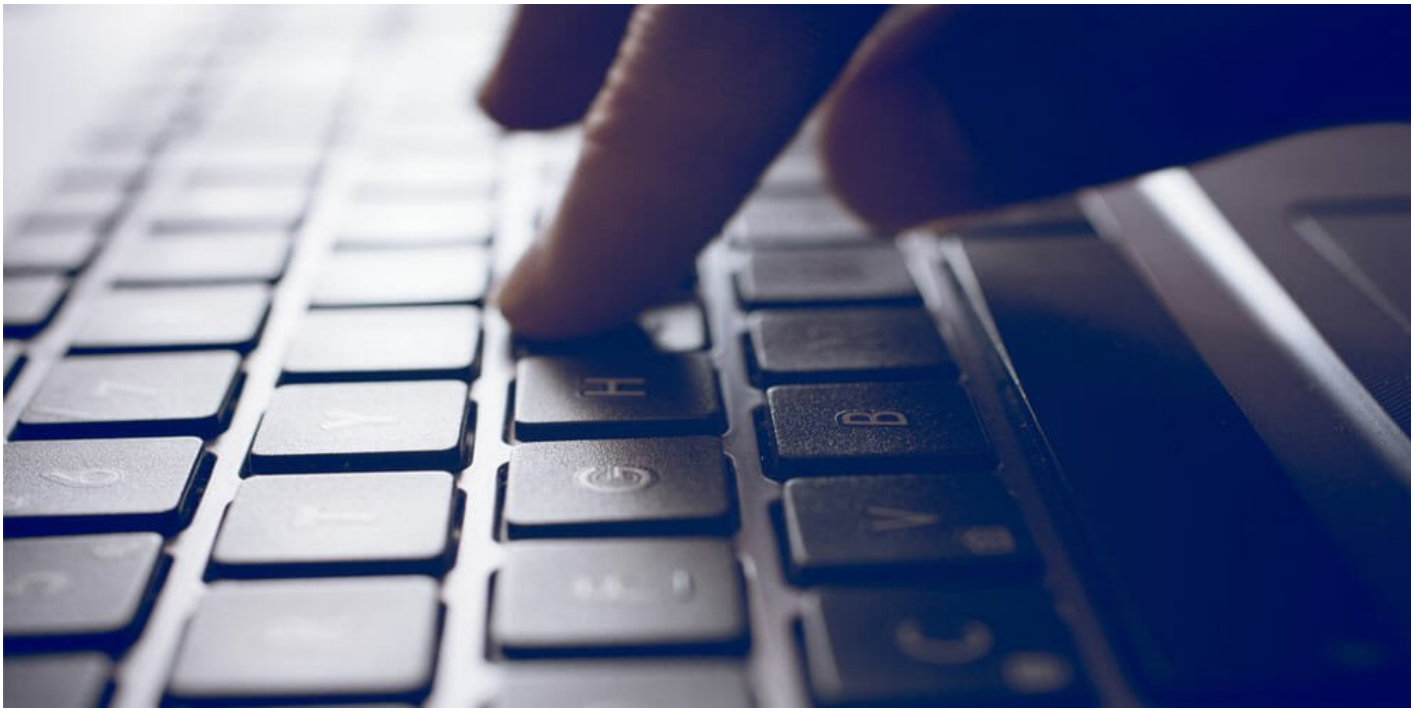
William Blair | Blog
REPRINTED FROM INVESTING INSIGHTS AT WILLIAM BLAIR



IT Security Stocks: All-Weather Tires

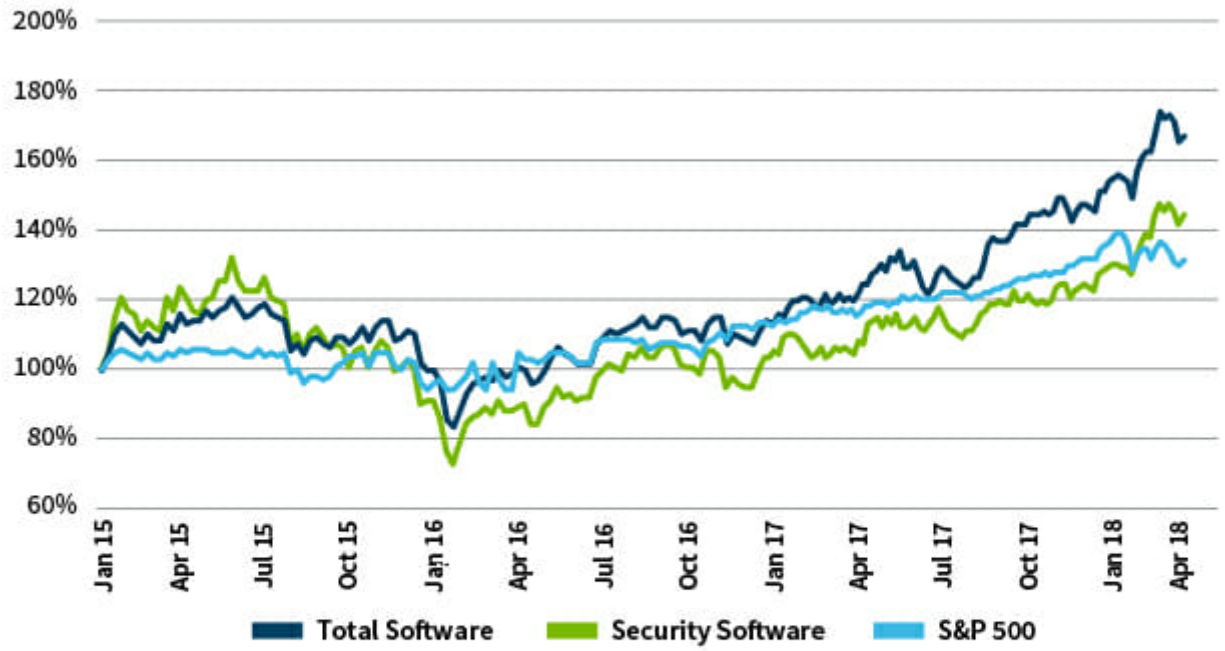
September 20, 2018

In a previous post, I discussed the evolving IT security landscape. In part two of this series, I'll discuss investment opportunities and how we evaluate IT security stocks.

In my view, IT security stocks are like all-weather tires—you can always build a case for owning them. That's because the need for security rarely decreases; rather, it shifts to address emerging risks.

In aggregate, legacy IT security companies have underperformed the broader software sector for the last three years through April 2018, as highlighted by a recent Morgan Stanley study.

Price Performance Since 2015: Security Software vs. Total Software[1]



Sources: Morgan Stanley Research, Company Data, Thomson Reuters, William Blair, as of April 2018.

1 "Cloud Security: Sizing the Silver Lining," Morgan Stanley, as of April 2018. Analysis excludes companies that have been acquired or that completed an initial public offering after January 2015.

Past performance does not guarantee future results. Indices are unmanaged, do not incur fees or expenses, and cannot be invested in directly.

One reason for the underperformance is investor concern over corporate workloads moving to the cloud. Questions that have emerged as this transition occurs include:

- Will companies still need traditional security approaches?
- Will this compress pricing for traditional security vendors? and
- In an innovation-driven space, are barriers to entry too low or are businesses subject to short cycle disruption?

In addition, there are concerns that traditional approaches will not adequately address tomorrow's threats, such as those from insiders or those hidden in clean code that will not be immediately flagged as malicious.

These concerns have created overhangs for some legacy vendors that are not as well positioned to address future threats. These vendors generally have larger market capitalizations and are more heavily weighted in the performance analysis cited above.

However, while this is a risk for some legacy vendors, the change will drive growth in technologies that can better handle perimeter-less networks and/or more effectively address new threat vectors.

Some of these areas include:

Technology	Functionality

Advanced data analysis (rebirth of SIEM)	Security information and event management (SIEM) software and services combine se information management (SIM) and security event management (SEM) to provide real analysis of security alerts generated by network hardware and applications. While this technology has been in use for well over a decade, the ability to monitor more compre data sets brought in from a greater number of sensors with advance detection techniq makes today's SIEMs more effective.
Artificial intelligence/machine learning	Leveraging large data sets and machine learning algorithms to improve detection whi lowering false positives. Like behavioral analysis, it can be additive to most forms of se
Automated incidence response	As soon as a security breach is detected and an alarm is raised, a company's system automatically responds—by quarantining infected machines, for example—without th assistance of scarce network security technicians.
Behavioral analysis	Monitoring network traffic and noting departures from normal operations to detect m activity. Behavioral analysis can be additive to most forms of security.
Cloud access security brokers (CASB)	Cloud access security brokers—software solutions that sit between a company's on-si infrastructure and a cloud provider's —allow organizations to extend the reach of thei policies to outside vendors, ensuring security consistency as employees access cloud CASB can also add visibility into shadow IT instances.
Identity and access management (IAM)	Identity and access management systems help manage digital identities, helping ensu the right individuals are accessing the right resources at the right times for the right re addition, they help reduce the time and effort to provision new users and to turn off u user accounts.
Internet of things protection	Today many products and devices monitor usage characteristics to improve the custo experience. These connected devices (sensors on home appliances such as heating an systems, industrial equipment including locomotives, airplane engines, power tools, a sports equipment, such as tennis rackets) pass information through the web to both c and decentralized locations. While most of this activity is innocuous and has little valu data such as confidential medical information needs to be secured in a cost-efficient m
Mobile security	Solutions that separate and secure corporate information on mobile devices without s employee's personal information. It also allows for quick deletion of corporate files in device or employee departure situation.
New antivirus (AV) approaches	At over $6 billion, the AV market is substantial. Traditional signature-based antivirus s are helpful for blocking previously discovered malware, but they struggle with undisco strands and/or malicious code that can morph. Today, companies are replacing old so with next-generation antivirus platforms that can stop modern attacks by incorporati behavioral analysis, greater application activity monitoring, analysis across larger data other methodologies to help catch malicious code and payloads before they are activa
User and entity behavior analytics (UEBA)	Insider threats are a significant concern that historically were not a focus of CISOs. New technologies can help lock down sensitive files as well as alert security teams when ins acting in a malicious fashion.

IT vendors that offer solutions incorporating these technologies are likely to benefit from strong secular end-

market tailwinds.

When evaluating IT security investment opportunities, we look for the same criteria as with all technology investments, including:

- a large addressable market
- a great value proposition to the customer
- strong competitive barriers
- a valuation that presents an attractive balance between risk and reward

However, with security companies, we also place heavy importance on several additional factors:

- A non-technology-oriented "edge" is highly valuable. IT security investments carry a high degree of leapfrog risk, since what works well today is often quickly rendered obsolete by tomorrow's technology. To extend revenue growth duration, the product needs an edge beyond just "better technology," be it some sort of network effect (such as collecting attack data at scale and using that to better protect all customers), a better distribution network or pricing model, a competitor exiting the market, or a functional tie-in with a separate non-security IT vendor, which increases the value proposition of both products.
- Second, the company's product or service should be "future proof," meaning it can work in current and future technology architectures, and will not require a complete rewrite as technology advances. Few technology products are truly future proof, since the pace of change requires consistent investment to remain relevant. But products that are addressing core threats and management teams that have demonstrated an ability to remain relevant despite shifting technology paradigms will typically garner much higher implied terminal valuations than those that cannot.
- Third, we look for companies that offer not just one product but product suites. Platform vendors capture value from multiple products, have lower sales-and-marketing expense, and are generally much stickier, leading to stronger competitive barriers and higher and/or longer duration of earnings growth.
- Last, we seek long-term (versus short-term) profit potential. Companies that are investing in their research, technology, and salesforce often have less-than-optimal margins in the near term, but are positioning themselves to create substantial long-term value. If we have confidence in the longevity of growth and margin expansion potential, we are usually willing to trade off the potential for small profits today for an opportunity for substantially larger profits tomorrow.

In conclusion, IT security offers both challenges and opportunities. We believe our framework will help us to successfully navigate both, which we believe may yield outperformance for our clients.

Corey Tobin, partner, is a research analyst and co-director of research on William Blair's U.S. Growth Equity team.

Disclosure:

This content is for informational and educational purposes only and not intended as investment advice or a recommendation to buy or sell any security. Investment advice and recommendations can be provided only after careful consideration of an investor's objectives, guidelines, and restrictions.

Information and opinions expressed are those of the authors and may not reflect the opinions of other investment teams within William Blair Investment Management, LLC, or affiliates. Factual information has been taken from sources we believe to be reliable, but its accuracy, completeness or interpretation cannot be guaranteed. Information is current as of the date appearing in this material only and subject to change without notice. Statements concerning financial market trends are based on current market conditions, which will fluctuate. This material may include estimates, outlooks, projections, and other forward-looking statements. Due to a variety of factors, actual events may differ significantly from those presented.

Investing involves risks, including the possible loss of principal. Equity securities may decline in value due to both real and perceived general market, economic, and industry conditions. The securities of smaller companies may be more volatile and less liquid than securities of larger companies. Investing in foreign denominated and/or domiciled securities may involve heightened risk due to currency fluctuations, and economic and political risks. These risks may be enhanced in emerging markets. Different investment styles may shift in and out of favor depending on market conditions. Individual securities may not perform as expected or a strategy used by the Adviser may fail to produce its intended result.

Investing in the bond market is subject to certain risks including market, interest rate, issuer, credit, and inflation risk. Rising interest rates generally cause bond prices to fall. High-yield, lower-rated, securities involve greater risk than higher-rated securities. Sovereign debt securities are subject to the risk that an entity may delay or refuse to pay interest or principal on its sovereign debt because of cash flow problems, insufficient foreign reserves, or political or other considerations. Derivatives may involve certain risks such as counterparty, liquidity, interest rate, market, credit, management, and the risk that a position could not be closed when most advantageous. Currency transactions are affected by fluctuations in exchange rates; currency exchange rates may fluctuate significantly over short periods of time. Diversification does not ensure against loss.

There can be no assurance that investment objectives will be met. Any investment or strategy mentioned herein may not be appropriate for every investor. References to specific companies are for illustrative purposes only and should not be construed as investment advice or a recommendation to buy or sell any security. Past performance is not indicative of future returns.