cavirin

SOLUTION BRIEF

Automated Security for Midmarket Enterprises

Helping mid-size organizations to quickly adopt security and assessment best practices, by offering the automation critical to balance limited manpower.

82%

OF MIDMARKET ENTERPRISES BELIEVE DATA SECURITY IS ONE OF THEIR BIGGEST CONCERNS

The 200,000 or so midmarket businesses in the United States, with revenues between $10M and $1B account for about a third of all Gross Domestic Product (GDP), but are sometimes overlooked in the context of the larger security discussion. These organizations deal with data just as confidential as the Fortune 500, including healthcare, educational, financial, and legal records to name a few, and face unique security challenges, including:

1. *Understaffed (or minimal staff)*
2. *Lack of budget and therefore lack of access to sophisticated security tools*
3. *Less training and understanding of regulatory compliance and cloud workloads*
4. *Held to high standards as part of a supply chain (or by their customers)*
5. *More likely that a major breach will put them out of business.*
6. *Lower chance of cyber-insurance coverage*

Because of these challenges, mid-size businesses are more likely to be targeted for attacks.

Their deployments span on-premise, the cloud, and now containers, but they can't act as system integrators, deploying individual solutions for each of these three domains. They need a single platform that will provide them with a consistent view, one that requires minimal training and is easy to consume. Cavirin's platform addresses these challenges, directly influencing 1-5 (on the previous page) and, if the company is evaluating 6, it can reduce insurance rates as well. These capabilities also align to perceived barriers according to a survey conducted by Thales (chart below).

2017 Thales Data Threat Report

A recent survey conducted by PwC found that, from 2014 to 2015, cyber-attacks rose 64% for midmarket companies. If the past is any example, these companies will experience more sophisticated attacks as larger enterprise deploy defense in-depth.

In another survey, conducted by NetDiligence/McGladrey, companies with revenues between $50 million and $1 billion accounted for nearly half of all cyber-claims. The median claim per company was nearly $77,000 in 2015.

THE MIDMARKET INFRASTRUCTURE

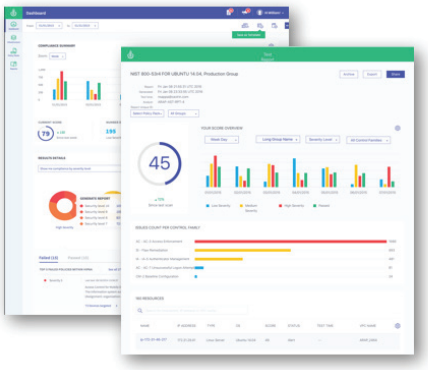
In many cases the midmarket environment includes a combination of on-premise (VMware/KVM) applications with public cloud (AWS, Microsoft Azure, and/or GCP) and in some cases containers (Docker). In fact, hybrid cloud adoption is said to be up to 71 percent year-over-year for mid-size organizations. In addition, Google Docs, Office365, Dropbox, and other SaaS applications are being widely adopted, although employees have less background in managing cloud-delivered services.

Compliance management for midmarket companies is top of mind. Protecting Personally Identifiable Information (PII), Payment Card Information (PCI), and Protected Health Information (PHI) data across (physical, public, and hybrid clouds) is what keeps many executives awake at night.

Within the midmarket environment, most security professionals feel they lack the tools and resources they need to monitor, analyze, understand, and mitigate internal/external threats, while regulatory compliance has become more taxing but essential - How can organizations close the security gap?

89% **OF BREACHED ORGANIZATIONS**
HAD A FIREWALL IN PLACE AT
THE TIME OF COMPROMISE

THE CAVIRIN SOLUTION



Cavirin offers a way out by securing workloads both on-premise and in the cloud. Cavirin's continuous security assessment and remediation platform permits mid-size organizations to quickly adopt best practices, by offering the automation critical to balance limited manpower. And, if in a regulated industry, it ensures the risk compliance of their servers. Although not replacing conventional perimeter defenses like firewalls, Cavirin offers an added level of security, looking from the inside out, by acting as a counter balance to the less robust perimeter security offered by some Unified Threat Management (UTM) systems. At a low cost of entry and the deployment of no new hardware, the business, be it $10M or $1B, now has access to true enterprise-grade hybrid cloud security.

Cavirin also offers deployment flexibility. If the business operates an on-premise data center, the solution is easily deployed. In the same way, deployment within AWS, GCP, and Microsoft Azure are options. Soon, the organization may also consume the offering as Cavirin-delivered SaaS or they may subscribe to their MSSP of choice. This last option is important for companies that may not have the in-house capabilities to deploy or manage the service. Forrester has cited that almost a third of midmarket enterprises go this path to take advantage of more specialized skills. In all cases, the customer has a consistent view across all deployment models.

"Technology is becoming more of a differentiator in the middle market. At a strategic level, technology is helping smaller, growing companies scale faster and increase their valuations."

HARVEY MICHAELS, DELOITTE CONSULTING LLP