White Paper

Automating the Threat Defense Lifecycle

The security strategy you've been waiting for

intel Security

Automating the Threat Defense Lifecycle

This white paper was written by:
Brian Dye
Corporate Vice President and
General Manager
Corporate Products
Intel Security

Table of Contents

At its core, our strategy, which we introduced at FOCUS15, is based on a simple concept: to create an integrated security system that automates the threat defense lifecycle so you can address more threats faster with fewer resources. With the recent announcement of our strategic partnership with TPG, we want to further define our strategy and demonstrate our unique position in the market and how we aim to make IT security as dynamic and responsive to today's most severe threats.

The results of our open, connected security system will be measurable, which is a simple but important concept. We define success not just through your satisfaction, but also through the impact on key CISO-level metrics. When compared to disconnected, non-integrated architectures, our systems are able to:

- Reduce overall time to protection from more than four hours to one minute.
- Increase incident response capacity by up to 30 times.
- Improve response time from 24 hours to less than seven minutes.[1]

Fundamentally, we are creating these integrated and automated security systems because we believe:

- **Protect, detect, and correct are better together:** The threat lifecycle of integrated security builds the best protection technology possible, finds and contains advanced threats, and rapidly remediates them, while adapting protection technologies to do a better job of blocking the next threats. Organizations with integrated security platforms are 30% better protected, and we want you to be part of that statistic.[2]
- **Only automation can overcome staffing issues:** You are clearly faced by a mismatch between your staffing (talent and volume) and the growth in number and sophistication of threats.[3] That gap is compounded by tools that force analysts to manually connect the dots across them, which takes even more time and effort. Deeply automated security systems are critical to help solve that problem. They help eliminate routine tasks, enable faster new hire onboarding, and free your strongest talent to tackle your hardest problems. We expect automation to reduce manual effort by up to 70%.[4]
- **No vendor can do this alone:** The security industry is one of the most fragmented areas of IT, and no one provider delivers the entire threat defense lifecycle. You need a practical way to integrate new capabilities into an overall platform approach. Only strong partnerships with industry leaders can create security systems that truly protect, detect, and correct.

With those beliefs fueling our strategy, we are building a platform-based architecture with four security systems: endpoint, cloud, hybrid data centers, and threat management. We'll describe each briefly and show you how they work together.

Endpoint

Most enterprises suffer from the problem of having too many siloed security solutions on their endpoints, which creates complexity and inefficiency, as these products don't work in unison or communicate with each other. Vendors often have either a great platform or great point technology, but not both.

Figure 1. Best-of-breed systems create complexity.

By building on endpoint security platform agent architecture and increasing our investment, we can deliver the full threat defense lifecycle for the endpoint, thereby reducing the volume of threats that get elevated to the security operations center (SOC) for analysis, while still providing a lower-cost system. Over time, you can expect:

- **Endpoint protection and endpoint detection and response (EDR) convergence:** Bringing our EDR solution, McAfee® Active Response, natively into the McAfee Endpoint Security architecture and driving even more cross-endpoint workflows.
- **More security technologies that do more together:** Expanding our existing capabilities to include behavioral security (both pre-execution and post-execution), machine learning, and more.
- **Cloud enablement:** Leveraging the cloud dynamically to drive threat detection and analysis.
- **Agent consolidation:** Delivering even more consolidation at the endpoint (the entire portfolio over time).
- **Extending to thin or closed platforms:** Extending to thin platforms, like the Internet of Things (IoT), and mobile devices through the McAfee Data Exchange Layer, proxy protections, partnerships, and more.
- **Expanded centralized management:** McAfee® ePolicy Orchestrator® (McAfee ePO™) software will continue to provide low total cost of ownership (TCO) for management and will expand the range of technologies supported both on premises and in the cloud.

Cloud

The rise of Software-as-a-Servce (SaaS) application usage and more mobile workers means the cloud has become the enterprise perimeter. This creates a need for a new generation of security and privacy technology while enabling cloud-driven business. As a result, we are building a single, fully integrated solution to provide cloud-delivered data security.

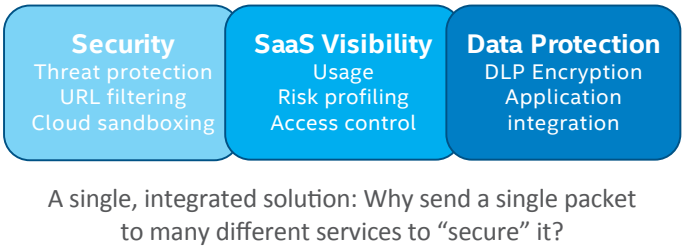


Figure 2. Cloud-delivered data security.

Over time, you can expect:

- **A world-class cloud data platform:** Building SaaS first from the ground up to deliver great performance and availability. This will include a global, load-balanced infrastructure with content delivery network (CDN)/peering data centers.
- **Security services:** A rich set of services, native to the platform, including web protection, sandboxing, cloud access security brokers (CASB), data loss prevention, encryption, and more.
- **Protection that travels with you:** Constant protection—whether you're in the office, at home, or on the road—through a range of traffic redirection options (forward/reverse proxy, DNS, and others). This includes packaging and then embedding the client proxy with the converged endpoint solution (for traditional endpoints and also IoT devices).
- **Next-generation security management:** McAfee ePolicy Orchestrator Cloud (McAfee Cloud ePO) software driving consolidated management across not just this solution, but also our other cloud-managed technology.

Hybrid Data Centers

As data centers evolve to software-defined data centers and more workloads run on either hosted data centers or public cloud, security organizations are faced with a new set of challenges. To help, we are building an integrated system to deliver visibility and security as agile as the cloud. Over time, you can expect:

- **Visibility:** Enabling a cross-data center view of workloads and threats across private and public clouds.
- **Workflow orchestration:** Making security as dynamic as the cloud, both through dynamic micro-segmentation (for private clouds) and workload auto-discovery (for public clouds).
- **Platforms:** Continuing to support next-generation platforms, building beyond VMware and Amazon Web Services to add Azure, OpenStack, Docker containers, and more as they emerge. This allows security teams to help their lines of business safely embrace these new platforms. IT security no longer has to be "the department of no."
- **Holistic security:** Delivering threat sharing and automated response based on server, north-south, and east-west (internal) threat traffic, which delivers both better protection and faster remediation than siloed approaches.

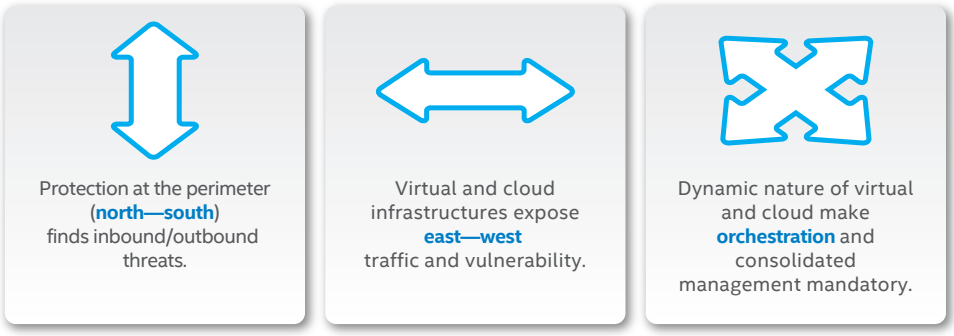


Figure 3. Responding to the challenges of hybrid data centers.

Threat Management

Within the SOC, the primary challenge is not just the scale of data, but how to sift through the large number of events and indicators of compromise (IoCs) to prioritize true attacks in progress or in the "golden hour," post-breach. This is where the security talent shortage is most acute. To help you with this over time, you can expect:

- **Security analytics:** Continued leadership in advanced data management, correlation, and security analytics to deal with both the volume of security data as well as the increasing sophistication of analysis.
- **Attack detection:** Investing more in attack detection, both during and post breach, ranging from sandboxing (on premises and cloud based) to behavioral analytics and beyond.
- **Attack investigation:** Market leadership in new technologies like attack reconstruction that help organizations to identify and respond at a full attack level, not just at an event or malware level.
- **Streamlined incident response:** Automated correction to drive end-to-end automated (and eventually, automatic) containment and response to attacks.

Connecting these Security Systems

Each of these systems help you address more threats faster with fewer resources. That said, because these systems are themselves built on platforms, they will work together to solve even bigger security problems. Here are just a few examples.

- **Closed-loop threat defense:** The four systems work together to share threat information and automate protection, which improves security and lowers cost. Using the example of a potential attack starting at the endpoint, our security systems automate the detection and response end to end (although a threat coming in through the cloud or data center would have the same flow).

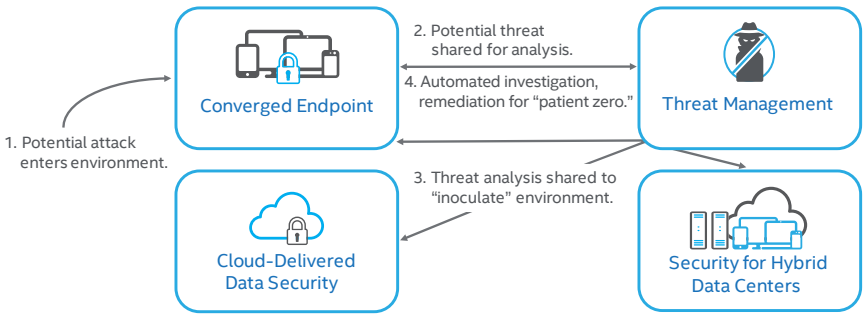


Figure 4. Closed-loop threat defense.

- **Mobile workforce security:** Due to the rise of SaaS applications, mobile workers can complete much of their work using only email, SaaS applications, and local computing resources. The combination of the converged endpoint and cloud-delivered data security systems is designed to create a "mobile clean zone" to not only secure mobile workers' devices, but also to keep organizations' data secure while off network, allowing users to more safely reconnect to the corporate network when needed. This includes technology from both Intel Security and our partners, for example, VMware AirWatch and MobileIron.
- **Security for Infrastructure as a Service (IaaS):** Securing the workloads and access of IaaS platforms, like Amazon Web Services or Microsoft Azure, highlights the interconnectivity of the public cloud, data, users, and SOC to defend it successfully:

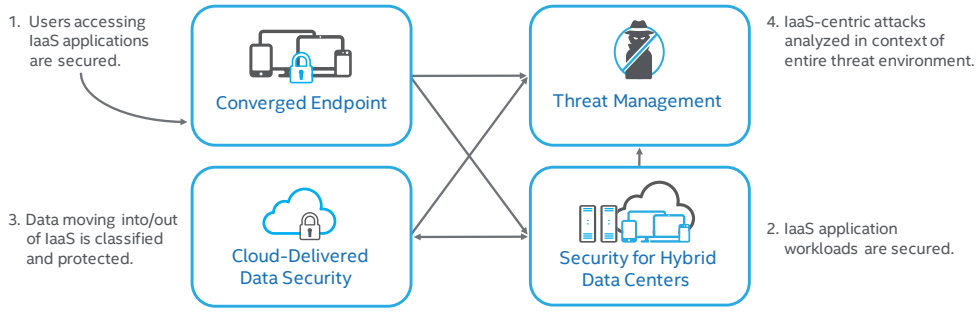
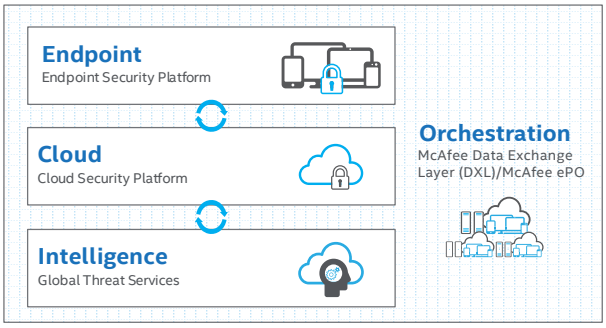


Figure 5. Security for IaaS.

Engineering Approach

Our strategy of building automated security systems is a fundamental shift in how we engineer solutions, moving from point products to integrated systems that deliver better security outcomes. In engineering these systems, we are focusing on four principles:

- **Partnership-centric:** We believe no vendor can solve this problem alone, so we are proud of the wide adoption of our open architecture. This started with McAfee ePO sofware and the more than 150 Security Innovation Alliance partners that have integrated to it and other Intel Security technologies. Over the past year, McAfee Data Exchange Layer has been adopted by more than 20 key industry players for threat sharing and automation.
- **Platform-based approach:** We built our systems on top of key platforms to accelerate time to market, extensibility, and scale.



Platform-based engineering reduces your cost and accelerates delivery.

Figure 6. Our platform-based approach.

- **Reinvented experience:** We have tripled our investment in user experience and are bringing a new, patent-pending user interface concept to the market that will let you do more with the talent you have. We're looking forward to showing you the new technology based on this user-interface approach.
- **Cloud-centric:** We are leveraging security both for the cloud (protecting workloads and data in the cloud) and from the cloud (delivering security analysis, threat intelligence, and management from the cloud). To be clear, if you appreciate McAfee ePO software today, you will appreciate McAfee Cloud ePO software tomorrow.

The right engineering approach is part of our execution. In addition to a solid engineering strategy, we are investing to succeed. We restructured our portfolio in 2H 2015 to create a substantial investment pool to drive execution against this strategy. We will draw from our current pool of expertise and will be adding new talent focused on delivering positive outcomes through these security systems.

A Unique Point of View

A common hazard across the security industry is that vendors start describing their strategies with common words, and, before long, everyone sounds the same. To help cut through the industry buzzword lingo, here are a few areas where we believe our approach is truly unique:

- **Integration:** We are combining point products and features into integrated security systems using common platforms. This is evident in the four security systems. Each combines the capability from three or more point products into a single system. We deliver this integration and management level with McAfee ePO software and the threat intelligence level through McAfee Data Exchange Layer.
- **Automation:** With integration as our foundation, we then build in closed-loop automation. This automation delivers more accurate detection, faster remediation, and closed-loop protection. These benefits increase directly with the breadth of products and technologies that we integrate—whether our own or from other security providers.
- **Orchestration:** With more of your organization freed up through automation, we then proceed to orchestration. While automation is at the tool level, orchestration is at the system level. Orchestration not only drives actions, but also coordinates teams and accelerates investigation. The gains across both security effectiveness and team efficiency are dramatic, which is why this is the ultimate goal of both integration and automation.

Learn More

Join us at FOCUS16 in Las Vegas this fall, where we will share with you the first round of technology delivery against this strategy.

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. Visit **focus.intelsecurity.com/Focus2016/** for more information. Intel Security is a division of Intel.

1. Internal laboratory testing of defense of advanced malware through the threat defense lifecycle comparing disconnected point product security system with integrated and automated system.
2. Penn Schoen Berland. Research on behalf of Intel Security, 2016
3. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)²-Global-Information-Security-Workforce-Study-2015.pdf, pages 10-14
4. Internal laboratory testing of defense of advanced malware through the threat defense lifecycle comparing disconnected point product security system with integrated and automated system.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com