Email is one of the most mission-critical services for any business today, yet it is also a key vector for inbound attacks and a natural exfiltration channel for stolen data. The current best practice solution for email security is a multifunction gateway platform capable of blocking a wide range of inbound threats, enforcing policy on outbound data, and encrypting all sensitive data in legitimate transmissions.

Unfortunately, even these protections are now proving insufficient. Spear phishing attacks that combine tightly targeted messages with sophisticated social engineering and advanced malware have been implicated in many recent data breaches. According to the SANS Institute, 95% of all attacks on enterprise networks are the result of successful spear phishing.¹

In response, some organizations are adding advanced malware detection to their email defenses, typically in the form of out-of-band sandbox appliances. The sandbox launches suspicious files in a secure virtual environment and monitors runtime behavior to detect malicious intent. All too often, however, this apparent gain in detection accuracy is quickly lost to poor integration and manual response processes.

For instance, most third-party sandbox appliances can only alert a human security analyst when a new attack is found. The analyst must manually create new blocking rules for the email gateway, and then begin the task of identifying and fixing the endpoints compromised during the sandbox analysis. Other common limitations of existing solutions include:

- A cost-inflating requirement for one sandbox appliance per gateway sensor.
- Poor integration between the sandbox and gateway, which typically come from different vendors.
- Reliance on a generic virtual execution environment that may overlook target-specific attack behaviors.
- Reliance on dynamic analysis only, rendering the sandbox vulnerable to various malware strategies for detecting secure environments and delaying execution of revealing behavior.

Key Advantages

- Finds, freezes, and fixes advanced malware and stealthy attacks hidden in email traffic.
- Adds true static code analysis and target-specific sandboxing to email security with no increase in gateway workloads.
- Plug-and-play threat blocking with no delay for human intervention.
- Gateway and sandbox appliances integrate with other McAfee network security products and services.
- A centrally deployed McAfee Advanced Threat Defense appliance provides malware detection services for multiple network security sensors.
- Data and reports generated by McAfee Advanced Threat Defense are automatically integrated into McAfee Email Gateway workflows.

Advanced Threat Defense for the Email Gateway

Broaden protection against stealthy malware.
A Security Connected Email Gateway and Sandbox Solution

The answer to all these challenges is a tightly integrated combination of McAfee® Email Gateway, a comprehensive email security solution, with McAfee Advanced Threat Defense, the industry’s most powerful and complete advanced threat detection appliance. The email gateway provides in-band traffic inspection and threat blocking through a set of malware detection technologies that are optimized for real-time execution. McAfee Advanced Threat Defense provides a more extensive and resource-intensive set of analyses that include both target-specific sandboxing and true static code analysis. Together, these two devices find and freeze new, unknown, and stealthy advanced threats. For a complete end-to-end solution, add McAfee ePolicy Orchestrator® (McAfee ePO™) software to quickly identify and fix any systems impacted by advanced malware.

- **Find**—Innovative analytical technologies work together to quickly and accurately detect sophisticated threats within email traffic.
- **Freeze**—Tight integration between McAfee Email Gateway and McAfee Advanced Threat Defense instantly stops infiltration attempts in email before they reach a user.
- **Fix**—Block newly discovered threats and search for similar infiltrations across the environment, initiating the endpoint remediation process when necessary.

![Figure 1. Integration points for finding, freezing, and fixing malware.](image)

Because the McAfee Advanced Threat Defense solution for email follows the Security Connected approach to enterprise security integration, it delivers a range of operational and defensive advantages that are unique in the industry, including:

- **Seamless interoperation and data exchange**—Tight integration links the gateway and sandbox appliances together with all of our other security products and services.
- **Plug-and-play threat blocking**—Attacks discovered by McAfee Advanced Threat Defense are automatically blocked by McAfee Email Gateway with no delay for human intervention.
- **Centralized sandboxing for multiple network security sensors**—McAfee Advanced Threat Defense can provide malware detection services for an email gateway, web gateway, firewall, and IPS sensor.
- **Report and workflow integration**—Malware conviction data and reports generated by McAfee Advanced Threat Defense are automatically integrated into McAfee Email Gateway workflows, eliminating much back and forth between screens during investigations.

**Security Connected**

The Security Connected platform from McAfee, part of Intel® Security, provides a unified framework for hundreds of products, services, and partners to learn from each other, share context-specific data in real time, and act as a team to keep information and networks safe. Any organization can reduce risk and response time and lower overhead and operational staff costs through the platform’s innovative concepts, optimized processes, and practical recommendations.
**McAfee Email Gateway**

McAfee Email Gateway consolidates inbound threat protection, outbound data loss prevention, encryption, advanced compliance, and administration into a single, easy-to-deploy and user-friendly appliance. The powerful set of inspection engines within McAfee Email Gateway, in conjunction with reputation intelligence from McAfee Global Threat Intelligence, provide the most complete protection available against the full range of inbound threats. McAfee Email Gateway prevents zero-day threats, targeted and blended attacks, and dramatically reduces the impact of spam and spam surges through a potent combination of dynamic spam classification and threat response. It provides integrated protection against viruses, malware, phishing, directory harvest, denial-of-service attacks (DoS), and bounce-back attacks.

McAfee Email Gateway also provides comprehensive outbound protection through a combination of sophisticated content scanning technologies, multiple encryption techniques, and granular, policy-based message handling to prevent outbound data loss and simplify compliance. It can be deployed as a hardware appliance, virtual machine, blade server architecture, cloud-based service, or as a hybrid of cloud and on-premises solutions. This flexibility enables affordable protection and scalability for the most demanding messaging environments.

Immense value comes not only from McAfee Email Gateway itself, but its ability to leverage the insights and capabilities of other McAfee security solutions:

- McAfee ePO software, which enables unified management and reporting for endpoint, data and network security, including McAfee Email Gateway. With end-to-end visibility and powerful automations that slash incident response times, McAfee ePO software dramatically strengthens protection and drives down the cost and complexity of managing risk and security.
- McAfee Advanced Threat Defense, the advanced malware detection component of this solution.

McAfee Email Gateway is a part of McAfee Email Protection, which enables customers to deploy on-premises, in-the-cloud, or as an integrated hybrid combination of the two. For more information about these products visit [www.mcafee.com/emailgateway](http://www.mcafee.com/emailgateway) and [www.mcafee.com/emailprotection](http://www.mcafee.com/emailprotection).

**McAfee Advanced Threat Defense**

McAfee Advanced Threat Defense is a multilayered malware detection solution that stacks an extensible series of inspection engines and analytical capabilities in a sequence of increasing computational intensity. This unique approach to complete and efficient assessment delivers a high level of detection accuracy and reliability with extremely high-throughput performance. The on-board analytics applied by McAfee Advanced Threat Defense include:

- Signature-based detection of viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks using a comprehensive knowledgebase created and maintained by McAfee Labs, which currently includes more than 300 million signatures.²
- Reputation-based detection using the McAfee Global Threat Intelligence network to detect newly emerging threats.
- Real-time emulation to quickly find malware and zero-day threats not identified with signature-based techniques or reputation.

---

Full static code analysis that reverse engineers file code to assess all attributes and instruction sets and fully analyze the source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, helping organizations better understand the specific malware they are dealing with and the impact it has on their organization. Full static code analysis provides critical insight into input-dependent behaviors and delayed or hidden execution paths that often do not execute during dynamic analysis and are overlooked by less comprehensive sandbox solutions.

Dynamic sandbox analysis that executes the file code in a virtual run-time environment and observes the resulting behavior. Unique among existing sandbox solutions, McAfee Advanced Threat Defense configures virtual runtime environments to match the target host based on queries to McAfee ePO software. Analyzing file behavior under the exact conditions of the intended host produces accurate results quickly and efficiently, revealing malicious behaviors that might not be triggered in a generic environment. And since many advanced attacks are designed to evade sandbox detection, McAfee Advanced Threat Defense includes innovative techniques to ensure code execution during dynamic analysis.

These techniques work together in coordination to efficiently identify many types of known and unknown malware. The combination of full static and dynamic analysis reveals the obfuscated and advanced malware not positively identified through lighter-weight analysis engines.

McAfee Advanced Threat Defense appliances are easily configured to apply only those analyses that have not been performed on upstream gateway sensors, eliminating the performance penalties of redundant inspections. McAfee Advanced Threat Defense appliances scale to throughput capabilities of up to 250,000 objects per day, allowing one advanced malware system to support multiple McAfee Email Gateway sensors.

An Efficient Closed-Loop Solution for Advanced Threat Prevention

The combination of McAfee Email Gateway and McAfee Advanced Threat Defense provides exceptionally efficient protection against email-borne attacks along with advanced malware detection and response. This is an automated, closed-loop solution that finds sophisticated attacks and freezes them in their tracks, removing malicious email messages without the need for manual intervention by overworked network operators or security analysts.

For more information on how our solutions can secure your network against stealthy, advanced threats, contact your representative or visit www.mcafee.com/atd.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative hardware-enhanced security, and unique Global Threat Intelligence, Intel Security develops proactive, proven security solutions and services to protect systems, networks, and mobile devices for business and personal use all over the world. www.intelsecurity.com.