WHITE PAPER

Understanding Your Attack Surface

The First Step in Risk-Based Security Intelligence

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

As chief information security officer (CISO), you're constantly being pressed to communicate how you're enabling the business, balancing security risk with business demands, and continuously improving security—not to mention reducing costs, becoming more efficient, and demonstrating return on investments.

If you delve into complex security topics and use jargon foreign to non-technical executive audiences (in other words, typical IT security talk), you'll lose their interest. We've all been in meetings where the presenter missed the mark, and you don't want to be "that guy." So how can you accurately depict the state of your organization's security in a way that everyone can understand? Applying analytics to your attack surface may provide significant help.

This Executive White Paper covers:

- What is meant by "attack surface," and how to reduce risk to your attack surface using existing and emerging technologies;
- Design goals for attack surface analytics; and
- The cybersecurity information that C-suite executives and boards want

Introducing Attack Surface Analytics

Imagine the ability to summarize everything you, your teams and your technologies do to secure your IT infrastructure into a single, meaningful score. If this was possible, it would provide a simple yet powerful way to communicate your organization's security posture to non-technical executives, board members and other stake holders. If this score was accurate, and you could add business context to it, you would have an effective way to demonstrate exactly how your security investments enable the business.

The financial industry has a lot of history defining and using this type of analysis. Companies and individuals can be sized up with a single credit score. Financial institutions frequently develop singular scores for rating risk, volatility, comparison with peers, and many other key indicators. For example, Morningstar, an independent investment research firm, scores investments using a star rating system that relies on many underlying metrics. In the sports world, professional baseball has been experimenting with this idea—a single score that indicates a player's performance and chance of future success (as seen in the movie *Moneyball*)—for years.

A single, valid security score may seem impossible. It's daunting to envision the processes and technologies required to aggregate, normalize and summarize a multitude of factors into a single index, score, or grade—especially given the range of security technologies deployed in most organizations.

At Tripwire, we are working on innovative and emerging new technology called attack surface analytics (ASA). Our goal is to equip CISOs and their security teams with newfound visibility into enterprise attack surface risk, enabling them to communicate the organization's security posture quickly and understandably, especially to executive audiences.

What is Your "Attack Surface"?

Put simply, your attack surface is the sum of your security risk exposure. Put another way, it is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks. A smaller attack surface can help make your organization less exploitable, reducing risk.

A typical attack surface has complex interrelationships among three main areas of exposure: software attack surface, network attack surface and the often-overlooked human attack surface.

- Today, briefing senior executives and board-level leaders on cybersecurity risk is a standard CISO job requirement
- Research shows that skilled communication about cybersecurity risks with non-technical executives is a key indicator of likely success, and often a CISO's greatest challenge
- Unfortunately, some CISOs find it difficult to translate mountains of data from security controls across the organization into business relevance—especially if they have no frame of reference or they're uninterested or pressed for time

Software Attack Surface

The software attack surface is comprised of the software environment and its interfaces. These are the applications and tools available to authorized (and unauthorized) users. The software attack surface is calculated across a lot of different kinds of code, including applications, email services, configurations, compliance policy, databases, executables, DLLs, web pages, mobile device OS, etc.

Network Attack Surface

The network attack surface presents exposure related to ports, protocols, channels, devices (from routers and firewalls to laptops and smart phones), services, network applications (SaaS) and even firmware interfaces. Depending on your infrastructure, you may need to include cloud servers, data, systems and processes to your network attack surface.

Human Attack Surface

Humans have range of complex vulnerabilities that are frequently exploited. One of the great strengths of highly secure organizations is their emphasis on communicating security awareness and safety principles to their employees, partners, supply chain and even their customers (as when using the web to gain secure access to bank or 401K accounts).

Many breaches begin with an exploit directed at humans and it's very clear that malicious intent, inadvertent errors and misplaced trust can all be exploited to cause great damage. Examples at of successful attacks vary widely, (most notably phishing and spear phishing), but a comprehensive index should include processes, physical security, and privileges (including the ability to attach, read or write to removable devices).

In summary, to accurately determine your attack surface risk, all three of these attack surfaces are must be considered. Using existing and emerging ASA technologies can provide improved insight and visibility to your organization's security posture in each of these areas, as well as provide the underlying basis for the score.

Design Goals for ASA

Most organizations have made significant investments in foundational and mature security technologies. These investments generally include vulnerability management (VM), security configuration/compliance management (SCM) and malware defenses. At a minimum, these technologies can combine to provide a starting point for attack surface risk assessment.

Design Goals of an ASA Index (or Score)

- **Summarized simplicity—**An attack surface analytics index should make the organization's overall security posture easy to understand for non-technical executives.
- **Intelligent and intuitive visualizations—**Security intelligence visualizations should simply convey actionable facts within the context of your unique business.
- **Aggregation and normalization—** Existing and foundational technologies such as VM, SCM, and malware defenses should all be included in the most basic ASA index.
- C**apable of drill-down—**Any index or underlying metric, security status, trend or comparison there should be include a way to trace back to the underlying data through drilling down.
- **Supports performance "bands"—** ASA should allow an organization to flexibly set its own baselines, thresholds and goals, as well as the appropriate ranges for each business unit or the overall organization.
- **Capable of comparisons—**The index should be capable of showing comparisons in order to allow business units to track their improvements over time, and provide comparison and trending across the entire organization.
- **Balanced outliers—**When seeking to provide a general condition of overall security posture, the influence of a single variable in the index should not unduly influence the overall outcome.
- **Supports weighting—**The index provides weighting on a per-factor basis.
- **Future extensibility—**The design is extensible to allow for additional factors as they are developed.

Emerging new attack surface analytics can aggregate and normalize underlying data and metrics from various security controls, and our ASA scoring at this time covers VM, SCM, and malware defenses to provide greater visibility into your organization's attack surface.

Defining Attack Surface

"Attack Surface" is not a well-understood term. It sounds confusing and negative. It also seems amorphous and unconquerable. However, just like the terms "attack vector" and "threat vector" are now often used in the security industry, attack surface is a real, working concept—albeit one that needs better definition and boundaries.

For discussion purposes within this paper, attack surface is the sum of IT risk exposure. It crosses all infrastructure, software, and human boundaries, and involves all points of interaction. It's where your assets are vulnerable, either now or in the future.

What Executives, C-Suite and Boards Want

Executive leadership (including the board member) is not typically interested in operational security details such as answers to questions about specific security control metrics. This information is too detailed and will be viewed as "noise" by those outside the IT and security teams. In many organizations, executives really don't care about security risks, but they are required by law to be informed of a significant security breach through regulations, standards of "due care" or because of the fiduciary responsibility.

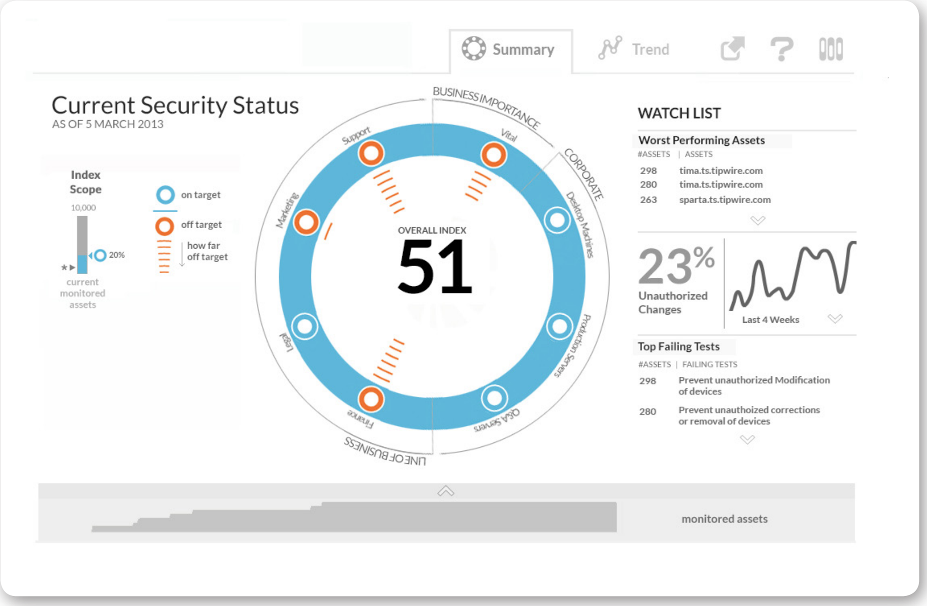
Instead of endless spreadsheet graphs and technical jargon, they want credible information about the organization's security posture over time that provides a frame of reference for trends indicating directionality. Eventually, this type of index could be used for competitive comparisons across organizations, business functions or processes.

It's also important to note that credible information is very different from an opinion. The informed impression is supported by verifiable facts. CFOs are asked for this type of information constantly (and they will often just deliver it verbally on the fly) particularly when the underlying financial frameworks (such as GAAP analysis) are already understood by executives. Over time, they have developed trust with the executive leadership team. Being able to back up the impression in a factual, convincing manner is one of the key ways to build trust with non-technical executive leadership.

As a CISO, you'll want to demonstrate how your group's activities protect and enable the organization. And you'll need to communicate that in ways that non-technical executive teams can understand. Ultimately, ASA technology can allow visibility and communication of security status through the lens of factual and actionable business context, suitable for consumption by executives.

In short, CISOs need what CFOs have—a framework of solid, well-understood metrics that make it possible to inform business and risk decisions by non-security executives. Further, this framework and these metrics will also enable the business to improve understanding and a shared accountability for security results.

The challenge with communicating to non-technical executives is often how to distill the mountains of security control data your team manages into a meaningful visualization. Ideally, you'll limit yourself to one or two slides, and be able to meaningfully communicate (without jargon) this to non-technical executives within 5–15 minutes.



Current Security Status
AS OF 5 MARCH 2013

WATCH LIST

Worst Performing Assets

#ASSETS	ASSETS
298	tima.ts.tipwire.com
280	tima.ts.tipwire.com
263	sparta.ts.tipwire.com

Top Failing Tests

#ASSETS	FAILING TESTS
298	Prevent unauthorized Modification of devices
280	Prevent unauthoized corrections or removal of devices

Fig. 1 Sample Security Analytics Visualization—Visualizing security with business context for non-technical senior executives is a significant challenge. Requirements include aggregating, normalizing, asset management and being able to drill down to underlying metrics for investigation and continuous improvement.

Security Analytics Visualizations

Everything is more understandable with good visuals, which is particularly true for busy executives. You as CISO have probably been asked for a visual presentation at times on the security status of your company or mission, or perhaps to illustrate how a breach occurred. Ideally, you're not only presenting when there's a security crisis, but instead have a regular briefing schedule with the C-suite and board. Often, your executive teams are looking for actionable information, and you're looking to guide and inform them so that the best business decisions can be made.

As CISO, you deal with an array of questions:

- Are we secure? What are our risks?
- What level of risk is acceptable to the company, individual business units and the security team?
- How do we rank our levels of security risk and apply that to infrastructure, software and people to help reduce our risk?
- Is the organization's IT security budget aligned with the right level of risk to support business strategies for capturing revenue and fulfilling customer obligations?
- How is the IT security team enabling—rather than hindering—the business?

ASA technology provides the security visualization scoring (visuals you need to quickly and effectively communicate attack surface risk) for the entire organization—by individual business unit, geographic region, OS/host characteristics, types of risk and exposure, etc.

Summary

What type of CISO are you? Perhaps you're a technical CISO, a hands-on professional who really knows the internals of the technologies you manage. Or perhaps you're a more operational CISO with a security framework mindset—not necessarily the technical "go-to guy," but supported by a strong and trusted team. Or you may even be a more business-minded CISO, where everything the company or mission does works out to a business strategy, a balance sheet and a clear ROI or financial reward that you can clearly articulate to your organization's executives.

Regardless of which category you fall under, it's becoming a job requirement that you show the C-suite and board how IT security enables the business, balances security risk with business demands, and improves overall security every day. Attack Surface Analytics can help you achieve these goals and ultimately help your organization make better business decisions related to its security.