

Taking A Smarter Approach to InfoSec

Author: Mark Bouchard

AimPoint Group
keeping IT on target

Taking A Smarter Approach to InfoSec

Executive Summary

The effectiveness of perimeter-centric security designs and traditional countermeasures that rely primarily on fixed parameters to provide protection is rapidly eroding. This is due in part to the rising tide of targeted attacks, but even more so to the increasingly dynamic nature of data, devices, applications, and infrastructure—a by-product of several major trends, including user mobility, the consumerization of IT, and cloud computing.

In response to these conditions, this paper describes a new, smarter approach to information security that:

- Acknowledges data as the heart of all security issues, and emphasizes the need to protect it wherever it resides;
- Brings greater attention and innovation to the discipline of threat protection; and,
- Focuses on solution characteristics—such as contextual awareness, real-time intelligence, and unified administration—that boost security effectiveness and reduce TCO across the board.

Among its many benefits, taking such an approach not only addresses current trends and the security challenges they create, but also puts organizations in a position to more readily adapt to whatever changes the future might hold.

The Only Constant is Change

For every opportunity change provides, there are invariably challenges as well. Just consider some of the top trends facing today's enterprises and the implications they have for information security.

Web 2.0 technologies. The potential to accelerate business processes and solidify customer retention is offset by the increased fluidity of data, a condition that makes it significantly easier to accidentally or purposefully disclose sensitive information.

User mobility. Along with greater 3rd-party access and inter-connectivity with partners, mobility boosts operational efficiency and facilitates new business opportunities. On the downside, it erodes the value of user location (i.e., inside vs. outside) as a security attribute, and exposes a major weakness of perimeter-centric security strategies (e.g., when itinerant users return to a corporate office with infected devices).

Consumerization of IT. Reduced expenditures for device acquisition and management and greater employee satisfaction and productivity are countered by the loss of visibility, trust, and control over a key component of the end-to-end computing path. An exploding population of client devices is also another location sensitive data is likely to reside.

Cloud computing. Public and hybrid options, in particular, deliver greater resiliency, agility, and quicker time-to-market. But they also complicate security by placing critical infrastructure, applications, and data outside an organization's established perimeter.

Targeted attacks. On the rise and with no upside to offer, advanced malware and targeted attacks—ones which are “purpose-built” to breach a specific organization, typically in a very stealthy manner—are manifestations of the increased emphasis hackers now place on stealing valuable data. Depending on your perspective, they also represent a step function increase in threat sophistication, or a step-function decrease in effectiveness for most organizations' security infrastructure.

The net result is that today's enterprises must be prepared to deal with a new, emerging reality where:

- (1) data, compute infrastructure, and users—rather than remaining in fixed locations—are increasingly dynamic and distributed, and
- (2) data is not only the “new gold,” but is also inspiring a new generation of extremely evasive threats and attacks.

The Trouble with Traditional Techniques, Tactics and Tools

The traditional approaches to security currently employed by most organizations have a number of critical shortcomings relative to the new reality discussed above.

Traditional walled-garden techniques rely on having a static environment. Establishing a defensive perimeter to protect all computing resources that reside within it, including data, may have worked relatively well at one time, however, this is no longer true. Mobility, virtualization, and cloud computing not only increase the prevalence of resources residing beyond an organization's physical boundaries, but also of their being able to dynamically migrate back and forth. How is adequate protection provided for resources “on the outside?” What happens when a device that becomes compromised while “on the outside” returns to operate “on the inside?”

Traditional tools rely too heavily on constants. It's not news that IP addresses, ports, and protocols are far from sufficient for defining and enforcing security policies. For instance, knowing that a given traffic stream is HTTP clearly has limited value, because it's the same protocol used by the vast majority of today's applications. However, a similar degree of vagueness is now applicable to a number of other potential policy elements as well. Take your average social networking application. Who's to say whether it's categorically good or bad? At least to some extent, a similar situation also applies for a user's location, the type of device they are using, and even who they are. Inside versus outside, corporate-managed versus not, and employee versus non-employee are no longer definitive measures of trust. The problem with traditional countermeasures in this regard is twofold: for the most part they (1) rely on too few attributes to make a security decision, and (2) treat the value of each attribute as black or white.

Traditional threat protection solutions rely too heavily on "the known." The majority of widely deployed threat protection tools operate on the basis of detecting known threats, or detecting unknown threats operating against known vulnerabilities. But this leaves a lot of ground uncovered. What about the increasing prevalence of advanced malware and other types of threats that operate on previously un-disclosed vulnerabilities? Or attacks that are not based on conventional software vulnerabilities at all—such as a spear phishing email that gets a user to send sensitive data to a hacker?

The impact of these shortcomings is that they hinder organizations from readily embracing many of the trends and technologies required by "the business" to remain competitive. Or, at least they should. Unfortunately, it's all-too-common that "the business" forges ahead anyway, either knowingly or unknowingly absorbing the greater risk this incurs.

Introducing a Smarter Approach to InfoSec

What today's organizations need instead is a smarter approach to information security, one that overcomes the shortcomings of traditional techniques and tools to better account for a new reality characterized by increasingly sophisticated targeted attacks and greater fluidity/portability of users, devices, infrastructure, applications, and—above all else—data. The cornerstones of such an approach include:

- **Placing greater emphasis on data protection.** Not only is data the primary resource being targeted, but also, with user mobility, consumerization, and cloud computing, it is now more exposed than ever. It stands to reason, therefore, that the data itself should be THE leading focal point of a modern security strategy.
- **Placing greater emphasis on threat protection.** This is appropriate because threats—for example, malware, spyware, and malicious insiders—are the vehicle that puts data at risk in the first place. Greater attention is also warranted due to the growing prevalence of targeted attacks and the relatively poor performance of conventional solutions at stopping them.
- **Utilizing security products and solutions that are smarter, by design.** This item speaks to the need to improve the effectiveness of all countermeasures in general, not only in the face of increasingly sophisticated threats, but also as the process of establishing who and what to trust steadily becomes a far more complicated, considerably less black-and-white endeavor.

Before examining each of these elements in further detail, it is important to clarify that placing greater emphasis on data and threats does not eliminate the need to implement and operate other types of countermeasures as

well. Perimeter-oriented defenses, such as firewalls, still deliver considerable value by significantly reducing an organization's attack surface and providing a base-level of protection for all systems within their boundary. Vulnerability management tools are another important example, as they too can substantially reduce an organization's susceptibility to both known and unknown threats.

The point is that taking a smarter approach to information security is not about upheaval and making drastic changes. Rather, it's about steadily re-prioritizing efforts to focus on what matters most in the post-PC, cloud computing era that is upon us: data, threats, and the essential capabilities that will enable organizations to achieve greater security effectiveness with less cost and complexity.

Placing Greater Emphasis on Data Protection

Establishing greater emphasis for data protection breaks down into three primary considerations. The overall goal is to have a complete set of data protection capabilities, everywhere they are needed, and to improve the granularity and, therefore, reliability of data access decisions.

Core data protection capabilities. Data loss protection (DLP) and data encryption are the backbone. For the former, full functionality includes robust data discovery and the ability to detect and prevent policy violations for data in motion (i.e., on the network), at rest (i.e., in storage), and in use (i.e., on endpoints). With the latter, encrypting traffic in transit over networks is merely table stakes. Ideally it should be joined by file/disk encryption for all types of client devices, as well as encryption for removable media, file servers, databases, and storage systems. Additional core data protection capabilities include general access management features and tools—for controlling who can access what data—and full-featured database security solutions (often combining encryption, access management, and other essential controls).

Comprehensive coverage. Data protection capabilities should be available and employed, as appropriate, for all locations and types of platforms—physical, virtual, and cloud. For instance, does it really make sense to encrypt data resident on users' PCs and then leave the same information un-encrypted when it is "deployed" as part of an infrastructure-as-a-service cloud implementation? Similarly, which is better: having DLP at only one location in the network, or having it sprinkled throughout a computing environment based on it being integrated with a range of gateways, such as those for email, web, and content security? To help reduce administrative complexity and boost overall effectiveness, functionality should also be as consistent as possible across all locations and platforms.

Better access management. The preference should be for tools that afford tighter and more effective control over access to data by employing greater contextual awareness. As discussed previously, many policy attributes are far less meaningful or definitive than they once were. Compensating for this condition requires being able to use a much broader set of attributes to build a more accurate picture of the level of trust and, therefore, degree of access appropriate for any given scenario. At a minimum, modern tools should be capable of accounting for what specific data is being accessed, by whom, using what application and device, from where, and when.

Beyond these primary objectives, it also makes sense for organizations to bolster protection for the main conduits to data, namely endpoints, servers, and applications. Once again, comprehensive coverage, functional consistency, and contextual awareness should be among the top criteria when selecting among the multi-function security agents and application-specific security gateways required to get the job done.

Placing Greater Emphasis on Threat Protection

The objective with this second dimension of taking a smarter approach to security is to more reliably thwart advanced malware and targeted attacks. Once again, the recommended approach is comprised of three primary components.

Better prevention capabilities. Network-based intrusion prevention and anti-virus are an essential starting point, but only that. Ideally they should be augmented by solutions focused specifically on neutralizing advanced malware and targeted attacks. Precisely what this means is still difficult to discern given the formative nature of this market segment. However, a couple of techniques that hold significant promise include:

- *Localized intelligence and analysis.* Global intelligence services primarily maintain the currency of a vendor's countermeasures by aggregating and analyzing findings across a worldwide customer base. They are not particularly helpful, however, when it comes to targeted attacks, which are increasingly unique to each organization being attacked. On the other hand, as a per-customer implementation of the same type of technology, a localized intelligence solution should in fact be well suited to detecting targeted attacks. Think SIEM if you will, but with a much more robust set of correlation capabilities and analytics.
- *Sandboxing.* The basic principle in this case is to intercept and then open/operate all unknown or suspicious files and executables in a controlled environment, such as a dedicated virtual machine, to determine whether they incorporate malicious code or not. This is by no means a new approach. It's just that virtualization technologies and the possibility for cloud-augmentation are now making it more practical to achieve.

Faster response capabilities. At the end of the day, even the latest-and-greatest prevention technologies will not be enough. Consequently, better threat protection also needs to include faster response capabilities. This hinges on the ability to identify that something happened in the first place, and is precisely why organizations must strive to (a) monitor everything they practically can, and then (b) actually do something with all of the data that is gathered. Looking for deviations from baselines is a good place to start. So too is better utilizing the visualization and analytical capabilities of existing log management and SIEM tools.

Extensive integration and coordination. Even more powerful than better prevention and faster response capabilities working alone, are ones that work together. This requires integration between the two. More than that, though, it requires intelligent coordination in the form of feedback loops that actually take advantage of available integration mechanisms. For example, one valuable use case would be to have items detected via monitoring and response capabilities subsequently be prevented. Going in the other direction, detected or suspected threats could be used as the basis to modify monitoring profiles, either temporarily for tactical purposes, or perhaps even permanently.

What it Means for a Security Solution to “Be Smarter”

A third infosec priority for today's organizations is the need for greater effectiveness, less complexity, and lower costs—not only for data and threat protection, but across the board. Some of the key mechanisms for achieving these objectives have already been introduced, but deserve repeating due to the need for organizations to pursue them in a much broader manner.

Contextual awareness. The ability to account for greater amounts of contextual information not only helps improve data access decisions, but also is instrumental for improving the effectiveness of virtually all types of countermeasures. The greater detection accuracy and policy enforcement precision that results is the key to having adaptive security that enables rather than hinders business productivity, while still delivering a maximum degree of protection.

Real-time intelligence. The combination of both global and local threat intelligence has the potential to boost the effectiveness of an organization's entire portfolio of threat protection and content security solutions, from intrusion prevention and anti-malware tools to web and email security gateways, and even SIEM platforms.

Integration *and* coordination. Extensive integration and higher-order coordination capabilities act as a force multiplier that closes gaps characteristic of standalone security solutions while also improving operational efficiency.

Unified administration. This item is essentially about extending the concepts of integration and coordination into the administrative domain. At a minimum, it should not be necessary to employ numerous management consoles (or even screens) to enforce policies and obtain visibility that spans instances of a control deployed across all of an organization's platforms—physical, virtual, and cloud. Ultimately, this unification should also extend across different types of countermeasures too, and not necessarily only within a given family of controls (e.g., data protection).

Conclusion

The current crop of business-driven technology trends—especially user mobility, the consumerization of IT, and cloud computing—are steadily increasing the diversification, distribution, and portability of client devices, server infrastructure, applications, and data. The rising prevalence of targeted attacks only complicates matters further, as traditional perimeter-centric security strategies and tools with narrow and too-rigid enforcement models are incapable of handling these changes.

To respond to this new reality, organizations are advised to pursue a smarter approach to information security, one that:

- Places greater emphasis on data protection—by acknowledging that data is the heart of the issue and enabling core/essential controls to effectively migrate with it wherever it resides
- Places greater emphasis on threat protection—by acknowledging the need for better prevention, faster response, and extensive integration and coordination capabilities
- Relies on tools that are inherently smarter and, therefore, able to deliver greater effectiveness with less complexity and at lower cost—for example, by incorporating greater contextual awareness, real-time intelligence, and unified administration

Such an approach is not meant to be implemented overnight. Indeed, some of the tools and capabilities necessary to support it are still emerging. For those organizations that embark on the journey, however, the resulting benefits should be worth the effort. These include having an approach to infosec that:

- Delivers comprehensive and robust protection for important data, wherever it resides;
- Provides stronger defenses against all types of threats, but especially targeted attacks;

- Enables rather than hinders business productivity;
- Improves operational efficiency and reduces security TCO; and,
- Addresses not only the current set of business-driven technology trends and their implications, but—due to its inherent adaptability—future ones as well.

About the Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and analysis company specializing in information security, compliance management, application delivery, and infrastructure optimization. A former META Group analyst, Mark has analyzed business and technology trends pertaining to a wide range of information security and networking topics for more than 15 years. A veteran of the U.S. Navy, he is passionate about helping enterprises address their IT challenges and has assisted hundreds of organizations worldwide meet both tactical and strategic objectives.