervading the IT security space, and see if we can get at the truth.

Decision Makers Are Divided

Two prevailing schools of thought:

Best-in-Breed
- Best solution in each domain
- Self-integration of proprietary system

Integrated Platform
- Embracing automation
- Open ecosystem-driven integration

Are Many Solutions Better than One?

Myth: *Using best-in-breed products in each security domain will protect organizations better than using an integrated security platform.*
Reality: *Integrated solutions deliver better protection.*

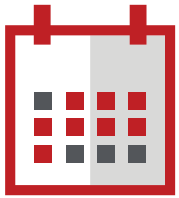
In theory, vendor diversification should allow organizations to cover all of their bases—security intelligence, threat detection, sandboxing, threat response—using the best technology out there for each domain. In practice, the result is often run-away complexity. The problem is that each time a new type of threat or vulnerability is discovered, a new best-in-breed tool emerges to combat it. So organizations end up with a constantly expanding patchwork of disconnected security solutions.

Security operations teams are met with a daily flood of data from endpoints, cloud services, and their critical environments, like data centers, manufacturing floors, and integrated control systems. Security operations teams find themselves swiveling between myriad complex management interfaces, trying to manually connect the dots between all of those sources to identify the nature of a threat and take action. And the results are not pretty: fragmented visibility, gaps in protection, and long delays between discovering and remediating exploits.

A recent McAfee survey of 565 security decision makers found that it takes an average of eight working days, or 64 hours, for a security investigation to move from detecting an exploit to returning to health. On average, respondents said they used at least four tools to get the job done, with many using more than a dozen.[10]

When digging deeper into the actual experiences of security teams inside organizations, the benefits of integration become even clearer. Of the security professionals surveyed in the PSB study, 25% have integrated 40% or more of their security workloads with one vendor. Compared to the 75% who haven't:

- **They were better protected:** 78% of the first group suffered less than five attacks in the past year, versus 55% for the second.
- **They detected threats faster:** 80% of security professionals in the first group discovered threats in eight hours, on average. In the second group, just 54% could detect threats that quickly.
- **They literally slept better:** Of those security professionals working with a third-party partner, less than a third (30%) reported that they lose sleep worrying about their security posture more than once a week. Among those who don't, 57% were facing a lot of restless nights.



8 Working Days/64 Hours

The average time to detect an exploit and return it to health.

Does Talent Outperform Automation?

Myth: *To respond to the growing security challenge, the best use of an organization's resources is to build up their pipeline of internal talent.*
Reality: *Talent can't keep pace—there's just not enough out there.*

According to the PSB survey, 60% of security professionals believe that bringing in more skilled IT security professionals is the best way to stay ahead of the growing threat. In an ideal world, we could put that hypothesis to the test, comparing results of organizations that staff up with the most skilled experts versus those relying on automated security tools. But in the world we live in, the comparison is moot, because that pipeline of talent doesn't exist.

According to a 2015 report from the Information Systems Audit and Control Association (ISACA), 62% of organizations are currently understaffed.[11] The majority of IT security positions take up to six months to fill. And 10% are never filled at all. In a 2015 survey of 507 IT security professionals conducted by the SANS Institute, 66% of respondents named staffing and skills shortages as the number one impediment to effective incident response.[12]

Cyberattackers aren't waiting around while organizations try to develop more talent and bring more expertise in house. The only option is to get more value from the talent already in place by giving them automated, integrated tools to work smarter and faster. The security experts inside organizations should be focusing their attention on the most complex cases—not spending their days chasing after low-level incidents for which the response could be automated.

Are Closed Security Solutions Superior to Open Ecosystems?

Myth: *A security framework of closed, proprietary solutions that's tightly controlled internally will protect organizations better than an open approach.*
Reality: *Open solutions allow organizations to onboard new capabilities and respond to threats faster.*

According to the PSB survey, 60% of security professionals prefer to use closed, proprietary security solutions and integrate them in house. The sentiment makes sense as, in theory, this allows organizations to exercise tighter control over their environment. In practice, however, many find that the perceived advantages of that kind of hands-on control are often inflated, and the tradeoffs underappreciated.

Most IT professionals agree that the optimal security strategy is to gather threat intelligence from multiple sources, and share it across the organization (uniting internal and external telemetry with diverse endpoint, gateway, and threat analysis systems). This is a core requirement for moving from a reactive security posture to a proactive one—where the moment a new threat is identified, every potential target in an organization is updated to protect against it. And this becomes even more important as the traditional network perimeter erodes and security operations teams struggle to

60% of security professionals prefer to use closed, proprietary security solutions and integrate them in house.

maintain visibility across mobile devices and cloud-based services and applications.

Organizations can build up an infrastructure to link their closed security systems together, but the time and costs involved can quickly spiral out of control. When none of the pieces work together, there are no synergies, no economies of scale, and no acceleration of team effectiveness. And organizations get caught in a never-ending procurement and integration cycle:

- **Step 1:** Procure a new technology to address a new threat or overcome an operational burden.
- **Step 2:** Watch the new technology's effectiveness diminish as adversaries adapt.
- **Step 3:** Find security teams over-burdened once again, as technology sprawl increases and they spend more of their time occupied with tactical efforts rather than strategic defense.
- **Step 4:** Repeat.

It's no wonder that in the Frost & Sullivan survey, 62% of security professionals said that their security efficacy was suffering as a direct result of technology sprawl.[13]

The alternative is to use open security ecosystems. These allow organizations to draw on both internal and external capabilities from a broad range of ecosystem partners, but in a way that is pre-integrated to allow these solutions to share information and automate their response. Organizations maintain the ability to use multiple industry-leading vendors across diverse security domains. But they gain the ability to onboard these capabilities much faster, and use them more efficiently.

Can Third Parties Be Trusted to Handle Threats?

Myth: *Organizations are better off relying on their internal team to handle threats, versus relying on a third party.*
Reality: *Organizations trusting third-party solution partners see superior results.*

Security professionals have well-earned confidence in their internal teams and systems. They have built up capabilities over many years and understand the inner workings of their organizations better than any outsider ever could, so it's natural to assume that internal teams are better equipped to protect an organization than an outside vendor (as 50% of PSB survey respondents believe).

However, while internal teams have unparalleled knowledge of the business, external parties that focus strictly on security typically have much broader and deeper understanding of threats. And they have a deeper bench for incident response and remediation than internal teams can provide.

Security ecosystems such as the McAfee Security Innovation Alliance can bring in tools and expertise from more than 100 security vendors and services spanning multiple security domains. Modern ecosystems consolidate security intelligence for botnets, worms, DNS attacks, and other threats. They integrate all of these capabilities so that individual products from multiple vendors can share security intelligence and coordinate response faster and in an automated fashion. Security teams can use workflows to automate threat response,

Eliminate up to 70% of manual operations related to threat defense and cut training requirements for in-house teams in half.

fill security gaps, and reduce the number of separate agents that have to be deployed on endpoints. All of which reduces routine, time-consuming security tasks and allows internal teams to focus their efforts on more strategic analysis and decision-making.

Based on McAfee research,[14] organizations that use ecosystems like these—instead of trying to coordinate everything manually in house—can eliminate 70% of manual operations related to threat defense and cut training requirements for in-house teams in half.

The Answer: Integration and Automation

Despite persistent disagreement about the best approach to combat the evolving security threat, the evidence is clear: automation and integration provide superior protection. This is not to say that organizations shouldn't be adopting innovative technology or that they should source everything from a single vendor. But bottom line, they cannot afford to continually onboard new capabilities at the expense of ever-increasing complexity.

Fortunately, the biggest security myth is that organizations have to choose between strong domain-specific solutions and an integrated architecture. With the right security framework, they can have diversification and consolidation. The key is integrating on an open platform, so that solutions across multiple domains can work together in an automated fashion.

When organizations embrace this integrated, automated approach, they gain:

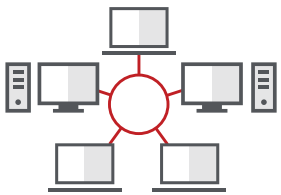
- **An adaptive security architecture:** With an integrated, automated security platform, organizations can link disparate security solutions into a single, adaptive defense fabric. Multiple solutions work together in real time to share information across previously siloed systems and processes. They detect emerging threats faster and coordinate the response automatically—without requiring operations staff to manually connect the dots.
- **A security platform that's open and ready for action:** Open interfaces and automated scripting allow organizations to onboard new capabilities much faster, and merge them with existing systems and processes more easily. Integrated systems make it easier to fill security gaps without adding operational complexity. They orchestrate the data, systems, and decision-making required to address emerging threats, and enable more effective threat detection, triage, and analysis.
- **Real-time insights for faster results:** With smash-and-grab tactics proliferating, insights that allow security operations teams to take action quickly are imperative. Integrated threat intelligence feeds and analytics provide visibility into files, processes, system changes, and indicators of compromise. Organizations using open, integrated security frameworks can share data across the IT infrastructure, including global threat intelligence feeds, organizational intelligence,

Overcoming Security Complexity

An Integrated Platform
You need a better platform, not another security product.

Automation
Your IT staff can work smarter not harder.

Open Ecosystem Approach
You can't go it alone and you don't have to.



and real-time threat information. Teams can more quickly ascertain which issues require intervention from their in-house experts, and take action faster.

- **Automation to lighten the load:** Automated workflows, scripts, and tasks translate approved processes into efficient and timely actions. Each immediate, automated response can compress triage, scoping, and containment times—and even stop an attack in progress within seconds.

Based on McAfee research,[15] organizations that embrace integration, automation, and orchestration can:

- Reduce technology sprawl in their security environments by 62%
- Reduce the amount of security technology they have to install and manage on endpoints by 85%
- Empower existing security talent to work more efficiently and effectively—up to a 1,000% increase in capacity that security teams can handle

For More Information

To learn more about how integration, automation, and open security ecosystems can help your security teams operate faster and smarter, contact your McAfee account representative or visit **www.mcafee.com**.

1. McAfee Labs, 2005-2016.
2. Verizon. "2015 Data Breach Investigations Report." 2015.
3. IDC, Intel, United Nations.
4. Intel Security. "Blue Skies Ahead? The State of Cloud Adoption." 2016.
5. Verizon. "2015 Data Breach Investigations Report." 2015.
6. Ponemon Institute. "2016 Cost of Data Breach Study: Global Analysis." June 2016.
7. Spiceworks. "The 2016 State of IT: Managing the Money Monsters for the Coming Year." 2015.
8. Frost & Sullivan. "The 2015 (ISC)2 Global Information Security Workforce Study." April 2015.
9. Penn Schoen Berland, 2016.
10. Intel Security. "How Collaboration Can Optimize Security Operations: The New Secret Weapon Against Advanced Threats." 2016.
11. ISACA and RSA Conference Security. "State of Cybersecurity: Implications for 2015." 2015.
12. SANS Institute. "Maturing and Specializing: Incident Response Capabilities Needed." August 2015.
13. Frost & Sullivan. "The 2015 (ISC)2 Global Information Security Workforce Study." April 2015.
14. Frost & Sullivan. "The 2015 (ISC)2 Global Information Security Workforce Study." April 2015.
15. Intel Security Internal Benchmark Testing Applied to Advanced Malware Cyber Defense Capability.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com