Should IT Vendor Consolidation Extend to Endpoint Security?

As IT organizations try to simplify vendor management, many are asking if consolidating on a single endpoint security vendor makes sense. It could hinge on the existence of an overall security framework. Here are some questions IT executives should ask themselves and their security technology partners.

Endpoint security is more challenging than ever, thanks in part to the consumerization of IT and the Internet of Things. Enterprises are tasked with maintaining a wider variety of network-aware devices, ranging from tablets, smartphones and point-of-sale terminals to RFID cards and tags.

“Where endpoints are concerned, the core security objective is to identify trusted devices and manage corporate data,” says Brent Conran, chief security officer at Intel Security.

Adding to the complexity is the prevalence of numerous, disparate point solutions for endpoint security, including antivirus, phishing, intrusion detection/prevention, identity management, access management and data loss protection. For years, technology companies specializing in one or more of those products have found willing buyers among most enterprises for whatever the source of the latest cyberattack had been.

“Systems and business processes are becoming increasingly integrated,” says Patty Hatter, chief information officer at Intel Security. “It is less likely that a security breach can be contained to a single system, application or platform.”

So it’s not surprising that many IT executives are starting to ask whether it makes sense for those multiple vendors to be consolidated into a much smaller number—maybe even just one.

Simplifying should begin by focusing on an enterprise-wide, coordinated security and privacy architecture, advises Conran. Maintaining a laser-sharp focus on your security framework can enable the business to take advantage of multiple endpoint technologies while addressing the numerous other challenges involved in protecting corporate assets.

“If you have a well-established cybersecurity architecture, you can plan your budgets, tactically and strategically, along the way,” says Conran. “You can make more swift and expedient decisions that support your architecture and improve your security posture, and avoid making purchases that you later regret or that create redundancies and complexity.”

Whether that framework is designed, built and/or managed by an internal IT team or—more likely—through a partnership with a trusted partner in the security market, committing to such an architectural framework is what matters most. But that commitment requires a lot of planning, which in turn means a lot of important questions need to be asked and answered. These include:

1. **Should we view the market for endpoint security products differently from that of networking or storage?**
   The wide variety of network-aware devices in place today only accentuates the breadth of the endpoint security market. Although it is a quickly changing marketplace, you can still make lasting decisions and retain return on investment. The key things to look for are vendors with a consistent architecture, published application programming interfaces, standard connectivity models and flexible management tools.

2. **Should we build that architecture ourselves and insist that vendors hook into it? After all, don't our people know our systems and processes best?**
   A big challenge with the "build-it-yourself" model is that it often lacks 360-degree, end-to-end visibility into security vulnerabilities. Relying on only internal IT/security teams not only takes those team members from other tasks that can benefit the business, but can also actually put the organization's business at risk if the team lacks sufficient expertise and experience in vulnerability assessments. It can also significantly increase the time required to spot and remediate security problems if the organization tries to attack the problem internally. Endpoint security is a rapidly evolving segment where most internal teams often lack the specialized knowledge to understand how endpoint security risks can throttle a business. For those who pursue the build-it-yourself approach, a comprehensive risk assessment from a dispassionate, experienced third party to fully grasp where vulnerability gaps may exist is recommended. This will help ensure that any overlooked areas are accounted for and will prevent a potential outage, loss or exploit from harming your business.

3. **Does it make more sense to just select a single vendor and its products, rather than create a framework that still has multiple product vendors?**
   The constant state of change in endpoint security makes it more essential than ever to look for vendors with a depth of knowledge in this market—something that not every security solutions vendor necessarily can offer. Using multiple vendors may offer an important overlap across products to ensure full coverage of potential gaps in security defenses. However, selecting a vendor with a broader and proven portfolio will allow an organization to reduce the number of vendors required to accomplish the goal, as well as cut down on expenses and management complexity. Your primary goal should be to have a comprehensive framework that ensures the most reliable, flexible and future-proofed approach to endpoint security. Once you have your framework, it will be easier to determine areas that you can simplify with one versus multiple vendors.

4. **How do I guard against making the wrong selection of endpoint solutions vendors?**
   First, create open, flexible solutions that aren't tied exclusively to specific software platforms. After all, the days of Windows-only shops, or even infrastructures built around proprietary operating systems, are long gone. Today's endpoint security frameworks must account for all major software platforms, including Windows, Linux, UNIX and proprietary approaches. It also should be able to support different architectural approaches, such as traditional on-premise, public cloud, private cloud and even hybrid solutions.

Next, be sure to take into account the accelerating rate of change in endpoint infrastructure. Because of the rapid adoption of new endpoint technologies, the best approach is to be prepared for change by creating an architecture that will allow you to easily plug in a new solution without disrupting operations or exposing vulnerabilities.

Finally, be sure to do your homework on potential vendors with which you may partner on technologies and on solutions architecture. You want to make sure you align your organization with a trusted partner that has financial strength and a stable technology base that combines a comprehensive and integrated product portfolio with a clear roadmap for the future. Also, be sure your partner brings a sophisticated threat-detection capability to the relationship. Its approach to security should view threats at a large, global level and be able to demonstrate multiple layers of proactive defenses from a variety of inbound attack vectors. Lastly, your partner's solutions need to integrate seamlessly into an overall threat detection framework in order to provide sufficient fortification and reinforcement of that framework.

Intel Security's Approach to Endpoint Security Architecture

Intel Security is a leader in both endpoint security products and comprehensive security frameworks that enable our products and those from third parties to work together.

Our Security Connected platform is a tightly integrated, unified framework for securing data across different endpoint devices, applications, security products and management solutions. Our approach enables open, flexible solutions that scale with your organization's needs as they change. It also helps you to simplify security management, enable the integration of best-of-breed endpoint security products and reduce operating costs.

If you plan to build your own architecture, our security solutions architects can support your internal staff and offer insights gained from a deep and broad knowledge of security vulnerabilities.

Interested in simplifying your environment? Security Connected comes with a real-time messaging bus and collective threat intelligence to maximize business resiliency and enable organizations to consolidate the number of security products and vendors to the most appropriate level.

Additional insights and suggestions are available through Intel Security's Security Connected Reference Architecture. From best practices to functionality and technical considerations, you'll find resources to help your organization learn how to enable connectivity of security products that are already installed and those still under consideration.

By supporting multiple products, services and vendor options, Security Connected helps organizations make smarter, more strategic decisions on endpoint solutions vendors without forcing those organizations to pick either a single vendor or continue to deal with an unwieldy number of suppliers with disparate, often incompatible solutions.

For more information on the benefits of partnering with Intel Security to define, build, deploy and manage a comprehensive endpoint security framework, go to

www.mcafee.com/us/enterprise/security-connected/index.aspx.