
# Security Synergy

David Balaban

Unity is power. It's a simple lesson, power and strength come from unity. But for information security, we haven't quite learned this lesson yet. It's not that we're not trying, we've made a real progress over the years, but there's something fundamentally still missing. Maybe it's time for unity.

We see all the benefits of unity around us, but when it comes to information security, we are still not there. In order to understand that, we have to understand the history of our industry.

For many years, we looked at security as a compliance or a check box exercise. We deployed security solutions to meet the letter of the law but not the spirit of the law, and we all know how this turns out. Data breach after data breach in the news made us realize that compliance does not equal security.

Our common approach to addressing security has been a concept known as a defense in depth. We deploy layers of security to try to protect our organizations. We started in the early days with the PC, trying to protect it from viruses and Trojans. With the adoption of the Internet and digital business, we moved to the perimeter where we deployed firewalls. Over the years, we've

continued to add layers to protect our applications and our networks, but this approach isn't working anymore.

Our enemies are winning, and the adoption of emerging technologies is only making the problem worse. Critical assets and data are no longer within my perimeter. So as an organization who is trying to make security investments, where do you turn for guidance?

Typically, we're going to look at the analysis, but analysis hasn't made this problem any easier.

We now have markets for vulnerability assessment, web application scanning, policy and compliance, security information and event management, endpoint detection and response, forensics and incident investigation, and threat intelligence. This doesn't include markets like governance, risk management and compliance, all the security devices, firewalls and IDS's, identity and access management or encryption. I'm confused. Do I need a solution in each of these markets? Do I need multiple solutions in a single market?

Let me give you a couple of examples. Do I need to buy a SIM, security information management system? SIMS detect less than 1% of new attacks. So to answer that question, you need to understand what use case am I trying to solve. If I'm trying to solve identification of attacks, then I probably don't need a SIM because it's not very effective. But if I am trying to solve a compliance reporting problem, which is what the original use case for SIM was, then maybe I should buy one.

Let's look at threat intelligence, this new emerging market where vendors have very little overlap in the data that they provide. Does that mean I need to buy more than one threat intelligence feed? Do I need to buy them all? Most organizations can't afford them all, so what do I do?

A lot of people already know this doesn't work. But if we know it's not working, then why are we continuing to do it? As vendors, why do we continue to build solutions to solve only a subset of security problems? As organizations, why do we continue to tie our budgets to these markets instead of the holistic security market? As analysts, why do we continue to create new markets instead of trying to solve the bigger security problem? And I think I know the answer why. There was no alternative.

We are off the map. Without a new map, we are going to do one or two things. We are going to stand and wait for orders, or we are going to continue to do what we have been doing, which we know doesn't work. This is the problem that we saw around the world. It's time for a new approach.

We need a security synergy. It’s not an endpoint solution or a next-generation security product. It’s looking at security holistically; it's made up of the critical security domains to unify your defenses. Let’s proceed to each of these domains.

**Discover**

The first domain is discovering. It's probably the most basic domain but it's the one we struggle with as an industry the most. If I don't know what's on my network or where my critical data is, how am I going to protect it? With emerging technologies, this is no longer just about servers and workstations, we have to understand mobile devices, cloud services and, the Internet of things.

**Assess**

The next domain is assessing.  I have to understand the security state of my devices. This isn't just about remote vulnerabilities, but more importantly about local vulnerabilities, misconfigurations, malicious files and processes. The number one attack vector for most breaches is still a phishing e-mail that exploits a client's side vulnerability. If I don't understand the security state of my network, I cannot stop that threat vector.

**Monitor**

Next is monitoring. Most people would equate this with the SIM. But it's more than that, it's not just about log collection, it’s about understanding activity on my networks. It means I need to do things like packet inspection and integration of actionable threat intelligence.

**Analyze**

Analyze and use the data from the first three domains to identify where malicious activity is in the network. This is things like event correlation, anomaly detection, and behavior analysis.

**Respond**

Respond is the output of Analyze. Once I have identified malicious activity, I need to do something about it. Most people would equate this to the security operations center for large organizations. Not every organization is going to have the budget or the resources to build its own dedicated security operations center. But they still need to be able to respond to mitigate attacks on the network, which means they need things like alerting and notification and workflow.

**Protect**

The last domain is the one that I think would take us the longest because it requires us to build trust. Trust with our systems, the data and the analysis that we are doing. But the ability to proactively protect our devices when we know something malicious is going on. These are things like applying the patch or disabling a port/service or isolating a device from the network.

**Security Synergy**

This all together is security synergy. There are several benefits that you can get immediately by adopting this model. We can identify attacks quicker. The average is still over two hundred days. If we can shorten that time down to days, hours or minutes, we can truly protect our critical assets and data. Another benefit is that we can be assured that we're making the right security investments. Can you assure that you're making the right security investments? Can you assure that those security investments are working? And if you answer no to either of those questions, then I encourage you to look at the security synergy framework to identify where your next investment should be.

By adopting this framework, it will prepare us for the future of information security.