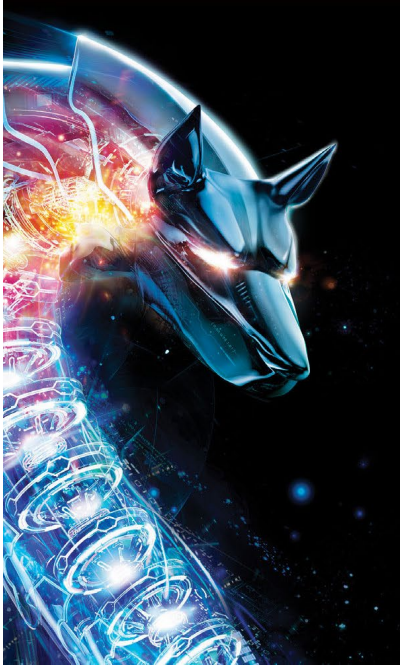
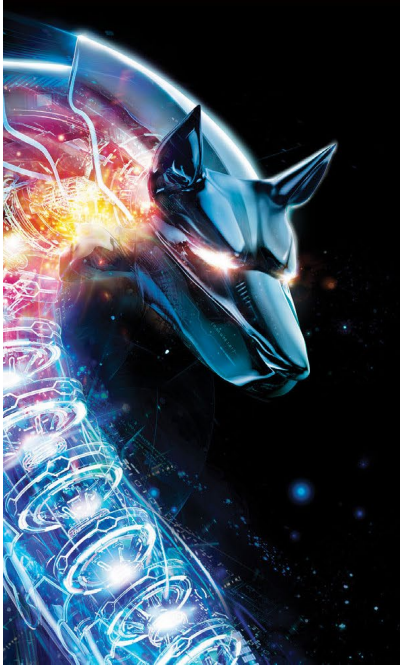


10 Critical Elements of Next-Generation, Layered Security

Cyber threats exploit vulnerabilities at all levels of the network, from the endpoint to the network stack to runtime environments. Protecting one layer while ignoring others is like locking your car, but leaving the windows open with the ignition key on the driver's seat. Effective IT security requires a layered approach that addresses known, previously unseen and advanced threats. MSPs are in the right position to help their clients craft a strategy with adequate protection measures and tools in place. Here are 10 critical elements that MSPs should include in layered security for clients.

1. **Mind the Endpoint:** Endpoint security has come a long way from anti-virus and anti-spam. While a robust solution still delivers AV and spam protection, endpoint security has become far more sophisticated. Today, a comprehensive solution combines signature-based and advanced features such as real-time monitoring and machine learning techniques to detect and block all types of malware, from previously known viruses to new ransomware variants to sophisticated zero-day threats.
2. **Surf with Caution:** When users visit websites these days, there's a risk they unwittingly will access infected or inappropriate content. MSPs' clients need web content filtering to prevent this from happening. Dynamic web content control allows you to block users and applications from accessing websites based on the content.
3. **Avoid Prying Eyes:** Full disk encryption is a necessary measure these days, especially when users carry laptops around. To add value for clients, MSPs should consider a solution with a central console supporting key management and compliance reporting for native encryption --BitLocker for Windows and FileVault for Mac. Encryption can prevent a serious breach if a machine falls into the wrong hands.
4. **Keep Them in Your Sights:** With roughly 400,000 malware samples emerging daily, no MSP can afford to take its eye off the ball when securing client systems. Real-time monitoring is a must. It ensures a process is in place to identify suspicious signs or abnormal behavior – and to take remedial action such as terminating processes and undoing changes made by malware.



10 Critical Elements
of Next-Generation, Layered Security

5. **Train Your Machine:** Machine learning is all the rage, but watch the hype. To be effective, machine learning must crunch gobs of data to compare good vs. bad samples and determine when malware is present. Machine learning algorithms are trained to spot and flag patterns, characteristics, and what can be considered suspicious behavior in order to identify zero-day and previously unknown threats. Reliable machine learning is adaptive; it keeps learning along the way to improve accuracy.
6. **Don't be Exploited:** Experienced hackers know to look for vulnerabilities they can exploit in applications, browsers, document readers, media files and runtime processes. A lot of breaches occur as a result of these vulnerabilities. To prevent this, use an advanced security solution that can monitor memory access routines to detect and block exploit techniques such as API caller verification, stack pivot and return-oriented-programming (ROP).
7. **Waste No Time:** The longer a malware sample remains in a client's network, the more damage it has the potential to cause. Your security solution, therefore, needs to have automatic remediation functionality so that as soon as something is flagged as malicious, a malware-removal process kicks in to neutralize threats and undo any changes made by the malware.
8. **Keep a List:** It's easy for clients to end up with infected applications in their networks as a result of a drive-by download or unintentional user action. To keep these applications out, select a security solution with a "blacklisting" application control feature. Blacklisting blocks programs that pose security risks or are deemed otherwise inappropriate for office use.
9. **Keep It Central:** It's hard to secure computing assets by managing them from different dashboards and locations. That just opens the door to breaches. MSPs are more effective when leveraging an integrated, centralized management console with visibility into the whole environment including data center, web, email, whether endpoints are running Windows, Mac or Linux. If you can't manage it all from one place, chances are you'll miss something.
10. **Demand Unity:** Centralized management goes hand in hand with unified security management. This allows you to administer security for physical, virtual, cloud and hybrid environments from one place. The unified approach reduces overheads, improves your security stance and ensures BYOD devices follow the same protocols as all other network assets.