Evaluating Multi-Layered Security
Security is top of mind for all IT managers these days. Preventing loss of data and securing access are top priorities. Ensuring comprehensive, end-to-end security, however, is much more challenging. Layered security solutions promise true secured access, but achieving these results takes time and the right solutions. Learn more about layered security for your organization. Topics covered include: Authentication, encryption, remote access, secure end-to-end messaging, and much more.

For a generation or more, “defense in depth” has been a byword for IT professionals tasked with building more-secure systems and applications. The idea is simple: since no one security methodology is perfect or universally applicable, the only cost-effective and functional strategy is first to layer them; second, to assess continually, and bolster weakest links; and finally to architect whole systems to insure downside mitigation. For example, encrypting critical databases so that if the network is breached, those seeking illicit entry can’t retrieve anything valuable.

The pragmatic philosophy of defense in depth is especially resonant for the enterprise, faced with the prospect of assembling and maintaining complex systems to bolster business productivity. It’s almost inevitable that the user-facing elements of these systems will be heterogeneous, and that much software and many solutions judged ‘good’ by a majority of business stakeholders – for productivity and cost reasons – will come with no great level of security. In fact, as all IT folks know, many of these systems are not secure. Even making these systems “arguably secure” is only possible within short time-windows, usually by by applying the latest round of patches, developed in response to the round of recently discovered exploits. The bad guys know this too, unfortunately. And they’re getting smarter at exploiting numerous weak links, both machine and human, that any complex enterprise presents to the world.
## COMPONENTS OF A MULTI-LAYERED SECURITY STRATEGY

<table>
<thead>
<tr>
<th>Sub-Frame</th>
<th>Components</th>
<th>Will Enhance</th>
</tr>
</thead>
</table>
| • Security Consulting Services  
• Security Monitoring Services | • Service provider will assess, measure and document current infrastructure, IT practice and staffing, business requirements; will then recommend, assist in product evaluation and selection, and implement a secure architecture | • Maintain brand reputation  
• Insure customer privacy  
• Assure global regulatory compliance and market access  
• Reduce risk of litigation  
• Target total IT investment  
• Reduce TCO  
• Improve operational resilience  
• Insure data integrity |
| • Network Monitoring apparatus and associated services. | • Service provider will monitor edge-network and other onsite defense and detection apparatus, notify and intervene as appropriate to mitigate damage and defend client assets | • Provides total situational awareness of infrastructure status, rapid detection and active mitigation of intrusions and threats.  
• Improves total security and operational resiliency.  
• Minimizes downtime lost to incidents.  
• Minimizes incidents by proactively responding to threats before exploits are implemented. |
| • Device Management  
• Virus and Malware Protection | • Remote file access, wipe, tracking, policy implementation and updates.  
• Real-time detection and quarantine of active viruses and malware. | • Cost-effective management of diverse and mobile devices.  
• Reduction of loss.  
• Control of IP.  
• Real-time protection of agents within and beyond the network edge. |
| • Endpoint data encryption | • Seamless architecture for applying file-based encryption and controlling file-level access for files on and off your premise. | • Core control of IP, PII and other regulated data without workflow disruption.  
• Fail-safe against unauthorized access of laptops and mobile devices, and against penetration of in-house data resources. |
MULTI-LAYERED SECURITY

The threat landscape, therefore, keeps changing. And the only practical response is multi-layered security. At base, multi-layered security is an expression of defense in depth, also incorporating the notion that security, however “holistic” the solution, must clearly address the concerns of diverse stakeholders for data integrity, operational efficiency, customer and employee privacy, business resilience, compliance, and litigation.

To achieve a truly multi-layered approach you need to start with a framework in mind for breaking down the problems of enterprise IT security and matching them to a solution. The most practical framework is the simplest that comprehends the problem, both technically, and in terms meaningful to the business.

Most IT professionals already know this. What they may wonder more about is how to evaluate multi-layered security solution portfolios; how to avoid what security-expert and Blowfish-cipher-creator Bruce Schneier characterizes as: “layering one mediocre security measure on top of another mediocre security measure” (see http://www.schneier.com/blog/archives/2010/03/should_the_gove.html).

To achieve a truly multi-layered approach you need to start with a framework in mind for breaking down the problems of enterprise IT security and matching them to a solution. The most practical framework is the simplest that comprehends the problem, both technically, and in terms meaningful to the business.

Also, it is important to note that applying the framework to evaluate competing products and implementing a layered security portfolio must be accompanied by what, in most cases, will be budgeted and braided into process as a parallel effort; namely that of automating infrastructure management, ensuring fundamental data preservation, and business continuity. While the “pointy end” of security is in the services and apparatus protecting data, identifying virus threats, evaluating network traffic and user behavior, and imposing policy, the base is in system and configuration management, patch administration, backup, and similar tools and processes. Or to put it another way: the deepest layer of multi-layered security is knowing that all your servers, network infrastructure, and endpoints are appropriately hardened and patched up to date; all your data is safe on the other side of the mountain; and being able to intervene nimbly when the red lights start flashing on the network monitor. Admittedly, in today’s complex enterprises that level of assurance can be hard to achieve. Rather, as Schneir notes in the article quoted above: “We’re all stuck with software written by who-knows-whom ... And we need to figure out how to get security from that.”
PARTS OF THE FRAMEWORK

It's easiest to see the value of the framework when it's applied bottom-up, from the “rubber meets the road” details of securing individual PCs, laptops, and mobile devices in real-time, to the highest-order plane, where systems and policy are managed, and where emerging threats are evaluated and responses developed.

User security is the first component you need to consider. When employees are under high pressure to produce results, people tend to be fallible. They prioritize the tasks at hand over procedures like corporate use policy. While policy management is important, it will never be the end-all be-all of security.

This means your corporate data is in constant danger of being exposed on laptops, USB sticks, portable hard drives, and removable static media, no matter what policies you set or try to enforce. The most pragmatic approach is to encrypt corporate data, using unobtrusive software and establishing simple, robust protocols for authentication, decryption, and file opening within approved applications and contexts. The most practical solutions for encryption are file- rather than volume-based, so secure data harmonious with the way end-users typically think about and manage the information resources needed for their work. This approach offers protection for data in transit among mass-storage devices, across networks, and on applications at the point of use. Such flexible encryption solutions offer a reliable layer of security for data that runs beneath applications, VPNs, corporate intranets, and other tools. Thus, even if an employee writes their desktop password on a Post-It and sticks it on their laptop (and the laptop is then stolen) your data will still be safe.

Endpoint security is the next framework component. This is the basic security cornerstone of virus protection which can be delivered via installed software or “as a service,” working in tandem with management appliances, software and services that let you enforce security policies on diverse equipment across the network and the internet. For example, you want a security system that blocks and removes questionable applications, or uses remote updates to block browser access to questionable URLs, thus security the endpoint. Since the internet is the source of so many security threats, a truly complete solution for endpoint security might even offer features for enhanced safety when accessing regular or enterprise-specific web applications. One approach some makers are exploring is to virtualize the browser: putting a more-secure instance of a popular browser in a virtualization sandbox. The approach reduces or eliminates the possibility of malware content compromising the browser and thereby accessing the file system, network, or local CPU and memory.
PARTS OF THE FRAMEWORK (CONT.)

The enterprise network – and the pivotal role of network security – rides one level higher in the framework stack. Network security occupies a privileged position in a multi-layered security model, because in practice, most threats are carried there, and exploit the network to propagate more deeply, steal information, and deny service. It’s generally agreed that network monitoring – both by machines and by highly trained people – is the best way to detect issues and reduce their risk.

A fully optimal network security approach, therefore, requires a suite of mechanical capabilities, as well as human attention and skills. Edge-network devices, which incorporate remotely manageable gateway/firewall functions, VPN termination, and content-aware filtering and detection (e.g., spam, viruses, etc.) are the ‘hardware/firmware’ part of this solution layer. These devices may also provide data-loss prevention – sifting packet contents for PII and other regulated information and preventing its transmission.

On the human side, you need the organizational capability and skill to monitor these and other devices around the clock, identify emergent issues, recognize illicit traffic-patterns, and intervene effectively to minimize damage, while also minimizing disruption of normal business processes.

A fully optimal network security approach, therefore, requires a suite of mechanical capabilities, as well as human attention and skills.

This is generally not a job that individual enterprises are equipped to manage in-house. In fact, it makes better sense to partner with a specialized provider of network monitoring and administration services for 24/7 situational awareness. This human value-add pushes us into the fourth framework level – that of architecture and strategy – since it makes best sense for this outside partner both to govern the administration of your ongoing global security strategy, and to help you assess and implement the architecture for realizing that strategy.

Topflight security service providers are equipped with the automatic tools to leverage human intelligence; empowered by constant research into and experience managing the changing threat-climate; and scaled to ensure that smart, mission-driven experts are available to stop the denial-of-service attack or inform you that 100 of your employees are being phished. Their contribution supplies the expertise, attention, and agility needed to make multi-layered security coherent and reliable, giving you room to make your IT operations and infrastructure more efficient and keep it answering to the productivity demands of your business.