Next Generation Intrusion Prevention System (NGIPS)

Enterprise Intelligence Brief

Q3 2019

ANDREW LOWE, JASON PAPPALEXIS

Overview

Intrusion prevention systems (IPS) are designed to identify and block network attacks against internal computing assets, as well as protect enterprise users against threats and exploits. An IPS must catch sophisticated attacks while producing minimal false positives and without introducing network latency.

211 of 383 survey respondents reported deploying IPS technology.

Enterprises that wish to make changes to their security architectures will often rely on insight from their peers. This brief presents results from NSS Labs' 2019 Security Architecture Study, which included survey responses from 389 information security professionals representing 26 US industries.[1]

Enterprises can use this information to gain critical insights into IPS technology, including information on how these security controls are being managed within organizations, where they are being deployed, who is responsible for purchasing decisions, and the extent to which API controls are being used for their management.

Findings

- About half (211 out of 383) of the survey respondents reported deploying IPS technology.
- 70% of respondents from very large enterprises (VLEs) and 64% of large enterprises (LEs) reported deploying IPS on premises; this is a shift from 2017 numbers (VLEs: 86%; LEs: 77%.)
- Most of the respondents reporting IPS deployment (64%) were from the insurance industry, followed by financial services (~58%), and health insurance (58%).
- For organizations that deploy an IPS, security efficacy was the highest-rated capability on average, followed by performance and then stability & reliability.
- Respondents ranked manageability, deployment/rollout effort, and vendor technical support as the most important operational factors to consider during product selection; risk tolerance, interoperability with other security products, and vendor reputation were also selected as important.

About This Report

This brief is part of an ongoing series on security products deployed within enterprise IT security architectures and includes current usage statistics for IPS within small and medium-sized enterprises (SMEs), large enterprises (LEs), and very large enterprises (VLEs).

[1] More information about this study can be found in the Appendix.

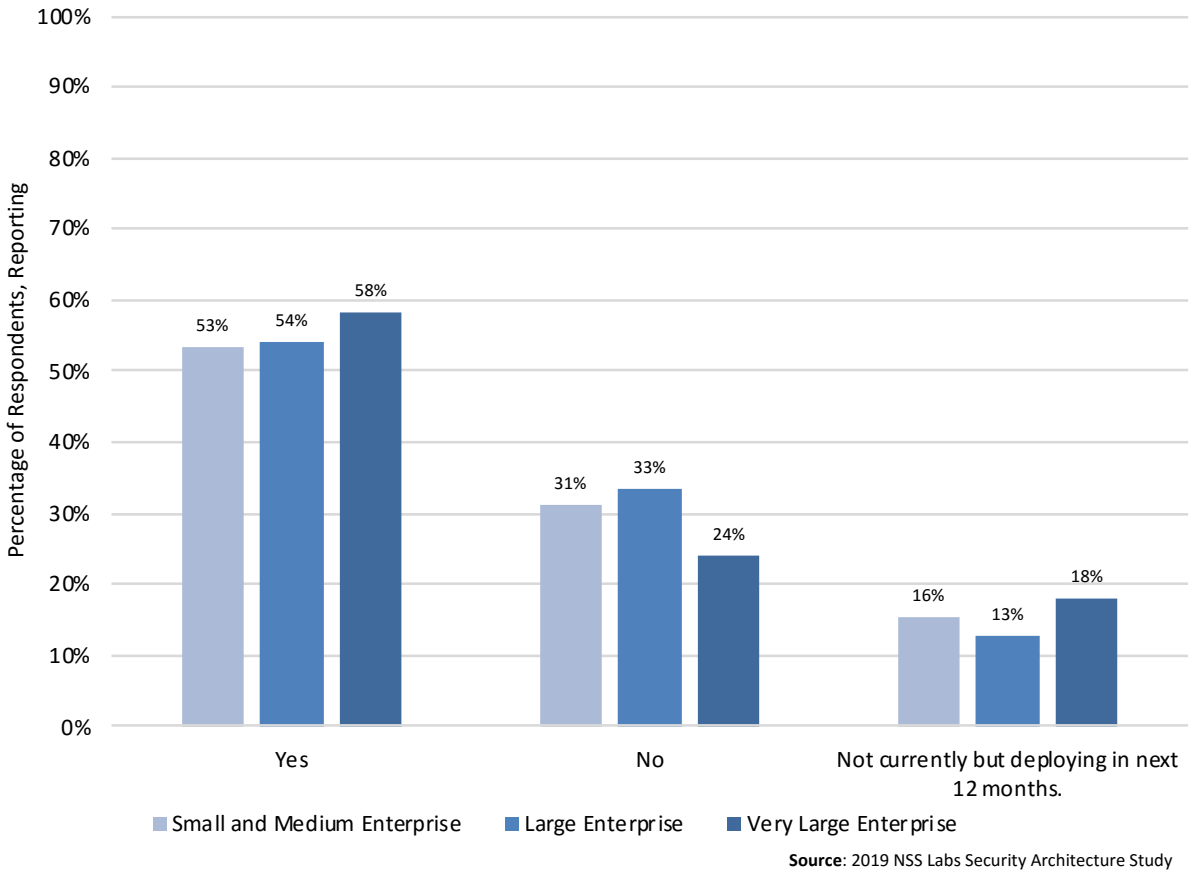
Definition, Method, Deployment, and Alternatives

Category	Description
Definition	Intrusion prevention systems (IPS) are physical or virtual appliances that decode and inspect network packets for exploit signatures. These appliances allow legitimate traffic to pass while also blocking attacks and resisting evasion techniques. Most IPS today also offer application awareness, user identification, and anti-malware functionality. Devices with these capabilities are known as next generation intrusion prevention systems, or NGIPS.
Method	NGIPS operate from OSI Layer 2 (data link layer) through OSI Layer 7 (application layer) to detect and block exploits, ensure protocol compliance with RFC standards, and filter traffic based on an enterprise's security policies. NGIPS also provide deep packet inspection (DPI) to block application-based attacks. Both IPS and NGIPS rely primarily on signatures to detect malicious activities. Features such as application control, user awareness, and anti-malware may require additional licenses.
Deployment	NGIPS often provide the final layer of inspection before data is passed to internal hosts, and they are deployed within network segments as inline or out-of-band. Depending on their needs, some enterprises may require inline mode (where packets are held while they are being inspected), while others may require out-of-band mode (where copies of packets are inspected). If out-of-band mode is selected, policy enforcement must come from a router or firewall. NGIPS are commonly deployed at the DMZ, in the data center, in the cloud, and in branch offices. IPS traditionally inspect north-south traffic and are placed behind firewalls or other perimeter security devices. IPS are increasingly being used as part of internal network segmentation efforts, providing fine-grained controls on east-west traffic. IPS are typically deployed by IT security practitioners with training specific to the technology.
Alternatives	Next generation firewalls (NGFWs) or universal threat management (UTM) products with IPS functionality; routers with IPS functionality, SD-WANs, or cloud-delivered gateways (includes proxies such as secure web gateways).

Figure 1 – Product Definition, Method, Deployment, and Alternatives

Product Use Within the Enterprise

IPS are typically deployed by large or very large enterprises rather than by small and medium-sized enterprises. Figure 2 illustrates IPS deployment by horizontal.



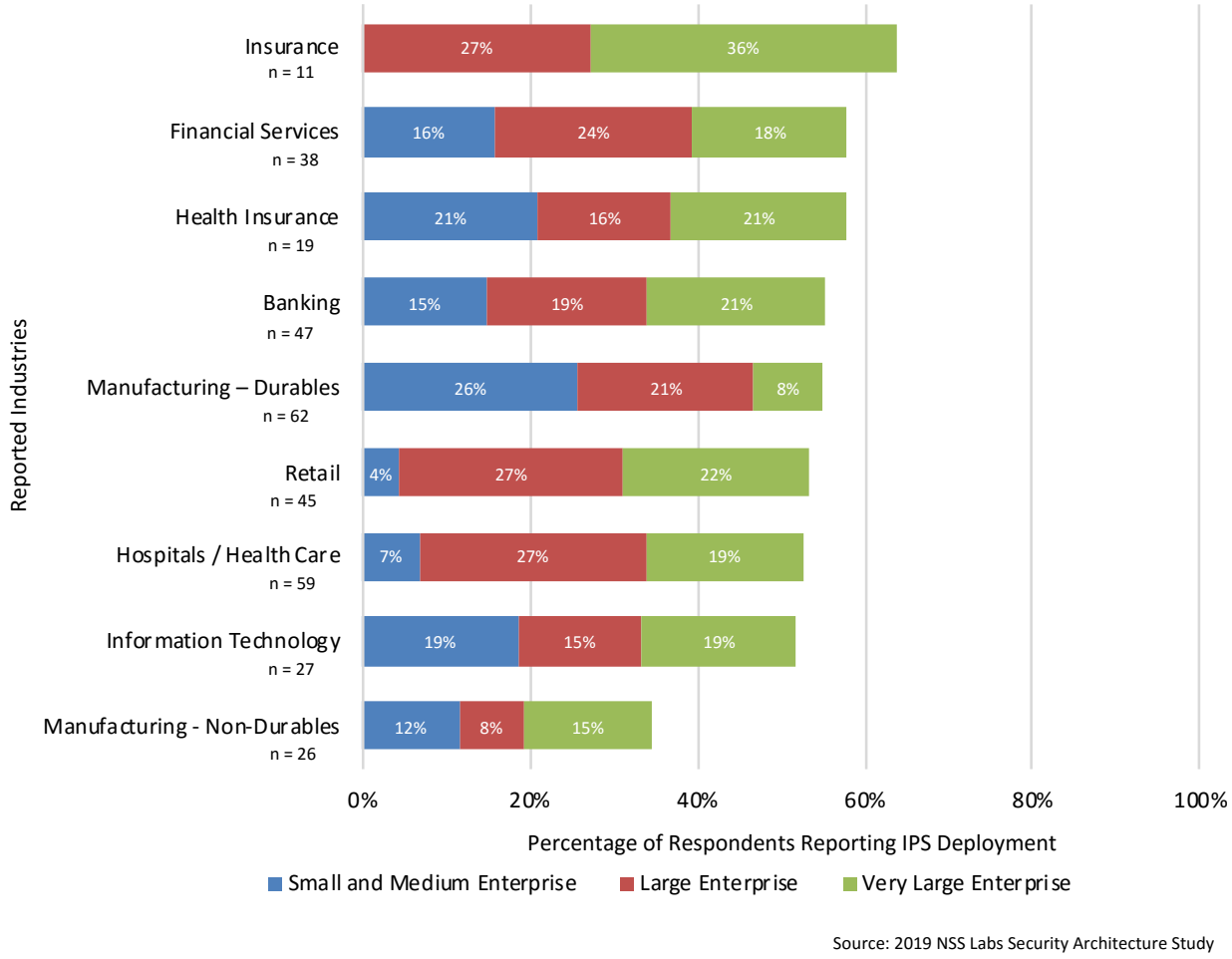
Source: 2019 NSS Labs Security Architecture Study

Figure 2 – IPS Deployment by Horizontal

Deployment Location and Segmentation

IPS provide protection against network-based threats and are most often deployed at the network perimeter to scan north-south traffic. However, since NGIPS products include application layer visibility, user-level visibility, and traffic enforcement capabilities, a growing use case for these products is for the segmentation of internal networks. The fine-grained policies in an NGIPS improve visibility into and control over internal network traffic (east-west) compared to traditional VLAN policies and ACLs, which are coarse-grained.

Figure 3 presents IPS deployment by vertical as reported in our 2019 Security Architecture Study. Note that only those verticals with a minimum of 10 total respondents are included.



Source: 2019 NSS Labs Security Architecture Study

Figure 3 – IPS Deployment by Vertical

Enterprise Teams responsible for IPS Management

In the 2017 NSS Labs Security Architecture Study, survey participants were asked which teams at their organizations were responsible for managing and maintaining IPS deployments. Across all horizontals, the security operations (SecOps) team option was the most commonly selected, followed by network operations (NetOps) teams and IT teams. Less commonly reported were infrastructure, architecture, and development operations (DevOps) teams.

Deployment Location and Form Factor

Enterprises most commonly install IPS as a virtual appliance (31%), followed by physical appliance (30%), IaaS-based IPS (27%) and IPS-as-a-Service (18%). Figure 4 displays deployment by horizontal.

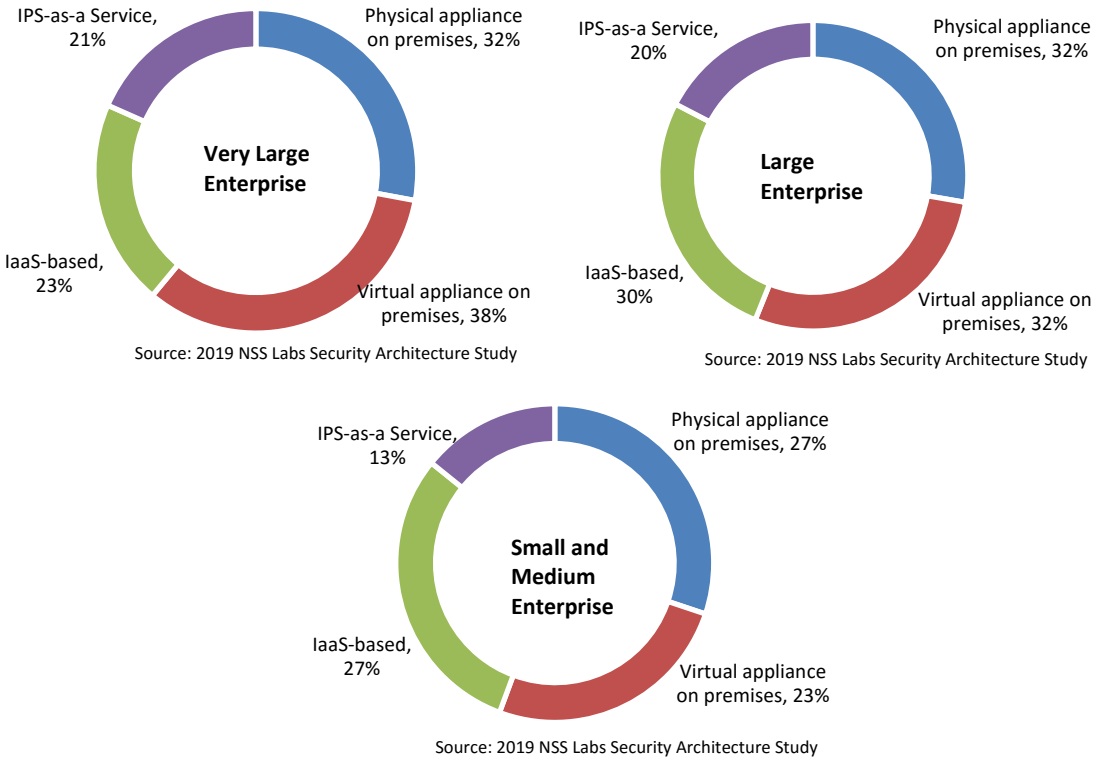


Figure 4 – What intrusion prevention system (IPS) form factors are currently deployed at your organization?

Rating IPS Functionality

Survey respondents were presented with nine metrics and asked to rate the functionality of the IPS most in use at their organizations. Figure 5 presents the average ratings in ranked order, from highest to lowest. On average, respondents ranked security efficacy the highest and third-party integration the lowest.

Capability	Ranked Ratings
Security efficacy	1
Performance	2
Stability & reliability	3
Vendor support	4
Management console – alert details	5
Deployment preparation and rollout effort	6
Management console – usability	7
Logging	8
Third-party integration	9

Figure 5 – How do you rate (your) IPS?

Product Selection

When enterprises consider security products, multiple factors must be considered, including operational and security product selection factors. Figure **6** and Figure 7 present ranked average ratings by survey respondents.

Operational Factors	Ranked Average Ratings
Manageability	1
Deployment/rollout effort	2
Vendor technical support	3
Product update frequency, stability and documentation	4
Capital/operational costs	5

Figure 6 – How does your organization rank the following operational factors for security product selection?

Other Factors	Ranked Average Ratings
Risk tolerance	1
Interoperability with other security products	2
Vendor's reputation	3
Third-party certified capabilities	4
Vendor market share	5

Figure 7 – When selecting security products, which other factors are most important to your organization in product selection?

Appendix

Most data in this report was sourced from the 2019 NSS Labs Security Architecture Study. The 2017 NSS Labs Architecture Study methodology is available upon request.

NSS Labs 2019 Security Architecture Study

In early 2019, NSS Labs conducted the 2019 Security Architecture Study to establish current US enterprise security architectures. The study had five primary objectives: 1) Map security product deployment, environment, management, and purchasing for the small and medium-sized enterprise (SME), large enterprise (LE), and very large enterprise (VLE); 2) Quantify trends in architecture deployments; 3) Determine which teams actively manage deployed security technologies in the enterprise; 4) Define purchase authorities; and 5) Gather enterprise perceptions of deployed security products with regard to performance, security efficacy, management, deployment, interoperability ,and vendor support

The study was conducted with the participation of 389 full-time US enterprise IT security professionals representing 26 US industries with a median IT security budget of US$10M – $49M.

Survey

A 136-item mixed-format battery was drafted by the NSS Labs Enterprise Architecture Research Group and delivered via an online survey platform, using a third-party panel service for pre-screening, participant role verification, and to facilitate accrual. The survey was logic coded, so not all respondents received all items in the survey dependent on their answers on previous items. To minimize errors resulting from primacy and recency effects, non-ranked survey response options were presented in random order. The survey had nine screening items and participants failing these items were excluded from final analyses. Additionally, speeders were excluded from final analyses using one-third median time-to-complete as the minimum epoch for inclusion.

Participants/Accrual

Potential participants were pre-screened for eligibility. There were multiple qualifiers for eligibility in this study, including both organizational and participant inclusion criteria. To be eligible for participation, a participant was required to be currently employed as a full-time information security professional with a minimum of three years in role as a security practitioner. Additionally, participants were required to be employed at enterprises with a minimum of 500 full-time employees (no SMB respondents). To minimize error due to non-response bias, and to drive accrual, participation was incentivized.

Accrual was facilitated by a B2B research panel service that verified participant role and organization prior to recruitment and screening. A nine-item screening block preceded the survey to validate human response (word-embedded image validation), full-time security role, title (technical support roles screened out), organizational size (fewer than 100 employees screened out), years in role (less than three years screened out), annual IT security budget (less than $500k/year screened out), and involvement with information security technology (“Not involved” with security technology screened out). Post-hoc quality control checks were performed with the following rubric to flag/exclude responses with 1) multiple nonsensical/noncontextual responses; 2) patterned

responses; 3) duplicate responses; 4) responses completed from non-US IP addresses; and/or 5) indicators of automated (bot) responses.

At close of accrual, 5,210 participants were screened; 458 participants completed the survey; and 389 passed quality control checks and were included in final analyses.

Margin-of-Error Statement

All surveys and polls are subject to numerous sources of error such as sampling error; coverage error; errors due to nonresponse; errors associated with question wording and response options; and post-survey weighting and adjustments. Where possible, controls for common errors were implemented in this study, including multiple screening items, quality control items, controls for speeders, and data quality checks for nonsensical or patterned responses. In keeping with the American Association for Public Opinion Research's Code of Ethics, NSS has chosen not to report a margin of sampling error for this study as random selection from this population was not feasible. Inclusion of a margin-of-error estimate could imply that our interpretations should be accorded greater confidence than the data warrants. Margin of error is an estimate of sampling error, not a measure of validity, and should always be interpreted with caution.

Survey Demographics for NSS Labs 2019 Security Architecture Study

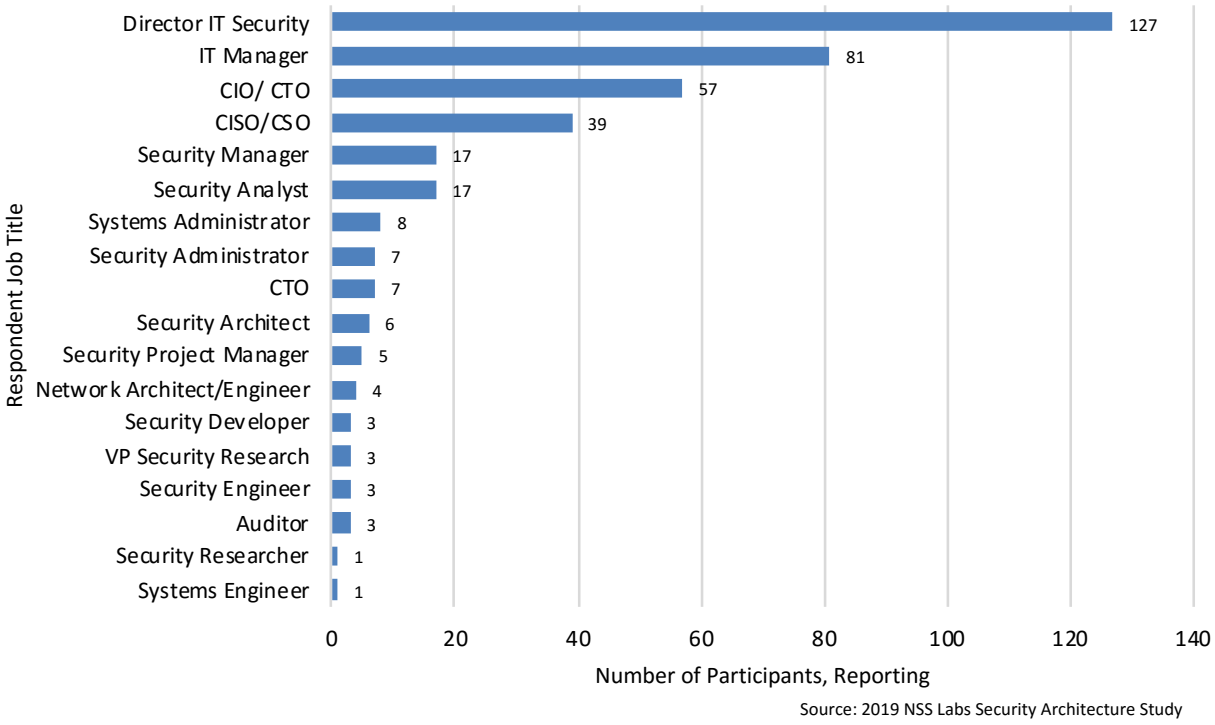


Figure 8 – Respondent Job Title

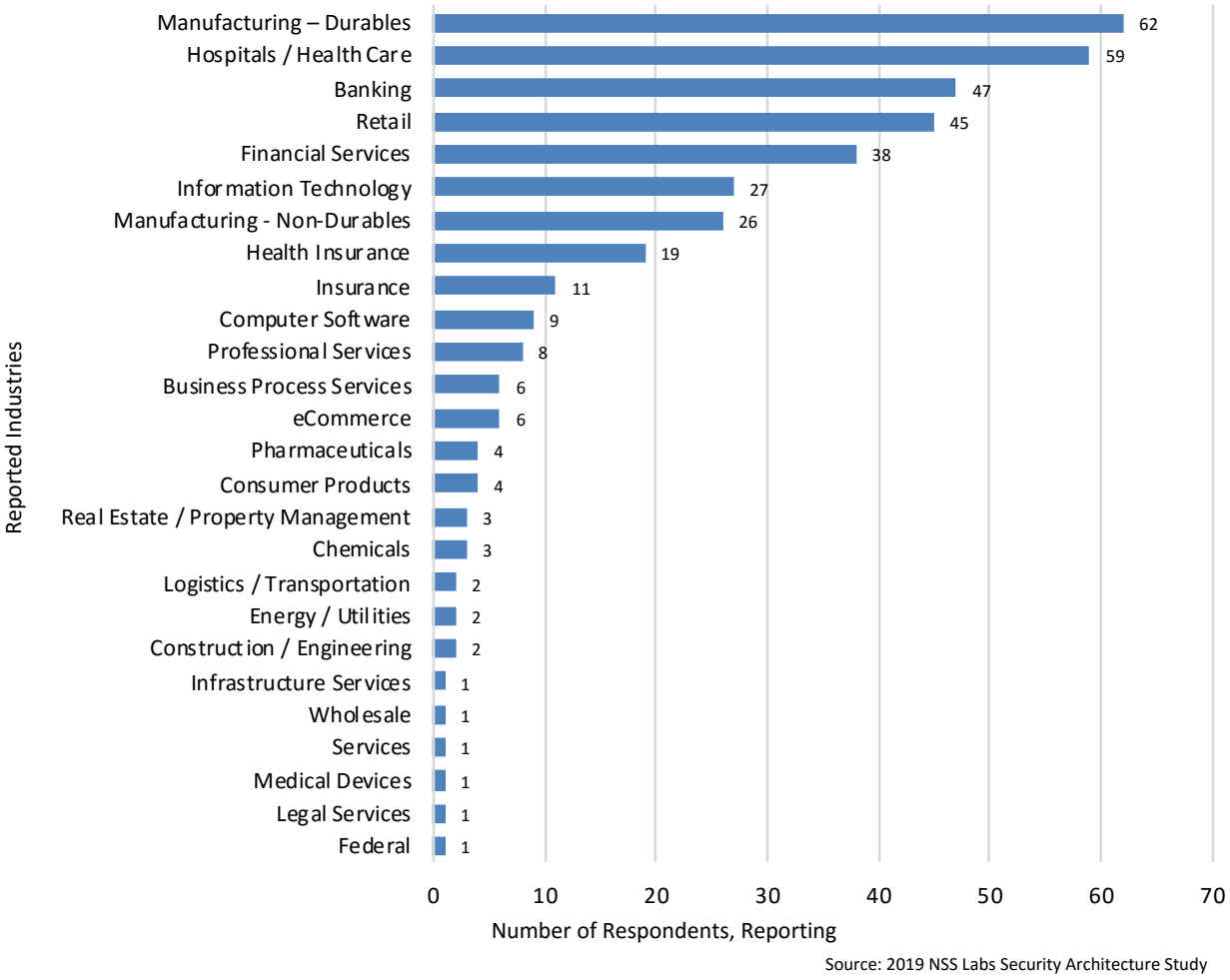


Figure 9 – Responses by Vertical

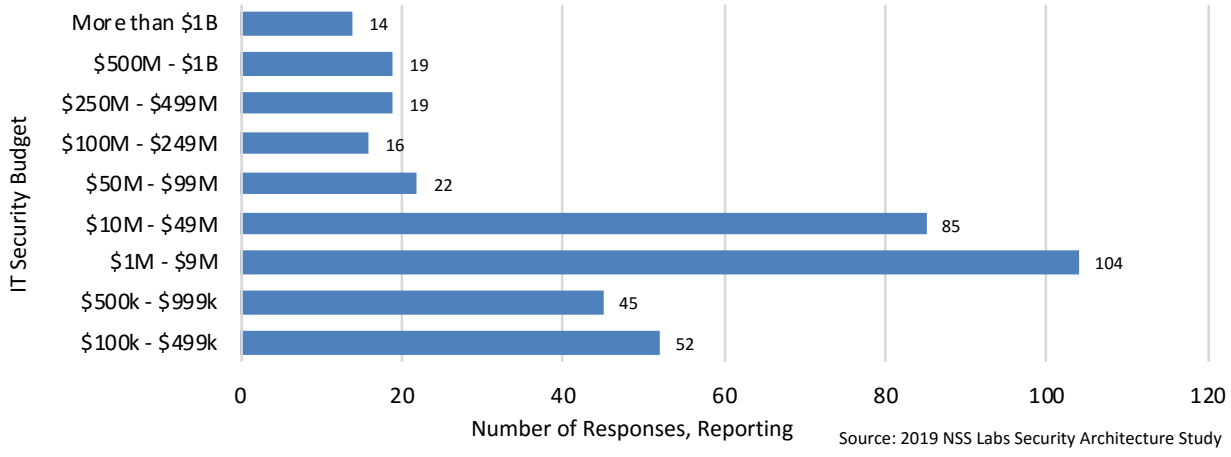


Figure 10 – Annual IT Security Budget

About the Enterprise Architecture Research Group

The mission of the NSS Labs Enterprise Architecture Research Group is to work with enterprises to solve security architecture and product challenges. We provide research and advisory services that are objective, accurate, reliable, and actionable. Our data comes from NSS test results, first-hand experience in the lab, novel primary research, and interaction with our enterprise clients.

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com