



Charting a New Course for IT Security with Coordinated Threat Defenses

Effectively thwarting modern malware and targeted attacks requires a new level of integration and coordination among traditional domain-level controls and next-generation, centralized security analysis, correlation, and management systems.

Licensed by:



EXECUTIVE SUMMARY



The story is the same for organizations of all types and sizes worldwide: too many threats are not only getting through their security defenses in the first place, but also going undetected for far too long. Furthermore, once a lingering threat is finally discovered, the required response activities are often onerous to the point of being ineffective, leaving the organization susceptible to recurrence of the same type of incident in the future. The bottom line is that IT security teams for countless organizations are losing the war against today's threat actors and their increasingly elusive attack techniques and malware creations.

Coordinated threat defenses is a new approach to enterprise security that helps address this situation. It builds on the traditional tactic of relying on comprehensive domain-level countermeasures by emphasizing the additional need for:

- Extensive, multi-way integration among domain- and management-level components
- Overarching, cross-domain security data analysis, correlation, and visualization
- Supplemental, global threat intelligence
- Intelligent coordination and automation of essential threat response capabilities

By promoting and facilitating a complete threat defense lifecycle – prevent, detect, determine, and respond – coordinated threat defenses promises to help today's IT security teams not just stem the tide of successful and lingering compromises, but perhaps also turn it. Subsequent to explaining the coordinated threat defenses approach and its key elements, this paper explores applicable options, trade-offs, and other considerations for organizations looking to migrate their security defenses in this direction.

ENTERPRISE SECURITY TEAMS ARE LOSING THE WAR

Although rising security budgets,¹ steadily improving technical countermeasures, and exhaustive efforts by most security operations teams are enabling enterprises to win a commendable number of battles against cyberthreats, by most measures they are losing the war. Need some evidence? Here are some convincing statistics that help make the case:

- 76% of surveyed security professionals indicated their organization had been compromised by at least one successful cyberattack in 2015 (source: 2016 CyberEdge Group Cyberthreat Defense Report).
- 99.9% of exploited vulnerabilities were compromised more than a year after the corresponding CVE was published (source: 2015 Verizon Data Breach Investigations Report).
- For 2014, the average defender-detection deficient – that is, the duration between earliest evidence of a threat/attack and the actual discovery of the compromise – was 205 days (source: 2015 Mandiant M-Trends Threat Report).

- In 60% of cases, attackers are able to compromise an organization within minutes (source: 2015 Verizon Data Breach Investigations Report).
- The heads of security for major critical infrastructures in the Americas indicated that incidents involving their computing systems are not only increasing (53%), but also becoming more sophisticated (76%) (source: 2015 Trend Micro Report on Cybersecurity and Critical Infrastructure in the Americas).

And to be clear, these findings are only the tip of the iceberg. In addition to numerous other statistics that reinforce these points, there is the unpleasant fact that the situation is actually worse than reported. After all, as high as some of these percentages are, they still don't account for the presence of compromises and breaches that remain unknown/undiscovered.

IT SECURITY CHALLENGES

The reasons for this situation abound. The industrialization of hacking and resulting increase in volume, velocity, variety, and sophistication of threats being deployed by today's threat actors are certainly a big part of the problem. How well (or not) organizations are responding to this escalation of threats is another issue. Related challenges include having too many gaps in one's defenses, potentially over-reacting to the diminished effectiveness of traditional threat detection technologies, and being hamstrung by cobbled-together security infrastructures that are little more than disconnected islands of protection.

Gaps in coverage. Primary domains requiring attention include the network, endpoints, datacenter (with its servers, applications, and data storage systems), and cloud. Add to these a variety of sub-domains and areas of concern – such as social media, the consumerization of IT, user mobility, operational technology, the Internet of Things, and the proliferation of web applications – and it comes as no surprise that IT security teams are struggling to keep up. Even when they do manage to address all of these different areas, there is still the issue of inconsistencies across the resulting defensive infrastructure – for example, in ease of management, effectiveness, and core capabilities.

First contact is now the norm. For most people, industrialization connotes mass production, with assembly lines delivering millions of copies of the same article. However, that is not how it works with hacking. Instead, greater efficiency, specialization, and modularization have led to a plug-and-play wonderland where even modestly skilled hackers can churn out thousands of variants of a threat that appear (and technically are) unique, but still convey the same payload. The proximate result is a substantial decline in effectiveness of traditional detection/prevention technologies, especially those that depend on signatures to get the job done. No longer is it sufficient to assume that a handful of other organizations will be the ones to suffer “first contact,” and that your defenses will be updated by the time each threat gets to your doorstep.

From a signature/hash perspective, 70% to 90% of malware samples are unique to a single organization.

(Source: 2015 Verizon Data Breach Investigations Report)

Too much of a good thing? Reacting to the rise of one-and-done malware and the imposing nature of the threat landscape in general, numerous industry analysts began beating a new drum a few years back. Specifically, the call went out for enterprises to make substantially heavier investments in threat **response** capabilities. The rationale behind this advice is that if you can no longer depend on stopping threats at your doorstep, then you'd better at least be able to quickly and thoroughly respond to them once they are discovered.

The upside to this shift in tactics is that it called attention to a part of the threat defense lifecycle that has long been under-appreciated and, therefore, neglected. The downside, however, is that some organizations have been taking it too far. Focusing on notification, eradication, remediation, and other aspects of recovery – to the exclusion of continuing to improve one's real-time detection/prevention capabilities – is not the answer. In fact, such an approach only exacerbates the situation; without effective detection, there is nothing to respond to.

Just because real-time detection/prevention is getting harder does not mean it is impossible. It just means there is a need to invest in newer, emerging technologies that are not dependent on previous observation of a given threat.

Disconnected islands. Built over time in response to changing attack surfaces, threats, and countermeasures, the security infrastructure at most organizations is a patchwork of disparate products. Other than a handful of one-way ties to a centralized SIEM, there is precious little integration between components. In addition, there is limited cross-component data analysis or correlation, and next to no automated sharing of information or coordination of response activities. The result is a sub-optimal security environment that is riddled with gaps and inconsistencies in protective coverage, painfully slow to account for newly discovered threats, and laboriously inefficient to operate.

TURNING THE TIDE WITH COORDINATED THREAT DEFENSES

Completely winning the IT security war is an unrealistic goal. However, recovering lost ground from our adversaries and perhaps even gaining the upper hand need not be. Indeed, we are hopeful that by pursuing a new approach known as coordinated threat defenses, IT security teams can not only stem the tide, but also turn it – to the point that they're ultimately winning all but the smallest percentage of their encounters with threat actors, both now and in the future.

Conceptually, coordinated threat defenses is straightforward: a comprehensive set of domain-specific countermeasures and an overarching security management platform operate in a tightly integrated and highly coordinated manner to address the complete threat defense lifecycle – see Figure 1. As with any complex system, however, the devil is in the details. To shed some light on the most significant of these details, the following sections elaborate on the key components, capabilities, and requirements of a coordinated threat defenses solution.

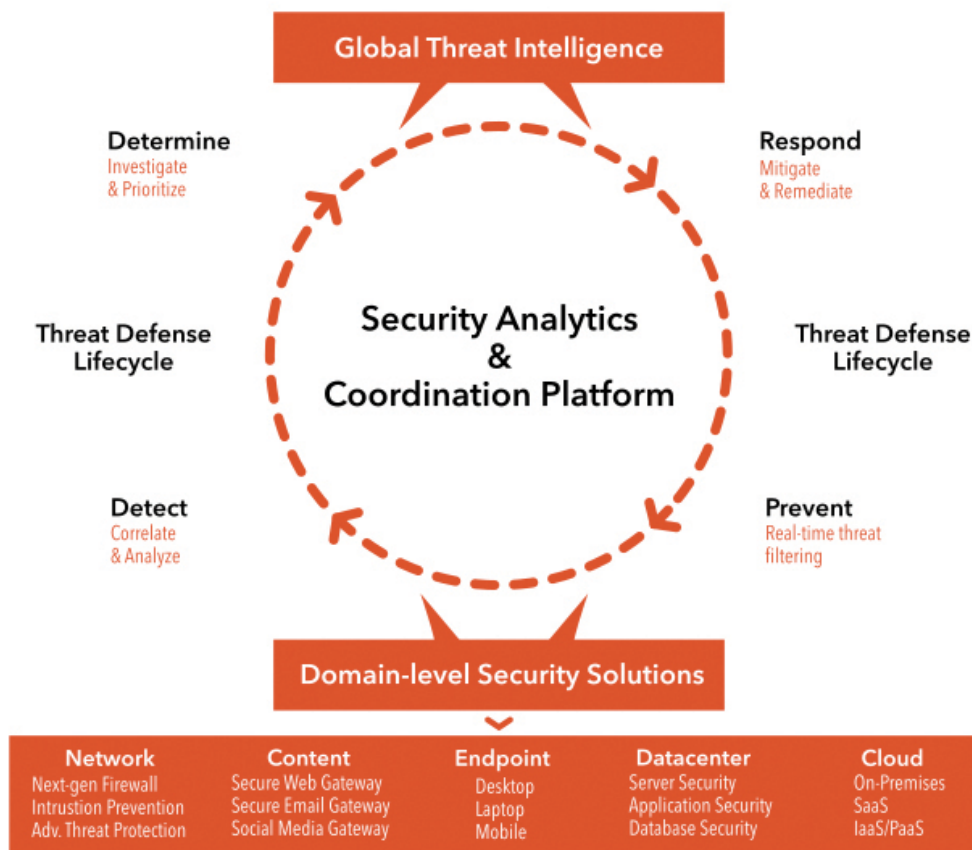


Figure 1: Coordinated Threat Defenses

Comprehensive controls. Deploying countermeasures for all of the primary domains and various sub-domains or areas of concern that apply to a given organization is only a starting point. To achieve maximum protection, IT security teams also need to ensure each solution sufficiently accounts for:

- the different layers of the extended computing stack – network/transport, device, system, application, data, and user. For example, while leading endpoint protection suites typically provide protection across all layers of the stack, it’s generally the case that network firewalls have limited capabilities at the application, data, and user levels.
- the full range of security functions that are applicable/needed – access control, threat prevention, encryption, monitoring, etc. In this case, it is appropriate to think of which aspects of the threat defense lifecycle a given solution should support. For example, most firewalls focus on prevention. In comparison, host security suites should ideally include capabilities that cover all four lifecycle stages.

Past tendencies and product limitations aside, the ultimate goal should be to establish coverage for all layers and most, if not all, security functions across all domains and sub-domains.

Continued investments in prevention. Responding to one-and-done threats by de-emphasizing prevention in favor of response is a mistake. To maximize effectiveness of their security infrastructure, organizations should instead look to achieve balance across all stages of the threat defense lifecycle. This means not only continuing to support traditional technologies capable of efficiently clearing out known threats, but also stepping up to newer ones that promise real-time (or close enough) protection from previously unseen threats. A handful of both familiar and next-generation technologies worthy of consideration in this regard include:

- Intrusion prevention systems featuring vulnerability-based signatures
- Network behavior anomaly detection
- Sandbox technology (on premises, cloud, and cloud-assisted)
- User/entity behavior anomaly detection

Extensive integration. A core tenant of coordinated threat defenses – and one of its greatest differences compared to traditional approaches – is extensively sharing information among the various components of the security infrastructure. Achieved through extensive integration, a primary objective of this sharing is to provide comprehensive aggregation of and visibility into all domain-level security events. In addition to supporting centralized alerting and reporting, information sharing lays the foundation for many of the other capabilities yet to be discussed.

To be clear, there is no “magic” in this area; rather, it comes down to evaluating candidate solutions against three essential criteria:

- The breadth and depth of available out-of-the-box integrations (ideally beyond the ordinary domain component-to-SIEM connection)
- The availability and flexibility of APIs for developing custom integrations
- The level of effort required to develop/implement such integrations

Overarching analysis and correlation. In comparison to the previous section, this is where the “magic” happens. The goal is nothing short of detecting threats that get through (or around) front-line prevention mechanisms and are not picked up by domain-level controls because of their limited point of view/sphere of influence. Past attempts to do just this fell short for a variety of reasons, including insufficiently broad reach/visibility (see previous section). The primary issue, though, was that most solutions offered little if any out-of-the-box event correlation and data analysis – instead, leaving those as exercises for already overwhelmed security operations teams to work out on their own, and in a largely manual manner, no less.

Fortunately, significant progress has been made in this area in recent years. The latest generation of security management and analysis platforms is starting to address the shortcomings of traditional SIEMs and other related solutions, in part by incorporating:

- Big data plumbing/infrastructure for effectively handling the growing volume, velocity, and variety of security data generated by the modern enterprise

- Meaningful degrees of out-of-the-box, cross-domain correlation
- Advanced analysis algorithms/techniques and big data analytics
- Machine learning technology, and other methods/mechanisms for increasing the automation of security data analysis
- Powerful yet flexible data visualization and incident investigation capabilities

Such platforms lie at the heart of the coordinated threat defenses strategy and, arguably, are the single greatest key to a successful implementation.

Global threat intelligence. Any security management and analysis platform is only as good as the security data at its disposal. Accordingly, an enterprise security team would be remiss not to supplement its organization's internally generated security events and data with a reputable, external source of global threat intelligence. The goal is to benefit from the exposure and findings of other enterprises – along with the output of one or more vendor “labs” that specialize in threat research and analysis. At the very least, security teams can leverage reputation data, file hashes (i.e., signatures), and other indicators of compromise (IOCs) obtained this way to enhance the effectiveness of both their threat prevention and detection solutions.

With richer information about threat actors in general, as well as their organization's most likely set of adversaries, they can also take advantage of more advanced and strategic use cases – such as proactive cyberthreat hunting and next-generation defense planning. The former is all about employing finely tuned processes and investigative techniques that leverage leading-edge intelligence to better find and isolate hidden threats, while the latter applies projected threat scenarios to help ensure the organization's defenses will be effective many years into the future.

By leveraging an intelligence provider that has put in place suitable processes and procedures to safeguard sensitive customer information, security teams can also benefit from the enhanced accuracy and additional insights that derive from the provider's ability to correlate and analyze organization-specific event data that is shared with it.

Intelligent coordination and automation. Another major objective of the extensive integration and information sharing discussed earlier is to enable more effective and efficient responses whenever new threats are discovered and/or new threat intelligence becomes available. For most security teams today, the best-case scenario for threat response is the automated updates they periodically receive for individual domain-level countermeasures. The worst-case, and still all-too-common, scenario is where threat response remains an onerous, highly manual, and often haphazard activity left to an already overloaded security operations team. The result, especially given the accelerating pace of new cyberthreats, is an ever-growing mitigation and remediation backlog that leaves the organization exposed for extended periods.

To address this critical deficiency, a coordinated threat defenses solution should include these key capabilities:

- Fully automated distribution of new threat data (e.g., signatures and other IOCs, obtained not only from external sources of threat intelligence, but also one's own security systems and infrastructure)

- Fully automated configuration changes to fix/update threat prevention rules and settings
- Threat data distribution and other responses that are not isolated, or 1:1 (i.e., from one product's management system to its own enforcement points), but instead are effectively shared, or many to many, as a result of being "coordinated" by a central management system

Note: Although obtaining truly effective cross-domain communication and response is likely to depend, at least in the near term, on having a uniform set of solutions at the domain level, the vision for coordinated threat defenses is that this should not be a constraint in the long run.

COORDINATED THREAT DEFENSES IN ACTION

Consider a typical targeted attack that begins with a spear-phishing email conveying one or more weaponized attachments. From this initial foothold, command and control (C&C) is established so associated threat actors can load additional malware and tools, laterally expand the scope of infection, escalate their network privileges, and gain access to systems containing valuable data/information. Exfiltration of said data ensues, often under cover of legitimate-looking (i.e., authorized) activities.

Although traditional defenses might uncover one or more of the individual phases of such an attack, rarely will all of the pieces be put together, and never will an appropriate response be taken across different components of the security infrastructure – that is, at least not without significant involvement by the security operations teams. As a result, the threat actors have the opportunity to adapt, and the organization remains compromised for an extended period.

With a coordinated threat defenses approach, the same attack unfolds much differently:

- Upon detecting an unknown file (i.e., the email attachment), the organization's secure email gateway sends it to a custom sandbox for evaluation.

- Upon determining the file is malicious, the sandbox solution generates a corresponding malware signature and other IOCs, including whatever details it can uncover about the associated C&C processes.
- Upon obtaining the various IOCs from the sandbox component, the centralized analytics and coordination platform reaches back out to numerous domain-level countermeasures – such as endpoint/server anti-malware engines, network firewalls, web security gateways, and so forth – to arm them with the artifacts they need to block the given threat and all of its associated activities.
- Bi-directional data sharing with a provider of global threat intelligence enriches the set of IOCs/artifacts that are distributed, for example, by automatically accounting for other campaigns being conducted by the same threat actors, as well as other IP addresses, domains, and URLs they are known to use.
- In the case of an advanced implementation, the centralized platform could also coordinate with other management-level components to automatically establish the scope of infection and remediate affected hosts.

The net result is a much more efficient approach for effectively thwarting modern malware and targeted attacks.

GETTING THERE

Transitioning from one's current security infrastructure and processes to a coordinated threat defenses solution is not something that can be completed overnight. But neither does it need to be an overly burdensome endeavor. Steady, incremental evolution will be the best approach in most cases, following on the heels of a comprehensive gap analysis and prioritization exercise. Options, trade-offs, and other significant factors to consider along the way include the following.

Best-of-breed vs. most-connected/coordinated. Pursue a strategy of using best-of-breed products/technologies at the domain level and, in general, the result will be better functionality but greater manual effort to achieve the desired degrees of integration and coordination. Pursue a single-vendor solution/suite and, typically, the opposite will be true: better integration and coordination in exchange for somewhat diminished capabilities and/or gaps at the domain level. Trying to determine which of these approaches would be more effective is a fool's errand that devolves into a series of largely intractable questions, such as:

- How much more effective is a set of best-of-breed components compared to the alternative?
- How difficult is it to integrate and coordinate the best-of-breed components?
- What degree of integration and coordination has the single-vendor solution achieved, and what, specifically, are the resulting benefits?

The key to avoiding this dilemma is to start with a single-vendor solution that not only features unparalleled integration/coordination capabilities and is best-of-breed (or at least nearly so) for the components it provides, but also is highly customizable and openly extensible. This way, best-of-breed and other third-party components can still be leveraged as needed or desired.

The role of SIEM. Technically, it should be possible to use an existing SIEM platform as the central component of a coordinated threat defenses solution. However, because traditional SIEMs are notoriously weak in several key areas – such as out-of-the-box correlation and analysis – such an approach is likely to require substantial manual effort to build, and then operate and maintain. A more logical role for existing SIEM investments is to serve as a collection and aggregation layer for domain-level security data, which then feeds into a higher-layer component specializing in analysis, correlation, and coordination. SIEMs may continue to deliver value in the areas of reporting and visibility (e.g., enabling drill-down into raw data records and fields). Over time, however, we expect that these and other SIEM capabilities will be subsumed into a new breed of centralized threat defenses platform.

Additional evaluation criteria. The newest, most important piece of this new approach to enterprise security is clearly the centralized, coordinated threat defenses platform. Many of the requirements that define it have already been outlined in preceding sections. Additional, significant criteria against which to evaluate candidate offerings include:

- Virtualization/cloud readiness – Modern security management systems should support not only traditional physical appliances, but also virtual appliances, cloud delivery, and hybrid deployment models. In addition, associated integration and coordination capabilities should operate across all of these environments (i.e., physical, virtual, on premises, and cloud).

- **Orchestration/SDN readiness** – More applicable (but not exclusively) to domain-level components, this item is all about: (a) supporting logical portability (e.g., not relying on fixed attributes for proper operation); and (b) having northbound integration interfaces to accept direction from other, potentially higher-layer management systems.
- **Reliability and scalability** – As the nerve center of an enterprise's IT defenses, associated components must incorporate robust, high-availability features – ideally including the option for active-active failover. To facilitate enterprise-wide deployments, potentially providing coverage for a globally distributed infrastructure, support also needs to be available for clustering, hierarchical/tiered deployments, and a variety of other scalability-oriented features.

Alternate lifecycles/frameworks. Individual details are less important than the general concepts conveyed herein, such as establishing comprehensive coverage for domain-level controls and maximizing the integration and coordination among them. For example, if an organization favors the 5-step functional model – identify, protect, detect, respond, and recover – of the NIST Cybersecurity Framework² over the threat defense lifecycle of Figure 1, then so be it. Making such in-kind substitutions is not only acceptable but also encouraged to enable better alignment with other best practices, guidelines, and standards the organization has already chosen (or is required) to adopt.

CONCLUSION

Enterprise security teams are losing the war against today's threat actors and their increasingly elusive attack techniques and malware creations. Although the industrialization of hacking and the rise of one-and-done malware are clearly big parts of the problem, they are not alone. Other contributing factors include too many gaps in most organizations' defenses, the isolation of typical domain-level countermeasures, and the recent de-emphasis of prevention-oriented solutions in favor of response-focused investments.

Coordinated threat defenses is a new vision for modern security infrastructure that we believe has the potential to help IT security teams stem the tide of modern threats – if not turn it. Anchored by a new breed of security management and analysis platform, the coordinated threat defenses approach focuses on achieving widespread integration, security data sharing, and collaboration among both domain and management-level components of an organization's security infrastructure. Expected benefits include fewer compromises, substantially shorter dwell times for threats that do manage to get through, and far less effort and expense required not only for incident response, but also to operate and maintain one's security infrastructure in general.

Footnotes:

1. According to the 2016 Cyberthreat Defense Report, nearly three-quarters of surveyed security professionals indicated that their organization's security budgets are expected to grow in 2016. Furthermore, 85% signaled spending on security exceeds 5% of the overall IT budget for their organization (*CyberEdge Group*, February 2016).

2. <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>



About Trend Micro

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Built on 29 years of experience, our solutions for consumers, businesses and governments provide layered data security to protect information on mobile devices, endpoints, gateways servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by more than 1,200 threat experts around the globe. Trend Micro has been developing a Connected Threat Defense framework by integrating our multiple layers of solutions from endpoint to cloud with central management to deliver the visibility and control our customers need to defend against today's sophisticated threats. Integrating the capabilities to detect, prevent, and respond across our solutions gives organizations the ability, in real-time, to identify attacks and remediate existing compromises.

About CyberEdge Group

[CyberEdge Group](#) is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles.



CyberEdge Group, LLC

1997 Annapolis Exchange Pkwy
Suite 300
Annapolis, MD 21401

800.327.8711
info@cyber-edge.com
www.cyber-edge.com

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of CyberEdge Group, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.