WHITE PAPER

McAfee
Together is power.

Five Ways to Rethink Your Endpoint Protection Strategy

WHITE PAPER

Five Ways to Rethink Your Endpoint Protection Strategy

Device security is no longer about traditional antivirus versus next-generation endpoint protection. The truth is you need a layered and integrated defense that protects your entire digital terrain and all types of devices—traditional and nontraditional. ESG Senior Principal Analyst Jon Oltsik frames it this way: "... endpoint security should no longer be defined as antivirus software. No disrespect to tried-and-true AV, but endpoint security now spans a continuum that includes advanced prevention technologies, endpoint security controls, and advanced detection/response tools."[1]

In today's survival of the fittest landscape, here are five ways to not just survive, but thrive:

1. More tools do not make for a better defense.

Scrambling to adapt to the evolving landscape, many security teams have resorted to bolting on the latest "best-of-breed" point solutions. While each solution may bring a new capability to the table, it's important to look at your overall ecosystem and how these different defenses work together.

There are serious shortfalls in deploying disparate, multivendor endpoint security technologies that don't collaborate with each other. Because point solutions have limited visibility and see only what they can see, the burden of connecting the dots falls on you. Adversaries are quick to take advantage of the windows of opportunity these manual processes create, evading defenses or slipping through the cracks unnoticed.

2. It's not about any one type of countermeasure.

As a never-ending array of "next-generation" solutions started to emerge and flood the marketplace, you were likely told more than once that antivirus isn't enough and what you need to do is switch to next-gen. In reality, it's not about achieving a next-generation approach or finding the best use for antivirus. It's really about implementing a holistic device security strategy that connects and coordinates an array of defenses. This includes signature-based defense (which eliminates 50% of the attack noise—allowing algorithmic approaches to run more aggressively with less false alarms),[2] plus exploit protection, reputations, machine learning, ongoing behavioral analytics, and roll-back remediation to reverse the effects of ransomware and other threats.

Connect With Us

Each device type has its own security needs and capabilities. You need to be able to augment built-in device security with the right combination of advanced protection technologies. The key to being resilient is to deliver inclusive, intelligently layered countermeasures—and antivirus is a tool that has its place in with benefits and limitations just like all countermeasures do in this unified, layered approach to device security.

3. All devices are not created equal.

Today, "endpoint" has taken on a whole new meaning. The term now encompasses traditional servers, PCs, laptops mobile devices (both BYOD and corporate-issued), cloud environments, and IoT devices like printers, scanners, point-of-sale handhelds, and even wearables.

Adversaries don't just target one type of device—they launch organized campaigns across your entire environment to establish a foothold and then move laterally. It's important to harness the defenses built into modern devices while extending their overall posture with advanced capabilities. Some endpoints, like Internet of Things (IoT) devices, lack built-in protection and will need a full-stack defense. Ultimately, the goal is to not duplicate anything and not leave anything exposed.

4. All you need is a single management console.

If you've been deploying bolted-on endpoint security technologies or several new, next-generation solutions, you may be seeing that each solution typically comes with its own management console. Learning and juggling multiple consoles can overtax your already stretched-thin security team and make them less effective, as they are unable to see your entire environment and the security posture of all your devices in one place.

But it doesn't have to be this way. Practitioners can more quickly glean the insights they need to act when they can view all the policies, alerts, and raw data from a centralized, single-pane-of-glass console.

5. Mobile devices are among the most vulnerable.

Mobile devices are an easy target for attackers and provide a doorway to corporate networks. We're seeing more app-based attacks, targeted network-based attacks, and direct device attacks that take advantage of low-level footholds. For this reason, it's essential to include mobile devices in your security strategy and protect them as you would any other endpoint.

Trending Statistics[3]

400+
security flaws in Android and iOS were published during the first six months of 2018

2/3
of mobile devices are running **vulnerable, outdated operating systems** that vendors are not patching

1/3
of total malware will be **mobile** malware by 2019

"… 55% of organizations currently struggle to rationalize data when three or more consoles are present."

—Source: MSA Research commissioned by McAfee on Security Management, January 2018

Did You Know?

McAfee® Endpoint Security comes out on top in third-party tests.

- **2018 AV Comparatives Test for business security products:** McAfee Endpoint Security was certified as an Approved Business Product with a perfect protection rate and "very low" false positives in a test that encompassed real-world malware threats, business malware and performance, and false positive detections. As the organization states in their report, "This product is undoubtedly powerful, and, as part of a wider McAfee managed platform, it offers a lot."[4]
- **2018 AV Test.org:** McAfee Endpoint Security has scored near-perfect protection and usability scores for the past year.[5]

McAfee Endpoint Security

McAfee has re-imagined device security to provide a single console with flexible deployment options to defend a broad set of devices with full-stack or overlay to native controls. Through a single-agent architecture with deep integration and automation, we remove silos between once-isolated capabilities to enhance efficiency and protection. As a leader in the industry, McAfee offers a broad portfolio of security solutions that combine established capabilities (firewall, reputation, and heuristics) with cutting-edge machine learning and containment, along with endpoint detection and response (EDR) into a single-agent all-inclusive management console. The resulting integrated

The Facts About the McAfee Device Security portfolio:

FACT: We consistently outperform competitors in third-party testing.

FACT: Our portfolio includes more than 10 endpoint solutions to defend your devices.

FACT: We offer the only true single-pane-of glass management platform that maximizes visibility and control across all your endpoints and all environments.

FACT: Our McAfee® ePolicy Orchestrator® (McAfee ePO™) management console is in use by nearly 40,000 customers.

FACT: Our security ecosystem is built on an open architecture that works with, not against, your third-party and OS security technologies.

FACT: McAfee is not just about legacy antivirus. We're continually innovating and leveraging advanced technologies to improve detection, protection, and response.

"To overcome the complexity created by too many device types, security products, and consoles, things must get simpler and the directional approach to security must shift. Modern device security needs to defend the entire digital terrain while understanding the risks at play. This first wave of the McAfee® MVISION technology portfolio provides businesses with an elevated management perspective where security administrators can more easily defend their devices and fight cyber adversaries in a cohesive and simplified manner."

—Raja Patel, Vice President and General Manager, Corporate Security Products, McAfee

endpoint protection platform keeps users productive and connected while stopping zero-day malware and advanced threats like ransomware before they can infect the first device—"patient zero."

McAfee can unify your endpoint defenses and build a device security strategy based on:

- **Single-console management with flexible delivery options:** SaaS, virtual, or on-premises
- **Integration with multiple operating systems (OSs):** Microsoft Windows Defender and Android and iOS
- **One platform that protects all your devices and enhances protection:** A single-agent architecture to manage and automate security for servers, traditional endpoints, mobile, and even embedded IoT devices
- **An integrated, collective endpoint threat defense:** Device hardening, fileless malware detection, behavior analytics, machine learning, signatures, credential theft protection, endpoint detection and response (EDR), and firewall

Summary: Device-to-Cloud Protection Starts at the Endpoint

Endpoints have extended far beyond on-premises servers and PCs and traditional operating systems. Mobile, IoT, and the cloud have changed the way we think of our device terrain and how to secure it. It's time to say good-bye to siloed, next-generation products and embrace a new expansive and inclusive device security model. This pioneering approach to endpoint security is what sets McAfee apart. There's a reason we call ourselves the "device-to-cloud" security company. As you accelerate your digital transformation, we enable you to innovate fearlessly. We won't let security issues slow you down. We provide endpoint security based on an open, truly integrated architecture that covers your entire digital environment and enables collaboration with solutions from other vendors—all powered by a unified management platform for complete visibility and control.

1. https://www.csoonline.com/article/3163450/security/rsa-conference-topic-endpoint-security.html
2. https://www.mcafee.com/enterprise/en-us/solutions/lp/sans-endpoint-survey.html
3. https://www.welivesecurity.com/2018/08/29/semi-annual-balance-mobile-security/
4. AVTEST.org Business Client Reports
5. https://www.av-comparatives.org/tests/business-security-test-2018-march-june/

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our 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.

www.mcafee.com.

McAfee™
Together is power.

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