White Paper

The Cloud-based Threat Defense Model

By Jon Oltsik

February, 2010

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Executive Summary

While the economic forecast remains uncertain in 2010, ESG's research indicates an increase in IT spending with a focus on security and risk management initiatives. Why are CIOs still so concerned about security? Which security technologies will they purchase? This white paper concludes:

- **Addressing new and ominous threats takes precedence.** ESG's research indicates that large organizations will purchase new security safeguards for network security, desktop/endpoint security, and messaging security. This indicates a renewed focus on threat defense. Large organizations face a barrage of new sophisticated threats attacking a multitude of technologies; new investments in threat management technology indicate a cry for help.
- **Existing threat defenses are no longer adequate.** The unprecedented volume and scope of new threats also exposes a multitude of weaknesses in existing security infrastructure: tactical tools operate in a vacuum and can't share information or coordinate protection strategies, signature-based technologies are only as effective as their latest updates, and product integration can help ease operations but to a great extent, an organization's security is completely dependent upon its security vendor's ability to detect new attacks and develop countermeasures. Conventional defenses cannot keep up with the volume, speed, and craftiness of the latest threats. Traditional means of threat detection/mitigation are broken and something must be done—soon.
- **Large organizations must embrace the cloud**. ESG believes that enterprises need to migrate from today's point tools and basic integration to a new cloud-based threat defense model The cloud-based threat defense model isn't a product; rather, it is a community of connected security technologies, shared information, security research collaboration, tightly integrated security products, and cloud-based resources. The cloud-based threat defense model's strength is that it is designed to take advantage of the network effect where value is proportional to the number of security nodes that participate.

Large Organizations Will Bolster Security Investment in 2010

With the global recession now a global recovery, large organizations are once again investing in IT. According to ESG research, 55% of SMB (i.e., less than 1,000 employees) and enterprise (i.e., more than 1,000 employees) organizations will increase year-over-year spending on IT in 2010.[1] Additionally, IT spending priorities will also change. IT investments will once again focus on new applications and IT services that help improve business responsiveness, competitiveness, and productivity.

Will this business-centric IT focus come at the expense of information security as it has in the past? Not this time. According to ESG research, 29% of organizations believe that "security and risk management initiatives" will have a significant effect on their 2010 IT spending decisions, while another 26% cite "regulatory compliance." The data indicates that CEOs understand the trade-off between IT risk and reward—new business applications designed to increase revenue, improve communications, bolster productivity, or lower costs must be also be protected with security safeguards in order to manage risk.

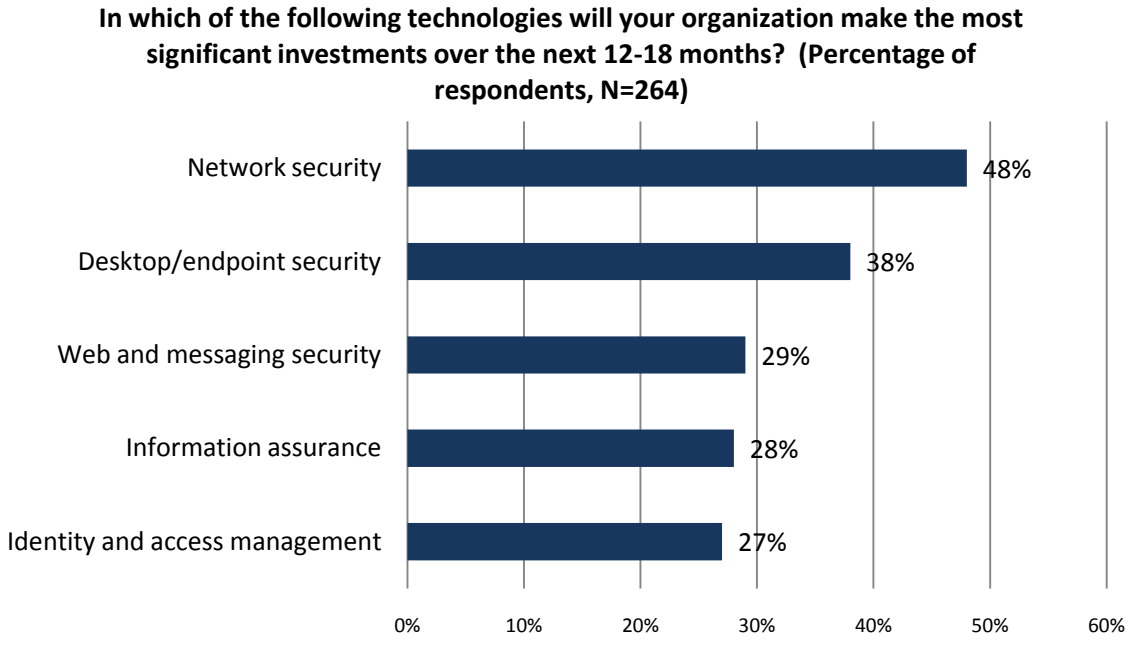
Security Technology Priorities

Security, risk management, and regulatory compliance are broad areas that could be addressed by numerous IT processes or security products. That said, ESG's data seems to indicate that 2010 IT spending will focus on protecting the confidentiality and integrity of assets and data. When asked what type of security products their organizations will purchase in 2010, ESG survey respondents pointed to network security (i.e., firewall, IDS/IPS, network gateways), endpoint security (i.e., desktop/laptop security suites), web/messaging security (i.e., anti-

[1] Source: ESG Research Report, *2010 IT Spending Intentions Survey*, January 2010.

spam, phishing/fraud protection, URL inspection, content inspection, etc.), and information assurance (i.e., DLP, eRM, encryption, etc.) (see Figure 1).[2]

Figure 1. ESG Research on 2010 Security Spending



Source: Enterprise Strategy Group, 2010.

What is Driving this Renewed Security Focus?

In the past few years, security investment was largely driven by regulatory compliance mandates. When the Payment Card Industry Data Security Standard (PCI DSS) mandated regular vulnerability scanning of IT assets or of security event logging, retail and financial services organizations purchased scanning and log management tools and services. While ESG's data indicates a continuing emphasis on regulatory compliance, security technology purchasing plans signify another area of focus: threat defense. ESG defines threat defense as:

> *A series of information security processes and defenses addressing all forms of unwanted intrusions, including attacks on computer systems, malware of all kinds, and even spam.*

Why are large organizations revamping the technologies that make up their threat defenses? Because of:

- **Unprecedented malicious code volume.** According to Trend Micro, the volume of malicious code variants increased by nearly 300% in 2009. SPAM volume showed growth in 2009, making up over 95% of total e-mail volume. While worries in early 2009 centered on Conficker and a possible renaissance of Internet worms, malware tended to be centered on cybercrime like identity theft, fraud, and botnet proliferation. At the World Economic Conference at Davos, researchers estimated that online theft now exceeds $1 trillion annually and will continue to increase.
- **Changing threat vectors.** In the past, most malicious code spread through system vulnerabilities or as attachments in e-mail messages. As users improved vulnerability scanning, patch management, and e-mail hygiene, cybercriminals found another wide open threat vector: the World Wide Web. In 2009, web threats increased by more than 500%—a frightening statistic, but only the beginning. Web threats are popular vectors for several reasons. First, many web applications are vulnerable, making them easy to infect. Second, users trust web sites from household brands like Business Week, Google, and Honda—all of which have been compromised. Finally, Web 2.0 technologies like AJAX, mashups, and JavaScript make

[2] Ibid.

excellent threat proliferation mechanisms for malicious code distribution and execution. Often, threats use multiple attack vectors: a spam e-mail contains a link to a malicious web site, which in turn houses a malicious file. Drive-by downloads have become commonplace. An end-user need only visit a malicious site to become infected.

- **Sophisticated adversaries.** Why does the cybercrime economy exceed $1 trillion? Because it has become a highly advanced, global, integrated market. Cybercrime is based upon a federated network of specialists for hire. Malicious code writers team with botnet owners to launch an attack resulting in the theft of thousands of credit card numbers from the United States. The stolen credit card numbers are then quickly sold on the wholesale market for pennies apiece. After a few transactions in the distribution channel, these stolen credit card numbers are offered on a black market web site with tiered pricing and volume discounts. With a foundation of Internet technologies and global connectivity, the entire cybercrime lifecycle—from planning through attack and monetization—can occur in just days or hours. Sequential downloads are one of the more sophisticated techniques used by data-stealing malware. A PC may be infected for months by malware that has no visible impact on system performance. This latency makes it harder to determine what behavior led to the infection because it's only discovered months later when the original malware downloads another piece of malware, one that does the real damage.
- **New targets.** Microsoft Windows bore the brunt of cyber attacks in the past. This will continue, but new technology proliferation and cybercrime specialization makes other systems attractive marks as well. There has already been a significant increase in malicious code aimed at Apple Macintosh systems over the past few years and ESG expects to see a similar ominous trend with popular smartphones (i.e., Blackberry, iPhone, Nokia, Windows Mobile). Browser-based exploits are also on the rise.
- **Widespread adoption of social networking.** Social networking sites like Facebook are built on a fundamental model of trust, sharing, and open communication. As such, these sites make a perfect nexus for cybercrime. Often, the definition of "friend" in the world of social networking is very loose and the capability for user-generated content poses inherent risks.

Existing Defenses are No Longer Adequate

For years, large organizations addressed security threats with a tactical "point tools" approach. When security operations complained that managing disparate tools had become a nightmare, vendors responded with common management and administration tools that sat on top of independent security technologies—not an ideal solution, but "good enough" for the latest threat du jour that came along. Unfortunately, point tools and cobbled together solutions are no longer adequate. Why? Today's combination of massive threat volume, changing threat vectors, sophisticated adversaries, and new targets simply overwhelms status quo security defenses because:

- **Malicious code volume can bury conventional signature-based security technology.** Traditional signature-based security technologies like endpoint security, antivirus gateways, and signature-based IDS/IPS depends upon a sequential lifecycle. When malicious code is discovered "in the wild," security vendors proceed with a step-by-step process that includes research, signature development, testing, and then finally distribution to their installed bases. This model was fine in the past, but even the most efficient security software vendors now struggle to keep up with the global cybercrime cabal that produces a new variant of malware every 1.5 seconds. Even if vendors could keep up, there is another inherent problem here: as signature databases grow, they consume more and more host-based storage, memory, and processing cycles. It doesn't take long until users are faced with a Faustian compromise between system performance and keeping up with security protection—neither choice is good for the business.
- **New threats exploit integration loopholes.** The onslaught of new web threats gives cyber bad guys a distinct advantage. Many organizations still confuse web threat management with basic URL filtering—an HR-centric technology built to block employee access to pornography, gambling, and hate crime sites. These firms are virtually helpless. Web threats are especially dangerous since they can also circumvent a number of security safeguards. A clever e-mail attack containing a compromised URL will not likely be

blocked by a SPAM filter. A browser-based malicious code script that changes the CEO's DNS settings will pass by antivirus gateways. Infected Facebook content may infect user systems, but it won't be detected by an army of firewalls, IDS/IPS, gateway appliances, or endpoint defenses.

- **Threat management demands a holistic approach.** While each security product has its own limitations, the real problem here is that each security technology is an island unto itself. With limited security integration, there is no good way to get a comprehensive picture of the threat landscape, tune policies, or react to constant changes.

Enterprises Need a Cloud-based Threat Defense Model

As the threat landscape evolved, multi-vector threats became the norm. In a world where malware was delivered first as e-mail attachments and then by spam messages containing links to malicious web sites, it was clear that web-, e-mail-, and file-based threats were really all aspects of the same problem. That meant that it made less and less sense to separate spam blocking at the gateway from malware scanning or URL filtering at the gateway from malware scanning. Today, it is impossible to separate malware protection from spam blocking and web filtering. When threats combine as they have, security defenses must be integrated as well. For example, anti-spyware has now been incorporated as baseline functionality for endpoint protection, whereas five years ago standalone anti-spyware was the norm. Likewise host intrusion prevention is now considered essential to protecting desktops and laptops, and has been incorporated into the endpoint products of leading vendors.

Unfortunately, threat defense integration may not be enough on its own. Why? Threats vectors change, malicious code mutates, and volume continues to skyrocket. Additionally, cybercriminals are in it for money, not fame. As a result, confidential data, including customer records and intellectual property, are more at risk than ever before.

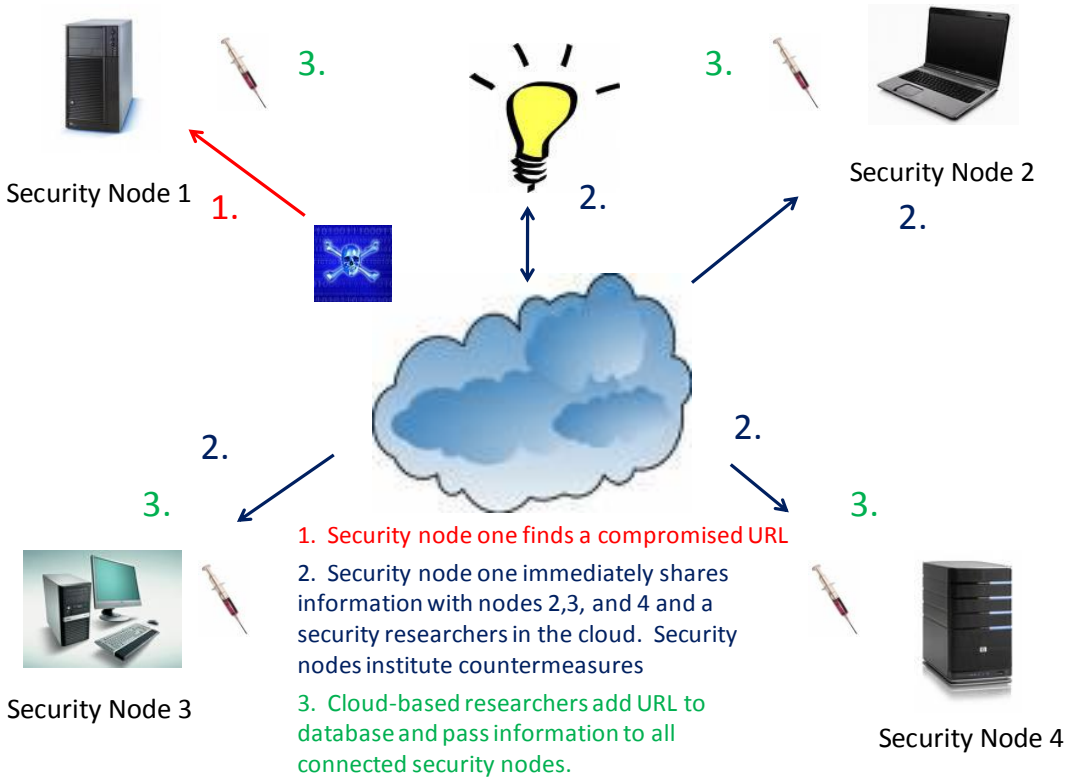
ESG believes that combating these new threats demands a break from the status quo to a new cloud-based threat defense model. ESG defines the cloud-based threat defense model as:

> *An integrated threat defense based upon networked security devices, shared information, interoperability, collaboration, and cloud-based resources.*

The cloud-based security defense model goes beyond APIs or message passing between individual products. Rather, it is based upon:

- **A community of security devices sharing information.** Cyber security is inexorably dependent upon information sharing. Typically, this is done through non-profit organizations (i.e., cert.org, sans.org), vendor consortiums, or specific industry Information Sharing and Analysis Centers (ISACs such as the Financial Services ISAC [FS-ISAC], the Multi-State ISAC [MS-ISAC], etc.). In a cloud-based threat defense model, this information sharing becomes interactive and immediate. When one security device on the network discovers a new malicious code variant or compromised URL, all other connected devices are immediately notified and provided with information about the threat location, properties, and potential impact (see Figure 2). This real-time response enables networked security device community members to take immediate corrective actions (i.e., block a URL, send traffic to a Honeypot, change a firewall rule).

Figure 2. Networked Node Cooperation in a Cloud-based Threat Defense Model



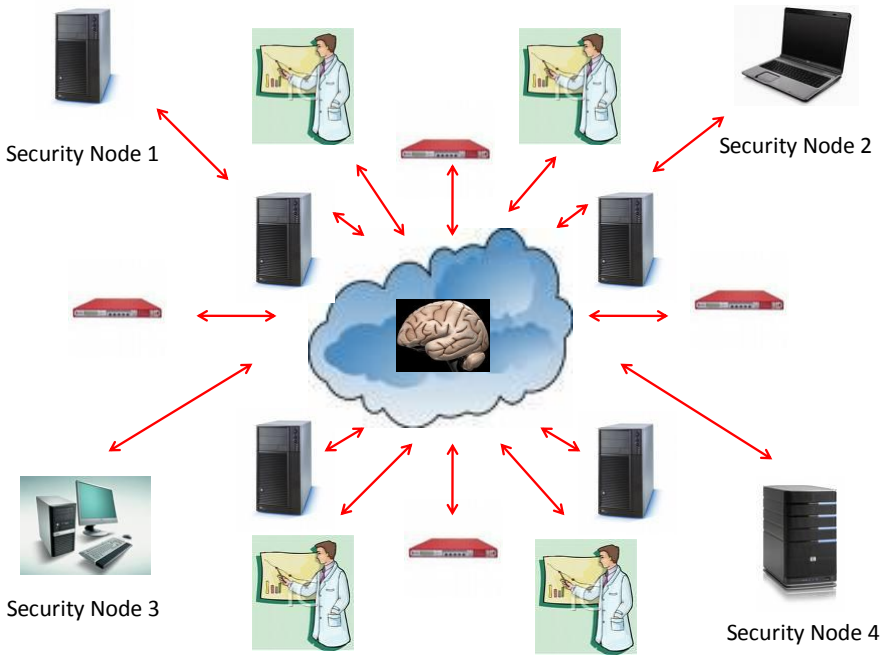
Source: Enterprise Strategy Group, 2010.

- **A collaboration of security research brainpower.** As described above, today's threats take advantage of security product limitations and loopholes. Yes, overcoming these vulnerabilities demands more comprehensive products, but constant collaboration between security researchers who can monitor networked-based security devices, share information, and think like cybercriminals is also required. Armed with network security devices acting as security probes, researchers can then figure out threat management vulnerabilities across product domains, and minimize threat management risks with tight product integration, threat visibility, and central management.
- **Cloud computing defense-in-depth.** A networked model, information sharing, integrated products, and security research collaboration all have a strong dependency on Internet communication, but ESG believes that strong threat defenses go beyond network connectivity alone. Threat detection/mitigation is actually a perfect fit for cloud computing. Why? Rather than depend upon finite system resources (i.e., processors, memory, storage, bandwidth) to run an ever-growing signature database, cloud resources can do a lot of the "heavy lifting" in computing operations. When a user accesses a suspicious URL, a system-based security agent can immediately query the cloud, check to see if it is a known threat, and respond accordingly—regardless of whether the user is on a secure corporate network or accessing the Internet in a public park via WIFI. A threat defense architecture built on a cloud foundation also improves overall threat detection/mitigation efficiency by eliminating the time needed for signature creation and distribution. Finally, businesses benefit as well since compute resources needed for signature database storage and processing can now be freed up improving system performance and bolstering user productivity.

Benefits of the Network Effect

In summary, a cloud-based threat defense model may be the ultimate "network effect"—the protective value of IT security actually increases as more endpoint security agents, security researchers, installed security systems, and cloud computing intelligence participates (see Figure 3). This is true because:

Figure 3. The Network Effect of Cloud-based Threat Defenses



Source: Enterprise Strategy Group, 2010.

- **Cloud-based defenses get better with use.** As in Metcalfe's Law, the value of a cloud-based threat defense model is proportional to the square of the number of connected users. The classic example here is telephone connections: two phones can only make one connection, five phones can make ten connections, and twelve phones can make 66 connections. With the cloud as an anchor, the value of these connections comes from two distinct attributes. First, the more security nodes there are on the network, the more information these nodes can exchange between them or share with security researchers and cloud resources. In addition, the more secure nodes in the network, the more likely it is that at least one of the nodes will stumble upon a new threat, even a targeted attack or new type of threat vector.
- **Security researchers add specialized knowledge and productivity.** As previously described, cybercriminals have become more specialized with attacks becoming a communal division of labor. Cloud-based threat defenses even the playing field by providing real-time information to specialized security researchers. By sharing information, expanding the security analysis, and collaborating on threats, vulnerabilities, and risks across the security spectrum, security researchers can respond more efficiently and more effectively.
- **More cloud computing resources for malicious code analysis, signatures, and storage.** Security is a resource-intensive business requiring an extensive investment in network probes, bandwidth, server hardware, storage capacity, and highly skilled personnel—yet another reason why point tools are no longer adequate. As threat volume and sophistication grows, it makes more and more sense to take advantage of this capacity and offload local security processing tasks to the cloud. This model has already taken off for e-mail security, with e-mail hygiene performed as a cloud service along with a local change to local MX records. ESG believes that it is inevitable that the cloud-based threat defense model will follow this widely accepted example.

Trend Micro: A Cloud-based Threat Defense Model Leader

Cloud-based threat defenses are not a blue-sky analyst vision, but rather a transition that is already occurring in the marketplace. One of the early innovators driving this shift is Trend Micro, a pioneering security company. In late 2007, Trend Micro shook the industry when its CTO, Raimund Genes, declared that the security industry's product-centric focus was no longer capable of keeping up with the volume and sophistication posed by cybercriminals. Genes then suggested a new model based upon cloud-based resources.

Over the subsequent years, Trend Micro changed its product design and support model to fulfill Genes's vision. As a result, Trend Micro has become a visible leader in cloud-based threat defense. The company's Smart Protection Network serves as its cloud-based backbone, coordinating its activities with a global network of Trend Micro security gateways and endpoint software. The Smart Protection Network aligns with ESG's cloud-based threat defense model because it is:

- **Anchored by its extensive installed base.** As a security leader, Trend Micro sells products to consumers, SMBs, and enterprise organizations across the globe. Trend's technology is also embedded in third-party devices. Once installed, all Trend Micro products combine for the "network effect" described above by providing automated smart feedback to one another as well as to Trend Micro's far-reaching team of security researchers.
- **A provider of integrated web, file, and e-mail protection.** Multiple security technologies reinforce each other to substantially increase overall security effectiveness. In addition to product integration, all Trend Micro offerings are also integrated with the cloud-based resources of the Smart Protection Network. All data collected by Trend Micro is then automatically cross-correlated across web, file, and e-mail vectors, and is augmented by Trend Micro security researchers. This level of integration provides one of the only real-time protection solutions available.
- **Positioned to take advantage of cloud-based compute power, storage capacity, and omnipresence.** Trend has the cloud-based resources to keep up with exponential malicious code growth. Furthermore, Trend Micro's Smart Protection Model offers an efficient avenue for signature distribution. Multiple network protection points, such as corporate gateways, mail servers, and endpoints, can be immediately updated with new threat intelligence. Network resources are protected through a combination of local and cloud-based signatures, with an emphasis on the latter. In this way, the Smart Protection Network delivers a defense-in-depth architecture, safeguarding systems whether they are connected over trusted corporate networks or the public Internet.

Given Trend Micro's Smart Protection Network, CIOs looking to move from tactical "best-of-breed" product-centric security to a more global cloud-based threat defense model would be well-served by researching, testing, and evaluating Trend Micro's offerings.

The Bigger Truth

Enterprise IT managers have often been forced to live by the old adage, "if it ain't broke, don't fix it." This is far from an ideal strategy, but in many cases, it works—installed Gb switches and 32-bit operating systems may not be state of the art, but they do get the job done. Unfortunately, this laissez-faire approach doesn't work with information security or, more specifically, with threat management. Cybercriminals are extremely ambitious and savvy, constantly looking for the IT equivalents of open windows and unlocked doors. Each new threat is a bit more sophisticated than the last, or they target at a different type of system, or they are delivered as a zero-day attack before technology and security vendors can respond.

In truth, security professionals should live by a different maxim: "an ounce of prevention is worth a pound of cure." In other words, security is all about anticipating the next attack to reduce risk and limit damages. This approach demands constant adjustments, information sharing and analysis, and split-second decision making. The old tactical product-centric security model does not align with this proactive approach; the cloud-based threat defense model does.

IT and business decision makers who ignore the increasingly menacing threat landscape may not realize what they are up against. It isn't a question of *if* your organization will be attacked—it is a matter of *when*. Leading CISOs will recognize these truths, sell cloud-based defenses to their bosses, and create a cloud-based threat defense network as soon as possible. To paraphrase another famous quotation, organizations that hesitate (with cloud-based threat defenses) may truly be lost.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0128 | www.enterprisestrategygroup.com