Create a Dynamic Defense for Comprehensive Threat Protection

**Challenges**
Most companies depend heavily on two or three layers to defend against advanced threats: An initial line of defense at the Internet gateway, plus a second layer on each desktop or server. In many organizations, the layers and vectors of defense are not working together, so each component must be as sophisticated as the threat. That's no longer possible in the dynamic landscape of cross-vector, targeted attacks, advanced evasion techniques, and zero-day exploits.

For example, an email may contain a link to an initially harmless website, bypassing email and web security solutions. By the time the user clicks the link, the website has been updated with malware that infects the user's machine. In a highly targeted attack—one designed for your specific industry or business—the phishing email sender, webpage, and malicious payload would all be so rare that they would not register with global reputation or signature-based defense systems.

In the example above, the evidence needed to detect and deflect an attack could be distributed in email, web, and endpoint protections, so no individual component would assemble a complete image of the attack. Attackers hide in these shadows.

With these gaps, it's inevitable that some nasty code will slip through these defenses. Few companies have the resources to deploy specialized monitoring tools and hire experts to capture and analyze anomalous code. Typically, nothing happens until a breach or attack is identified—often days, weeks, or months after the event—and specialists are called in to determine what happened where and to define a remediation and recovery plan.

As more industry organizations and companies rally to share indicators of compromise such as hash files, consumption of this information remains primitive, manual, and slow. Defenses still react too slowly.

**Solutions**
It's time to learn as we secure and adapt as we protect. Comprehensive threat protection requires the right layers within each asset and within your infrastructure—working together, learning from each other, in real time. As an orchestrated system of systems, your defenses must share data and follow dynamic processes to expedite identification, containment, and remediation.

**Reduce vulnerability to opportunistic attacks**
First, organizations should reduce the attack surface for opportunistic advanced threats by upgrading security solutions in endpoints and network gateways. Going far beyond signatures, effective protection technologies should hunt for known and emerging threats using dynamic detection heuristics at the endpoints and network gateway. In addition, full-stack, multilayer traffic normalization and analysis should uncover evasions at the firewall, while deep content inspection at the email and web gateway block phishing and web-borne attacks. These technologies should be able to collaborate to share information with cloud-based services that constantly correlate threat intelligence from multiple types of sensors and sources.

**Gear up for targeted attacks**
Exposure will fall to a minimum when you block based on collective threat intelligence—a combination of the first-hand experience your products and people acquire within your environment plus the global and third-party threat...
intelligence that is available from vendors and industry sources. Integrating this information into your protections can let you go beyond detection to blocking immediately based on file attributes, source and destination addresses, timing, and prevalence. You may also be able to adjust the “knobs and dials” of your technical controls to accommodate your own risk posture.

Add scalable malware analysis
Any remaining unusual code should be handed off directly to a dedicated appliance that can perform high-speed analysis and detect subtle, advanced threats using both static and dynamic techniques. Malware appliances can incorporate the static and emulation techniques used in advanced content gateways or next-generation intrusion prevention systems (IPS), apply dynamic analysis—sometimes called sandboxing—which runs the code in a safe environment to see what it tries to do, and fully investigate code paths using static techniques that reveal clever timing and alternate execution paths. This comprehensive analysis will reveal malicious intent and behavior to quickly and accurately convict a threat.

Use automation to speed response
If malicious code is confirmed, then the analysis system should tell your other security tools to detect and block that code immediately should it appear anywhere throughout the network, simultaneously quarantining infected hosts. The information should also spur your defenses to track down compromised systems for remediation. Today, these efforts are often manual. However, when you integrate threat intelligence with endpoint security and network security, you can use automated workflows to quarantine and remediate compromised hosts automatically—in real time.

Add additional layers for defense in depth
Advanced threats (and the hackers using them) will look for vulnerabilities in laptops, tablets, mobile devices, applications, file servers, and databases. You can reinforce the anti-malware on these systems with controls that prevent system exploitation, creation of back doors, rootkit installation, and malware execution if the code is able to install. Common tools include host IPS, application control, vulnerability scanning, real-time kernel protection, and change management monitoring. Add database activity monitoring to protect critical assets in the data center. Integrate these systems together to create a manageable mesh of defenses that improve your resistance to multipronged attacks.

Enable live and forensic investigations
These technical gateway, endpoint, and network controls should reduce the chance that advanced threats will get in or infect your assets. However, today’s best practice is to assume that there will be compromised systems within your network. You must enhance your ability to detect, dissect, and disrupt the attack sequence in real time by ensuring your security operations center can centrally monitor your entire environment for advanced threat activity, data exfiltration, and suspicious user behavior.

Given the volume of network traffic, comprehensive advanced threats protection requires a “Big Data” class security and information event monitoring (SIEM) system that can aggregate, correlate, and mine data from multiple sources: Endpoint system logs, network gateways, user directories, inventories of devices entering and leaving the network, and more. With end-to-end visibility, humans can mostly monitor patterns and higher-level threat trends, letting watchlists and automated systems tackle the tactical defenses.

Best Practice Considerations
• Link coverage at all attack vectors: Network, endpoint, web, and email.
• Incorporate diverse static and dynamic analysis technologies to detect threats using advanced evasive techniques and variable timing and execution paths.
• Collect and correlate threat information from all available sources including local, global, third-party, and manually entered threat data to equip your defenses with the best-available information.
• Layer defenses to provide reinforcing protections that can prevent system compromise and remote access and halt attacks in process.
• Ensure automated communication and integration between all layers of protection to enable detection and remediation in milliseconds, not days or weeks.
• Fuse real-time intelligence and organizational preferences into designs to minimize false positives, detect emerging threats, and allow the system of systems to make context-aware decisions.
• Centralize management and monitoring across all protection technologies to lower costs and improve visibility, response, and decision-making.
Value Drivers

- Close coverage gaps to prevent loss of sensitive data such as intellectual property and regulated data.
- Reduce disruption to users and the network by preventing infections and malicious traffic.
- Improve resilience through an organizational ability to detect, convict, and contain targeted attacks before damage is done.
- Automate manual tasks and workflows to lower the event-to-incident confirmation time.
- Reduce remediation, consulting, forensic, disclosure, and legal costs.
- Prioritize critical events to focus time and resources more accurately and increase incident-handling capacity.
- Improve situational awareness through real-time visibility into changing risk and threat events.
- Enable agility through modular and open architecture and integration with legacy and third-party systems.

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected.