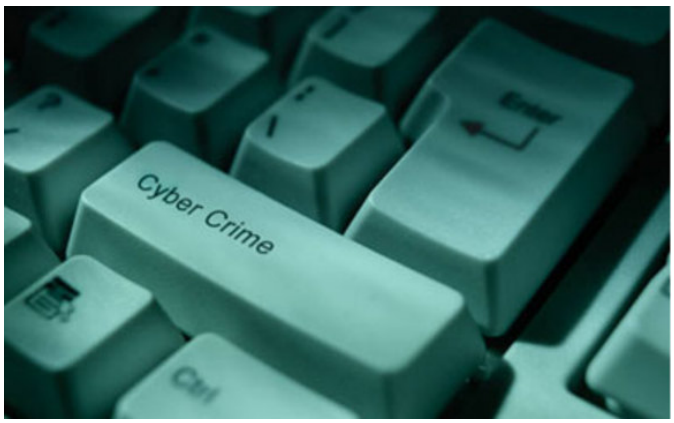
Gartner urges enterprises to shift security away from mere blocking and detection to active detection and response to attacks-- all in order to avoid what it calls "aggressive business disruption attacks."



Such attacks are defined as "targeted attacks that reach deeply into internal digital business operations with the express purpose of widespread business damage. Servers may be taken down completely, data may be wiped and digital intellectual property may be released on the Internet by attackers… These attacks may expose embarrassing internal data via social media channels-- and could have a longer media cycle than a breach of credit card or personal data."

"Preventive controls, such as firewalls, antivirus and vulnerability management, should not be the only focus of a mature security program," Gartner continues. "Balancing investment in detection and response capabilities acknowledges this new reality."

Thus the analyst predicts 40% of large enterprises will have formal plans to actively address aggressive disruption attacks by 2018, up from none at all in 2015-- marking out an opportunity in security as more enterprises become aware of an escalating situation.

Go Gartner Says By 2018, 40% of Large Enterprises Will Have Formal Plans to Address Aggressive Cybersecurity Business Disruption Attacks