Security Connected Reference Architecture
Solution Guide

Disrupt Targeted Attacks

Synthesize IT operations and security controls into an agile architecture.

intel Security

Time to Embrace an Adaptive Security Model

Security Connected

Our Security Connected framework makes it easy to reduce complexity, response time, and operational costs while simultaneously improving your security posture in the face of growing risk. Hundreds of products and services from Intel Security and its partners share context and intelligence in real time to learn and adapt to keep your critical information and infrastructure safer. Standard interfaces bridge Intel Security innovations and end-to-end infrastructure to your environment. It's the agile foundation of an adaptive security architecture.

Challenges

In early 2015, an Intel® Security survey[1] of incident responders at 700 organizations uncovered the hurdles and opportunities facing investigators of targeted attacks. With an increase in the attack surface and the industrialization of cybercrime, we found incident response teams are overwhelmed, constantly fighting fires that exceed their capacity. Many have invested in countermeasures and tools, but the friction and fragmentation that they need to overcome is leaving them ineffective in the fight.

Investigations Take Too Much Time

- According to 47% of survey respondents, most time is spent scoping an attack, determining what was altered on a system, what this alteration did, and what other systems may have been affected.
- 42% say taking action to minimize the impact of an attack consumes their time. And until triage and containment activities are complete, the attack remains active and the business is at risk from data loss and destruction.
- Third and fourth on the list is the time it takes to analyze security intelligence to detect incidents (41% of respondents), followed by vulnerability assessment and determining what other systems might fall prey to that attack based on an understanding of the attack chain (39% of respondents).
- Root cause analysis is also time consuming (38% of respondents). More than one-third (35%) said altering controls to prevent future types of malware attacks is a big resource drain.

The survey also showed that responders know they can be more efficient if they have better detection through better analytics and training. They also want tighter integration between security data and the systems that operate IT infrastructure. This synchronization helps merge security and operational data and processes so you can both identify critical events and dig into them to perform the required investigations.

"Security professionals are inundated with security incidents, averaging 78 investigations per organization in the last year, with 28% of those involving targeted attacks—the most damaging cyberattacks."

—Tackling Attack Detection and Incident Response, Enterprise Strategy Group, April 2015[1]

More Data than Sense

As we look at the responses, most of these detection and correction efforts combine human expertise with tools and data. All efforts can be improved through access to and better interpretation of relevant data, policy-based workflows, and appropriate and facilitated automation.

So what's holding these valiant security operations teams back? Turns out that security has been a cost of doing business, treated as overhead, with few metrics and limited risk analysis. There's an infrastructure, but not a conscientious and resilient architecture.

Silos of People, Process, and Technology

Traditionally, security projects have been chosen, implemented, and operated with an eye to solving a specific problem: protection, detection, correction, and (separately) compliance. Few security teams have had architects articulating an integrated design or an adaptive model. Unlike other long-term infrastructure in IT, until recently security products have not adopted a common data sharing model, messaging infrastructure, or efficient way to link and maintain process integrations that cross workgroups.

Instead, security products have been chosen by desktop, network, and compliance buyers without a conscious plan to integrate, enable data sharing, or establish the resilience necessary to keep up with increasingly subtle threats. They have been minimally maintained and replaced when contracts expire, rather than as business and technology changed. 'Set and forget' was a legitimate goal for some security gear.

If this description sounds like your organization, you should understand that attackers use this antique approach against you. They've proven that point-product decisions create white space. Their toolkit-based and targeted attacks use this weakness to penetrate, persist, and strike—at sensitive data, vulnerable systems and applications, and critical infrastructure.

"58% of respondents want better detection tools while 53% say they need better analysis tools for turning security data into actionable intelligence."

—Tackling Attack Detection and Incident Response, Enterprise Strategy Group, April 2015[2]

Solutions

Intel Security recommends that you unify the protect, detect, and correct stages of managing threats so you can build a comprehensive security model to combat targeted attacks. While each stage has its own unique set of tactics, they all work together to provide context and leverage insights. This concept—an adaptive security model—applies learning immediately throughout a collaborative architecture and provides the overall cyber-resilience required to outmaneuver adversaries, contain intrusions quickly, and avoid excessive financial damage.

To protect, detect, and correct more effectively, review your incident response program to see how well it functions as a machine. Is it a network of separate components, or an integrated, high-performing, and continuously available system? How well do each of the processes integrate with and enrich each other? Is it a closed and continuous loop? As you optimize the protect, detect, and correct steps, you'll synthesize IT operations and security controls to form an agile, increasingly automated architecture. Here's how you make it happen.

Modernize Protections

While prevention shouldn't need an overhaul, each control in your arsenal could use a check-up, particularly with respect to threat intelligence and malware detection. Customized attacks likely start with phishing, corrupted websites, evasive techniques, and zero-day malware. Several actions improve countermeasure effectiveness and prevent incidents that may be sophisticated, but not necessarily highly targeted.

Take full advantage of the capabilities available in the preventative controls you already have. Harden and isolate systems from attack using endpoint suite features such as application blocking and behavioral signatures. Let email and web gateways detect and block suspicious files, sites, and phishing messages before they reach the user. Software updates, add-on modules, and Security-as-a-Service are the lowest cost, lowest disruption ways to acquire current features.

Integrate threat intelligence into countermeasures bidirectionally, so your controls share discoveries with each other and with researchers and other corporations. For instance, endpoint, email, and web protections consume, generate, and share threat intelligence with networked analytics for closed-loop threat analysis. This allows you to move from a mode of constant tactical encounters to learning and adapting.

Finally, make your architecture adaptive using automated blocking based on evolving reputation, risk scores, and policies, or other attack understanding. These efforts should be considered part of 'routine maintenance' for your security infrastructure.

Detect in Real Time

With fewer attack components penetrating your network, you should have fewer events to investigate, and the items you find should be worthy of attention. The primary task becomes convicting events quickly to reduce dwell time.

To help incident responders, deep analytics tools have escaped from the forensic lab to the security operations center (SOC) and become useful to desktop and network operations. Endpoint detection and response and security information and event management (SIEM) tools collect event, system, flow, and process information from all attack vectors, then thoroughly analyze malware, network traffic, and connections. By comparing indicators of attack with localized threat intelligence, these systems elevate visibility of significant events and trigger automated and human workflows. The less critical and simply noisy events are filtered out or handled based on policy.

Architects should evaluate based on both compelling features and practical long-term utility, such as the adaptability to integrate with existing and future systems. Every analytics feature must come with a concrete plan to live

Best Practice Considerations

- Revisit your controls to see how much of the functionality is already available from your current solutions before purchasing a 'silver-bullet' product.
- Pay for external threat intelligence only if it matches risks and activities within your environment.
- Harness events at all attack vectors to inform attack analytics.
- Invest only in solutions that link security controls with data capture, advanced analytics, and rapid response tools.
- Incorporate diverse static and dynamic analysis technologies to detect threats using advanced evasive techniques and variable timing and execution paths.
- Centralize incident management and monitoring across all systems to lower costs and improve visibility, response, and decision-making.

within efficient investigation workflows and policy-based management. If it doesn't, it's a gadget that quickly becomes shelfware in the pragmatic and intense climate of investigations.

"Data breaches are up 55% year over year while 70-90% of malware discovered is unique to individual environments."

—Verizon Data Breach Investigations Reports, Verizon, 2015[3]

Contain and Correct

Once the team identifies compromised systems, centralized systems with orchestration expedite containment and remediation. It's critical to connect endpoint and gateway data sources with other systems and incident-management workflows for searching, visualizing, and acting on findings. Responders and surge staff—including operational teams—can navigate multiple systems, attack vectors, users, network segments, and timeframes with agility to find and root-out attack components. In the past, these tasks were done manually. Now, software systems do the bulk of the work with minimal human effort. Humans can focus on the higher order assessments and decisions.

Architect for Agility

The above efforts will likely tear down the barriers that keep security operations reactive. Modern security components, integration models, and management systems encourage an orchestrated approach. This unified model extends the integration in endpoint and network protection as well as the end-to-end visibility, baselining, analytics, and work-stream automation in SIEM platforms.

With these fundamentals, you can refine controls, policies, and processes for greater effectiveness. A conscious program to take security architecture up the maturity curve provides clear benefits. Incident responders effectively interrupt attacks, and security teams replicate the efficiencies enterprise IT has achieved with integration of other functions, such as enterprise resource planning (ERP).

Value Drivers

- Shrink exposure and dwell time to prevent loss of sensitive data such as intellectual property and regulated data.
- Reduce helpdesk calls, surge fire drills, and user disruption by preventing and containing compromise.
- Reduce remediation, consulting, forensic, disclosure, and legal costs.
- Prioritize critical events and automate tasks 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 our Security Connected framework, visit: www.mcafee.com/securityconnected.

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

1. www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf
2. www.mcafee.com/us/resources/reports/rp-esg-tackling-attack-detection-incident-response.pdf
3. www.verizonenterprise.com/DBIR/2015/