

Lockdown!

Stratecast Partners' Michael Suby:
"Security ecosystem" may be the
best defense against a world of hurt.

Suby recommends taking a holistic approach to security programs and spending.

MICHAEL SUBY is co-program manager for the Communications Service Strategies & Opportunities (CSSO) Analysis Service at San Antonio, Texas-based Stratecast Partners, with a specialization in assessing VPN, security, managed services, and other business communications solutions. Previously, Suby worked at Qwest Communications International Inc. and AT&T. He recently spoke with Bill Laberis, F5 World editor in chief.

Q What are the key factors for the attention being paid these days to network security?

A There are several and they are all important. There is a compelling need to protect vital corporate assets, which is what network information is. There are mounting concerns about the difficulty in meeting the regulatory compliance requirements of mandates like Sarbanes-Oxley and HIPAA, while at the same time maintaining the reliability of the business. And finally, you have to consider the accelerat-

ing pace of openness of today's networks to accommodate mobile workers as well as partners, customers, and suppliers. There is a lot to be concerned about.

Q Increasing expenditures must be a concern as well?

A Exactly. At the same time organizations are scrambling to protect their networks, there is a rising tide of concern about the expense of doing so. You have to make a concerted effort to be pragmatic about expenditures for security solutions. Specifically, companies can no longer afford to add independent islands of security solutions that aren't connected in some planned way with what is already installed and running. The norm too often has been for companies to take care of their most pressing security concerns with point solutions, all the while missing the opportunity to look at security investments and expenditures in a holistic or systematic way. By looking at security from this holistic approach, it is possible to get more



than a dollar's worth of protection from each incremental dollar spent because you can leverage a security ecosystem and not just solve a spot problem.

Q Security spending seems to swing from centralization to purpose-built devices and lately back to centralization. Is there a trend, and is best-of-breed dead?

A We won't ever see the pendulum swing completely one way or the other because there will always be a certain level of interest in buying point solutions. For example, an organization may want to manage certain security solutions completely on its own, keeping them isolated from other elements of the security ecosystem. Plus, where security investments have already been made, it is not always prudent to just rip out and replace.

All that said, what we are seeing from our customers is a strong desire to look at solutions that build multiple security functional domains together. For example, it seems that things like antivirus, intrusion detection, and network access might almost naturally go together and be provided by one vendor with one centralized management environment.

Q What are the advantages of one method over the other?

A Each approach has its advantages. Enterprise circumstances vary such that the advantages are unique to each enterprise. For most, a hybrid solution will eventually become the more prominent approach: a combination of network-based managed services and premise-based solutions. We are still a couple of years ahead of that point because there is a level of maturity that needs to occur before it all comes together in a hybrid approach. In fact, you are now seeing certain partnerships evolve where providers and vendors that formerly were going in different directions are now partnering and trying to provide customers the best of both worlds.

The key point about hybrid security solutions is that they provide multiple layers of protection, which is what customers need and want.

Q Is there a companion need for discrete groups like applications, networking, and security to work together more effectively to build a security ecosystem?

A Yes, absolutely, and in fact this is already changing in many businesses. More and more frequently, you'll find groups like security and networking reporting directly to the same executive or office. Moreover, the application owners are having a much greater say in the discrete elements of the overall network security strategy since that strategy can impact the viability of the applications they deploy. In this regard, the network security people are becoming more of a supplier of security services directly to the application owners.

Q Speaking of security costs, is security ROI becoming more provable?

A Over time it will. But security spending will probably always have very qualitative aspects. Security spending is not easily quantified, in part because the threats are not predictable. Leading security solutions provide a high level of extensibility, incorporating multiple security functions in an orchestrated manner, as well as adaptability to meet the fast-changing needs of the enterprise and flexibility to change quickly.

Q Are there security practices or trends that have particular interest for you?

A Yes, that would be the trend toward not undertaking security projects just for security's sake. Increasingly, it is important that when you look at points on the network where security technology is being deployed, you find other technologies and functions are being deployed as well. For example, it is common to add application acceleration to the same points where security is layered. In this regard, it will make sense over time that it is not just security that a vendor is supplying, but security plus elements of improved application performance.

Q What will be the prohibitive factors to the establishment of this security ecosystem?

A There are impediments in organizational structure in terms of deciding what concerns or needs should be addressed first. And the decisions reached may not necessarily follow the most efficient path leading to this unified or holistic approach to a security ecosystem. A unified solution may not necessarily have the specific capabilities the enterprise is looking for at the current time, so the business may continue down a path of best-of-breed.

Also, just as there is an installed base of technology at most companies, there is also a specific base of skills that can't be changed overnight. Instead, companies have to map out how they are going to go from point A to point B in some logical fashion that doesn't result in a disruption to the end users' experience, or a disruption of the business.

Nonetheless, today's organizations *must* ultimately move to greater efficiency in terms of their security administration and a better end-user experience in terms of their application performance.

Q What security technologies or services do you think merit close attention these days?

A There are a growing number of network access control solutions out there by a lot of well-established and newer suppliers, which makes it challenging to pick the right one. We're also seeing an evolution of enterprise reporting capabilities, particularly as they relate to regulatory compliance.

What's needed in the compliance area is a systematic means of gathering relevant information to help businesses understand where they are in terms of compliance as well as to help them make the best type of decisions to move forward. Finally, there is a lot of activity in this area of data leakage, which focuses on making sure that sensitive and valuable information is distributed properly and securely, and that distribution can be easily monitored.

Q What are the traits or characteristics of a good security vendor?

A There are a number and their importance varies with the enterprise. Certainly, look at how well a vendor's solution fits into the existing network and security infrastructure, and how extensible it is. Is the vendor selling products and solutions that are scalable and work well with other vendors' solutions?

Also, organizations should look carefully at the long-term viability and financial stability of a particular vendor during the evaluation. *