



Lippis Report

White Paper

Lippis Report 129:
The Gestalt Approach To IT Security Takes Shape

by
Nicholas John Lippis III
President, Lippis Consulting

July 2009



Lippis Report 129: The Gestalt Approach To IT Security Takes Shape

Today's Enterprise IT defenses against malware or exploits are built by deploying a set of security appliances that mitigate specific threats. This appliance approach was very effective during the 1990s when dominant threats were hackers attacking corporate IT assets via the Internet. As hackers were joined by cybercriminals an economic motive to target personal data and create greater havoc materialized along with increased exploit sophistication. In fact, most of today's threats are blended, meaning that an exploit might enter a corporation through e-mail, then pass through the web which ends up having botnet traffic that eventually infects a client and phones home to a botnet server. An exploit could use three or four different vehicles before it launches a full-scale attack, bypassing legacy or siloed security tools. These blended attacks result in the all-too familiar consequence of security breaches including company image damage, personally-identifiable information (PII) theft, service downtime, cleanup and remediation costs, compliance penalties, and corporate liability. So how do security leaders defend against these assaults? The solution lies in the fact that the more IT security defenses can view the better control defense they enjoy. Enter the Gestalt approach to IT security.



Unique Uses Cisco Network Virtualization at Zurich Airport to Realize Business Revenue Outcome

[Listen to the Podcast](#)

The Gestalt Approach

The word Gestalt means a structure, configuration, or pattern of elements so integrated as to constitute a functional unit with properties not derivable by summation of its parts. In other words, IT needs to think about an IT security approach that delivers greater defense than the sum of its siloed security tools and appliances. Over the years IT has been too product focused in its efforts to mitigate exploits. Anti-X client software, firewalls, intrusion detection and prevention systems (IPS), network behavior anomaly detectors (NBAD), alarm aggregators, etc., were deployed and operated independently to address specific exploits. This resulted in a largely product centric siloed approach to security. IT ends up having many defense "bits and pieces" but not an overall view and control over their threat level. Traditional IT security looks at defense as: "I have devices providing security to devices that are targets." The Gestalt approach is a way to make sure that every device is contributing to the security of the corporation by being able to share information and work collaboratively to defend against increasingly sophisticated exploits through increased visibility and control.



Cisco Offers Security Framework Named SAFE

[Listen to the Podcast](#)

The Gestalt approach had not been possible before as different security vendors focused solely on their product, device or appliance. There was no common language or organizing principal that allowed security devices and security features within network devices to collaborate in an effort to mitigate and remediate a threat. The Gestalt approach turns the IT security industry on its head. Exploits or malware hijack corporate IT assets such as email, web sites, the network, etc., to deliver their damage or target personal and secure data. In a Gestalt-based security architecture the network becomes an important component of IT's defense arsenal. The best example of the Gestalt

approach is Cisco's SAFE, a security architecture and framework to network existing security devices so they work in unison and thus deliver a higher level of IT defense.

Cisco SAFE

Cisco SAFE is designed to address the disconnect between individual security devices not being able to share and communicate information with each other and not being able to leverage network intelligence. Note Cisco SAFE is not a product; it's an approach to securing IT assets complete with a reference guide that shows IT how to achieve highly secure networks. SAFE starts from the perspective that IT organizations have invested in security tools and appliances and offers a way to network these devices and gain greater value from them through configuration suggestions, best practices and how-to guides.

SAFE provides detailed blueprints on each segment of the network, be it the campus, data center, branch, wide area, etc.; these are called "places" in the network. The blueprints provide information such as security device placement, kinds of applications supported, network functions, and what threats are associated with the unique place in the network either, directly or indirectly. For example, the campus network may be viewed as being directly attacked; however most of the time the campus is simply overwhelmed with traffic as an attack is passing through it on its way to the data center. So how does IT secure all the areas of the network? What kinds of technologies need to be put in place to obtain the Gestalt effect?

The Security Control Framework

To make SAFE usable, Cisco developed the Security Control Framework (SCF). SCF is a way of thinking about security so that there is a consistent approach regardless of the place in the network. To achieve this simplification SCF focused on two principal ideas, visibility and control. The first is how to increase visibility into a segment of the network and second is how to increase control over end-points, devices and traffic resident in that part of the network.

Using the concepts of visibility and control a series of design guidelines or reference architectures for all the places in the network in a typical enterprise was developed and is available here. There is a SAFE design blueprint for the data center, campus, Internet edge, branch offices, partner connections, customer connections, e-commerce sites, the WAN, etc., each with their own unique functionalities. There are separate design guides for each of these "places" as well as a design guide that crosses "places" in the network providing a common approach to a solid network security foundation.

Proscriptive And Prescriptive Guides

The guides provide information to answer such questions as what are the fundamentals for securing a switch, WLAN guest access, a router, etc? What security technologies do you need to have in place? How do you best enable security that's built into the devices themselves, the integrated switch security features or WLAN controllers for example? Each design guide starts at a high level of device placement then increases in granularity providing security confirmation recommendations, identifying common threats, and implementations. The guide dives into command line instructions to configure devices appropriately to ensure proper operation of the device in that network place to maximize security defenses there. For example, a guide would provide guidance as to the placement of an alarm aggregator and recommend configuration thusly so it communicates with other devices. It may prescribe the placement of a firewall and IPS while proscribing best practices based on lab and customer test. The SAFE guide modules, organized by network "places", have the value of being fully vented, tested and validated thanks to thousands of hours of engineering time. SAFE is both proscriptive in terms of a view, but also prescriptive to assist IT organizations in achieving a high level of security defense by providing device configuration.

WAN Advantage: New Thinking in Branch Office and WAN Edge Design plus Services

[Get the White Paper](#)

Cisco SAFE Reference Guide

[Get the White Paper](#)

Cisco SAFE Solution Overview

[Get the White Paper](#)

It's in this systematic approach to securing each "place" in the network that SAFE delivers a higher level of defense than the individual devices themselves or what a collection of devices would deliver. Information and intelligence is thus leveraged across security components and coupled with network intelligence providing increased visibility of threats and defense control. The main purpose of SAFE is to enable a systemic view of threats and security defenses so that organizations have the best mitigation tools possible. The days of buying IPSs and firewalls, for example, and thinking that an organization is secure have been over for some time. IT organizations are in an arms race with hackers and cybercriminals, meaning that unfortunately its job of securing its organization is never going to be done. But securing IT assets can be made easier by recognizing this fact and shifting thinking away from a component point of view toward building a defense that is systemic across an organization reaching as far and wide as the tentacles of its network. This is strategic thinking about security where the focus is on the whole as opposed to the parts.

Cisco provides a suite of professional services that tie directly to each SAFE module. Cisco also provides full life cycle professional services for SAFE such as an overall pre-SAFE assessment that identifies existing security equipment that can be leveraged complete with gap analysis and vulnerability closure to design and implementation, through on-going management and optimization. But the SAFE reference guide is free and is designed for IT organizations to implement on their own or with a systems engineer. The 300-page document is available here and will walk you through the step-by-step guides for how to implement SAFE.

The Gestalt approach to IT security and Cisco SAFE offers new thinking in defending corporate assets by networking and configuring each device with a security role as a contributor to the overall security posture of an organization, delivering greater visibility and defense control.

**Cisco SAFE: A Security Reference Architecture
The Changing Network and Security Landscape**

[Get the White Paper](#)

Cisco SAFE Security Architecture Poster

[Get the White Paper](#)