

2006 Security Incites and Predictions

What are the Security Incites?

Annually, Security Incite will publish a list of the key “trends” and expectations in the security business for the next year. Called “Security Incites” and written from the perspective of the end user (or security consumer), Incites provide direction on what to expect, assisting the decision making process as budgets and technology adoption plans are finalized for the upcoming year. Each Incite provides a clear position and distills the impact on buying dynamics and architectural constructs. Incites also set the stage for Security Incite’s upcoming research agenda.

What’s the difference between a “Security Incite” and a “Prediction?”

Predictions are things we expect to happen within the next 12 months, and tend to be more event-oriented. The Security Incites provide a broader perspective across the security domains and can take a longer than 12 months view.

2006 Security Incites

1. No Mas Box (Less Boxes, More Functionality)

Users will increasingly revolt about adding yet another narrowly focused security appliance into their network and actively examine new “simplification” architectures. New Unified Threat Management (UTM) products, using blade servers and virtualization technologies, appear in 2006 putting vendors that license key intellectual property at a disadvantage. Management of the integrated UTM environment will remain difficult through 2007.

2. Get the NAC!

The increasing number of ingress points into corporate networks (mobile, contractors, VPN) forces users to migrate to a virtual network infrastructure with a secure net and an unsecured net. Network Admission Control (NAC) architectures gain traction in 2006 to facilitate this architectural construct, but do require homogeneity of equipment pushing the pendulum away from best of breed providers.

3. Who are you?

Identity Management (IDM) breaks out in 2006, as ROI-driven password management and single sign-on (SSO) initiatives are deployed en masse. Smart users increasingly figure out that strong and centralized IDM provides “good enough” authentication and authorization for compliance purposes, accelerating market growth in 2H 2006. Yet, identity federation continues to lag in a cloud of useless vendor bickering and standards immaturity until mid-2007. Token-based

authentication finally hits the wall, as passwords remain good enough and no compelling alternative appears.

4. Stay Out of Jail

Compliance continues to generate tremendous hype, but largely remains a red herring throughout 2006. Smart users will use the compliance word to get funding for critical imperatives (perimeter redesign, identity management) and sufficiently document their processes to keep regulators happy. Those not so smart users figure encryption is a panacea and buy some; ultimately realizing making encryption work on a large scale basis hasn't gotten any easier.

5. Losing The Religion

Everyone finally realizes in 2006 that regardless of technical approach (IDS vs. IPS vs. firewalls vs. anomaly detection) it's all about detecting and blocking malware quickly and effectively. Users expect to see multiple techniques implemented, spurring another wave of consolidation as vendors look to bring complete enterprise-class UTM solutions to market.

6. Endpoint Hostile Takeover

Driven by the prevalence of unwanted applications, internal zombies outbreaks, and documented information leaks enabled by key loggers and spyware, users will increasingly lock down endpoint devices, despite pushback from the business users. Limitations of the Windows XP security model makes lockdown difficult in 2006, but much easier when Microsoft's Vista operating system is ready for deployment beginning in 2007.

7. Bad Content is Bad Content

Given "innovation" by spammers and fraudsters, keeping content filtering algorithms accurate and timely is proving very difficult for content-focused security vendors. In 2006, heuristics-based detection cocktails fall out of favor, pushing the pendulum back towards signatures that favor entrenched AV vendors. Users increasingly embrace "in the cloud" content filtering for e-mail, IM, and web traffic because it allows them to get rid of another box in the perimeter and stop worrying about exponentially increasing message volumes.

8. Security Management (oxy)Moron

Stand-alone security information management (SIM) plateaus in 2006, as consolidation continues and the need for large-scale system integration makes acceptable "time to value" out of reach for all but the largest enterprises. Closed

correlation systems increasingly take root as users swing towards homogeneity and ratchet back expectations on which devices really need to be integrated into the management system, while leveraging the reporting infrastructure for compliance purposes.

9. Services

Managed Security Services provide increasing value in terms of both operational capabilities and content filtering. Users realize that removing threats “in the cloud” provides better bang for the buck for mature technologies (firewalls, IPS, anti-spam, gateway AV, web filtering). The biggest challenge in 2006 will be integrating operational and reporting capabilities across internal and MSS spheres of control.

10. Built to Last (Securely)

As application security functions are further integrated into UTM platforms in 2006, focus shifts to actually building software securely. The high tech vertical will lead the way in embracing behavioral changes for developers, source code analysis tools, and techniques to protect data at rest. New Web 2.0, SOA and on-demand application architectures with better security models increase in importance.

11. It's Time for “Stupidity School”

Though distasteful, security professionals will be forced to undertake a structured and comprehensive education program to stop employees from doing stupid things. Given the sophistication of attacks and the difficulty in stopping them at the perimeter, educated personnel may be the only defense.

12. Battle of the Titans

The big will continue to get bigger in 2006, as frenetic consolidation continues as product line breadth outweighs actually functionality. By the end of 2006, it becomes apparent that the real battle is between Cisco and Microsoft to control the architecture of networks and applications moving forward. As with other huge “marketectures,” users are caught in the crossfire, but 2007 will see enough additional functionality for those embracing homogeneity to see a wave of infrastructure upgrades. Vendors not strongly aligned with one of the two titans face irrelevance by 2009.

2006 Predictions

1. M&A continues, with small deals to acquire innovative technology being most prevalent. No blockbuster security deals (> \$500 million) will happen in 2006.
2. Vendors relying on licensing OEM technology find a world of hurt, as important intellectual property is acquired and licensing terms become increasingly unattractive. The UTM blade architecture makes intellectual property valuable real estate and those with strong IP positions see higher value exits.
3. Microsoft has limited positive impact on security in 2006 (despite the introduction of OneCare), but the AV market is living on borrowed time. Integrated security and endpoint presence for enforcement provides a visible hook for MSFT to catch up to Google.
4. Increasingly bigger VARs start flexing their muscles and make or break a number of vendors in 2006. Those “made” vendors get big M&A outcomes in 2006.
5. Continued vulnerabilities in AV and spyware products attract the attention of tort lawyers who target AV companies after the resurgence of a well-known attack renders most SMBs defenseless. Larger enterprises with multiple layers of defense escape unharmed and point to the criticality of a layered defense strategy.
6. Open source security stumbles in 2006, and the changing business models and decreasing effectiveness of Nessus, Snort, and MailAssassin are not well received. Service providers make significant investments to drive a future renaissance in open source UTM software, SIM, web filtering and encryption to dramatically reduce their cost to deliver MSS offerings.

About Security Incite

Security Incite is an industry analyst firm specializing in the information security market. Our mission is straightforward: Help subscribers protect their information assets more effectively by making better decisions. We provide timely analysis on information security topics and publish detailed, actionable reports to ensure that high profile projects are executed successfully.

Security Incite was founded to address a real need to provide objective, relevant and inciteful security research by focusing on what's right, as opposed to what pays well. Focusing on bold, thought-provoking and irreverent analysis, Security Incite helps organizations make better decisions. Our tagline is "No Bias. No Bull. Real Incite," which does a good job of explaining our philosophy and our focus.

Security Incite publishes *The Daily Incite*, a unique, refreshing, no holds barred newsletter about the information security business. And you never know who is going to be on the receiving end of one of President Mike Rothman's famous rants. As a bonus, subscribers also receive Security Incite's BUYING SECURITY PRODUCTS ebook. To subscribe, send email to dailyincite@securityincite.net or visit <http://securityincite.com/dailyincite>.