Mastering Modern Endpoint Protection

Six steps to better enterprise protection today and tomorrow

Organizations have added layer after layer of defense to stay ahead of the latest cyberattacks. In theory, they should be better protected. Instead, security teams are drowning in tools and interfaces. According to the 2017 Forrester report, ***Mastering the Endpoint***, organizations now monitor 10 different security agents on average and swivel between at least five different interfaces to investigate and remediate incidents.

There's a way to get ahead with fresh thinking about endpoint security. Drawing on real-world experiences from more than 250 security decision-makers along with insights from Forrester and McAfee, here are six essential steps for mastering the modern endpoint and protecting the enterprise both today and tomorrow.

1. Build a security framework that scales and adapts to the changing threat landscape.

A growing number of IT security decision-makers value integrated defenses and prefer a single, coordinated system. However, barely a third (35%) have automated and operationalized threat intelligence across their architectures.

The concept of adding multiple layers of defense is widely accepted, but the key to gaining the most value out of these layers is connecting them using a flexible, adaptive security framework. By implementing defense layers that communicate with one another, you achieve greater efficiency and efficacy. The ideal framework is extensible, allowing you to continually add new layers to the fabric as business and security requirements change.

2. Integrate detection and response capabilities into everyday operations.

According to the report, the majority of organizations have been breached in the past 12 months and most struggle to remediate across all infected endpoints. Administrators need the ability to quickly follow the tracks of the threat and clean up everything it touched. Unfortunately, those capabilities are typically limited to specialized investigators, and there just aren't enough of them to go around.

Adding yet another advanced investigation suite won't solve this problem. By implementing a solution that integrates detection and response capabilities into everyday endpoint operations, front-line administrators can respond quickly when infections inevitably hit.

3. Minimize false positives so you can focus more on critical tasks.

Survey respondents ranked accuracy and avoiding false positives as the most needed endpoint security feature. The ability to fully contain infections the first time they are encountered ranked a close second. But more than 80% see significant barriers inhibiting their ability to manage risks, including the time and effort needed to manage security solutions and difficulty prioritizing newly discovered vulnerabilities.

The best answer is to improve the coordination between security tools to drive down false positives. Defenses that share threat intelligence can automatically validate or exonerate a potential threat, so human administrators don't have to. By eliminating layers of complexity and manual effort, front-line security teams are empowered to cut through the noise and respond faster. Create even more focus by automatically surfacing the highest priority incidents and provide a clear workflow for resolution.

4. Share threat intelligence in real time and immediately apply the learnings.

Up-to-the-minute threat intelligence is essential for protecting against evasive malware. According to the survey, 48% of organizations rely on threat intelligence to identify threats that evaded prevention. Nearly as many use intelligence feeds to hunt for threats in their environment and gain clarity and context.

The ideal threat intelligence strategy combines external sources with intelligence gathered from your own environment. Your platform should share the intelligence across multiple layers of defenses in real time—automatically, without requiring administrators to swivel between interfaces. The platform should then immediately apply information gleaned from one infection to every other security system in your environment.

5. Use advanced machine learning and the cloud for scale and speed.

Survey respondents listed the time needed to get new signatures and manually update endpoints as the top challenge in managing endpoint security.

Modern strategies rely on a smarter approach. Implementing and utilizing advanced machine learning capabilities, both locally and in the cloud, allows you to statistically compare suspicious executables against thousands of attributes of known threats—without signatures. The ability to analyze both static code features and an executable's actual behavior allows you to uncover hidden threats in seconds.

6. Consolidate agents and manual processes.

Endpoint security administrators aren't just imagining that their lives have gotten more complicated. Eighty-one percent of respondents believe that there are barriers in place that inhibit their ability to effectively manage risk.

By consolidating multiple tools, systems, and reports into a single management console, manual processes are drastically decreased. By adopting a consolidated approach, you can reduce the number of agents your team administers and automate manual tasks with streamlined workflows. Instead of spending hours battling disparate interfaces, you empower your team to control multiple layers of endpoint security with automated, "set-it-and-forget-it" capabilities.

Learn More

For more details on how other organizations are responding to their own endpoint security gaps, and Forrester's recommendations to address them, **download the report**.

McAfee™
Together is power.

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