CYBERSECURITY 2017

HEALTHCARE PROVIDER SECURITY ASSESSMENT

A KLAS-CHIME Benchmarking Report

KLAS | FEBRUARY 2017 | PERFORMANCE REPORT

ABOUT KLAS & CHIME

Using the voice of healthcare software and services customers, KLAS has measured healthcare IT vendor performance since 1997. Today, KLAS collects and publishes customer feedback on over 800 products and services. Roughly 30,000 providers work with KLAS each year. Since healthcare IT is often a nuanced and complex discussion subject, over 98% of KLAS research is collected in live conversations over the phone, to ensure accuracy and clarity. All interviews are strictly anonymous, and participants are granted broad access to the feedback of other participants. Vendor access to KLAS' findings is available through subscription and individual report purchases.

The College of Healthcare Information Management Executives (CHIME) is an executive organization dedicated to serving chief information officers and other senior healthcare IT leaders. With more than 2,300 CIO members and over 150 healthcare IT vendors and professional services firms, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of information management to improve health and healthcare in the communities they serve. For more information, please visit www.chimecentral.org.

ABSTRACT

Security in healthcare has never been more critical. As payment and delivery reforms propel the industry toward greater connectivity and information exchange, new vulnerabilities arise. Cybercriminals are continually finding new and more sophisticated ways to attack networks and are searching for even the smallest crack. In an effort to benchmark the current state of security preparedness across the healthcare industry, KLAS and the College of Healthcare Information Management Executives (CHIME) embarked on a study to assess best practices and gain insights on healthcare organizations' current security programs.

ABOUT THIS CYBERSECURITY RESEARCH

This executive brief is a subset of a larger report produced through a collaborative effort between KLAS, CHIME, healthcare security professionals, and other provider executives to examine how technologies are being deployed to address such areas as data loss prevention (DLP), identity and access management (IAM), mobile device management (MDM), and security information and event management (SIEM). The executive brief is intended to provide a clear view of the healthcare security landscape for interested parties across the nation, including industry leaders and policy makers.

Working with their Security Advisory Board, KLAS designed a detailed questionnaire to measure the current state of healthcare security, including vendor capabilities. Over the course of four months in 2016, KLAS conducted nearly 200 interviews with chief information security officers (CISOs), chief information officers (CIOs), chief technology officers (CTOs), and other security professionals. To cover the largest number of impacted providers and patients, the research targeted mainly integrated delivery networks (IDNs) and hospitals, with some additional input gathered from large physician practices (75+ physicians). Below is a breakdown of the organizations and respondents that participated in this study.

Figure 1 **Key Participants by Provider Type and Job Level**

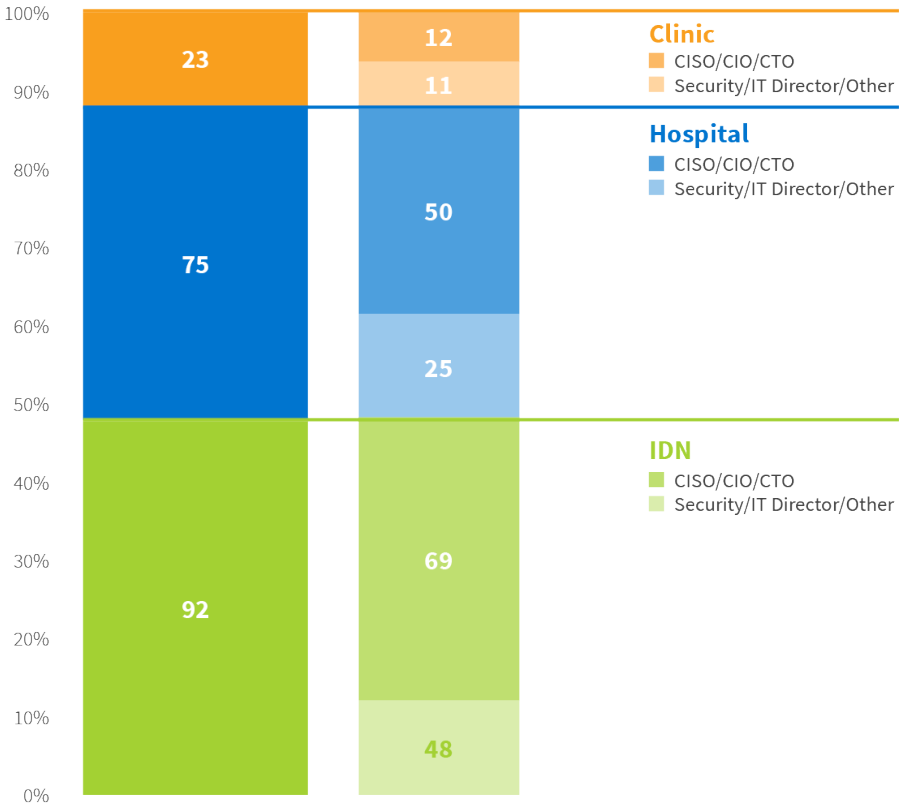
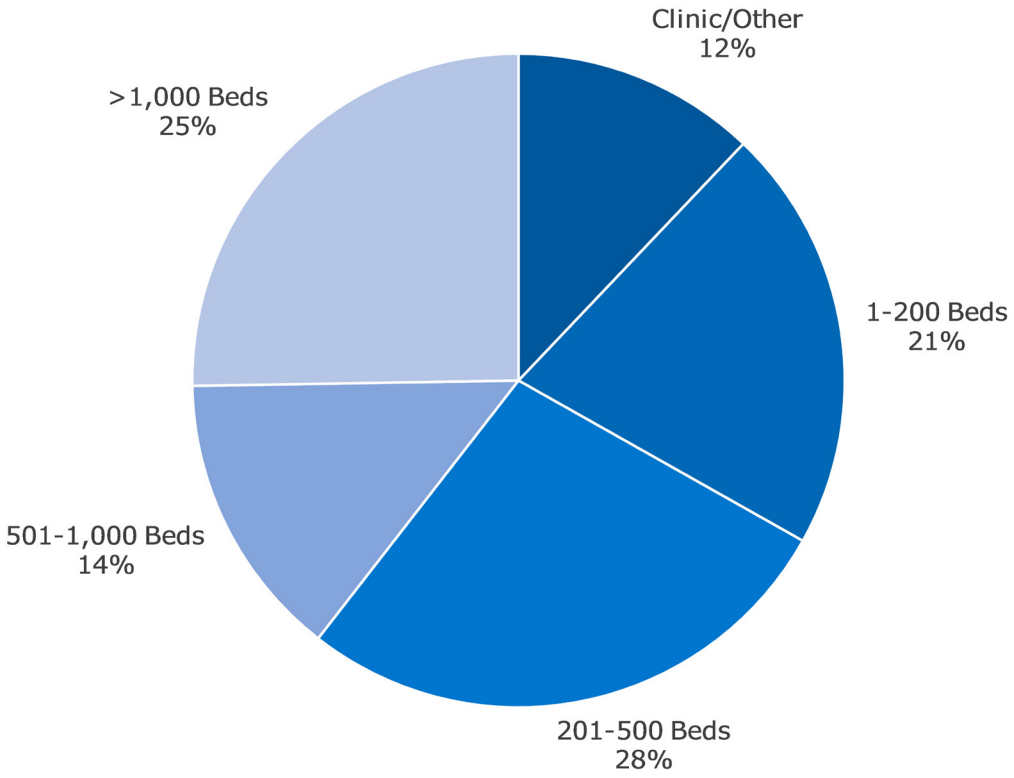


Figure 2 **Survey Participants by Organization Size**
n=190



WHERE IS CYBERSECURITY IN HEALTHCARE TODAY?

As part of the questionnaire used to gather this research, KLAS asked each organization to provide insight on the details of their cybersecurity programs. Their responses will serve as an initial benchmark for future assessments of industry practices. Among the key findings are the following:

- Nearly all organizations have someone in charge of their security program, though that role is sometimes filled by someone who is not solely dedicated to IT security.
- 40% of organizations have a VP/C-level in charge of their program. About half of these are CISOs; the other half are CIOs/CTOs.
- Compared to those in an IT role, respondents with a security background more often report having a VP or director (often a CISO or security director) in charge of their security program. They are also significantly more likely to have a cybersecurity framework in place and a deeper breach-readiness level.
- Only 16% of organizations feel they have a fully functional security program; nearly all of these are IDNs or larger hospitals.
- More than half of organizations that are still developing their security program are spending less than 3% of their total IT budget on security. As they begin to build out more robust programs, organizations are more likely to spend a higher percentage of their budget on security, likely due to increased staff, infrastructure, and software costs.
- By far, the NIST Cybersecurity Framework is the most commonly used framework.

Figure 3

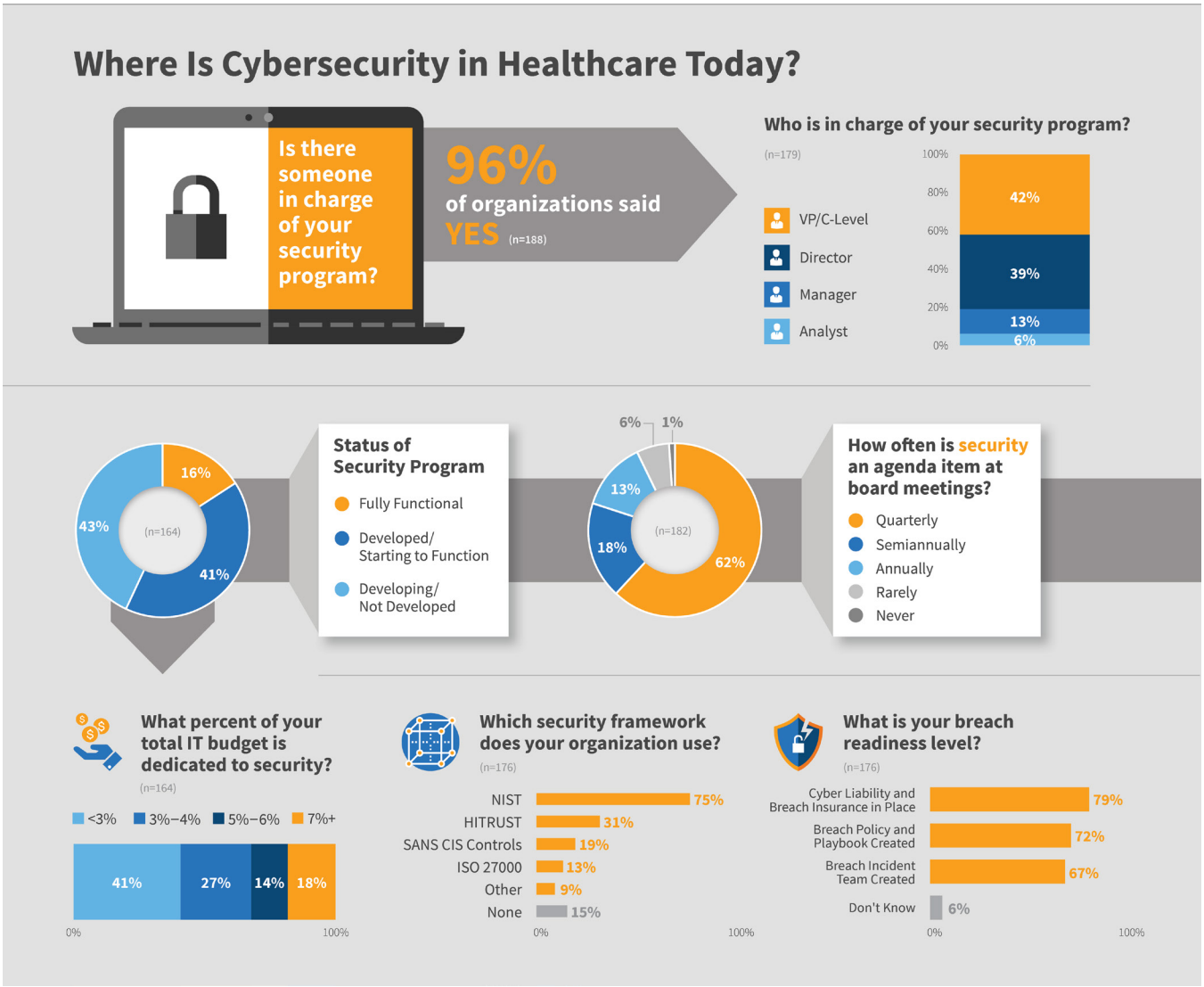

Where Is Cybersecurity in Healthcare Today?
Is there someone in charge of your security program?
96%
of organizations said
YES (n=188)
Who is in charge of your security program?
(n=179)
VP/C-Level
Director
Manager
Analyst
100%
80%
60%
40%
20%
0%
42%
39%
13%
6%
Status of Security Program
Fully Functional
Developed/ Starting to Function
Developing/ Not Developed
16%
43%
41%
(n=164)
6%
1%
13%
18%
62%
(n=182)
How often is security an agenda item at board meetings?
Quarterly
Semiannually
Annually
Rarely
Never
What percent of your total IT budget is dedicated to security?
(n=164)
<3%
3%–4%
5%–6%
7%+
41%
27%
14%
18%
0%
100%
Which security framework does your organization use?
(n=176)
NIST 75%
HITRUST 31%
SANS CIS Controls 19%
ISO 27000 13%
Other 9%
None 15%
0%
100%
What is your breach readiness level?
(n=176)
Cyber Liability and Breach Insurance in Place 79%
Breach Policy and Playbook Created 72%
Breach Incident Team Created 67%
Don't Know 6%
0%
100%

Figure 4 **Who Is in Charge of Your Security Program?**

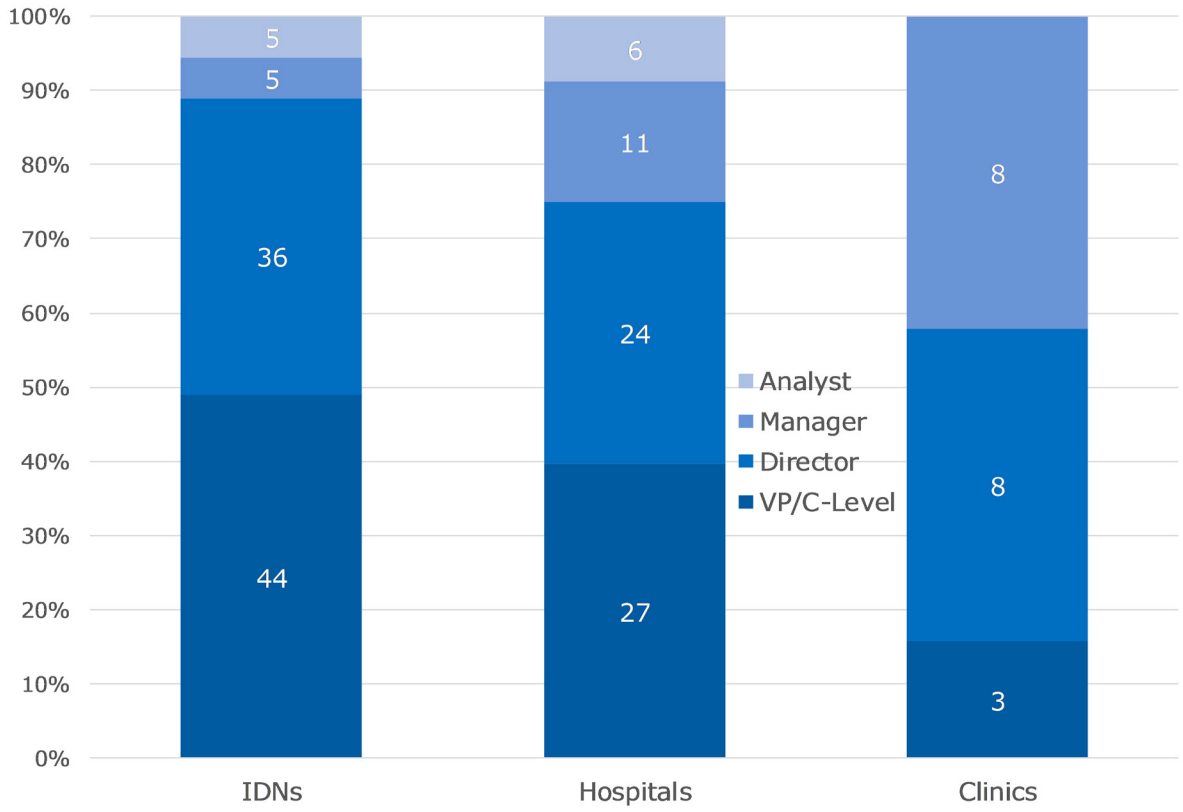


Figure 5 **How Often Is Security an Agenda Item at Board Meetings?**

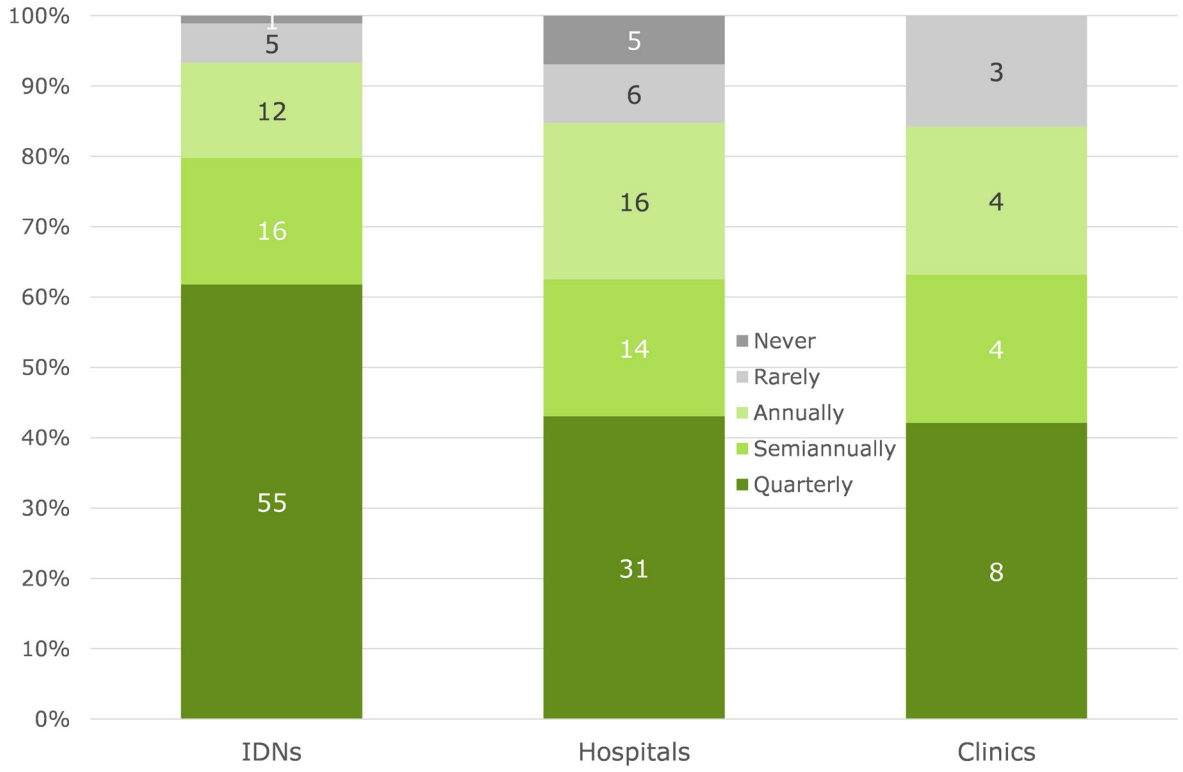


Figure 6 **What Percent of Your Total IT Budget Is Dedicated to Security?**

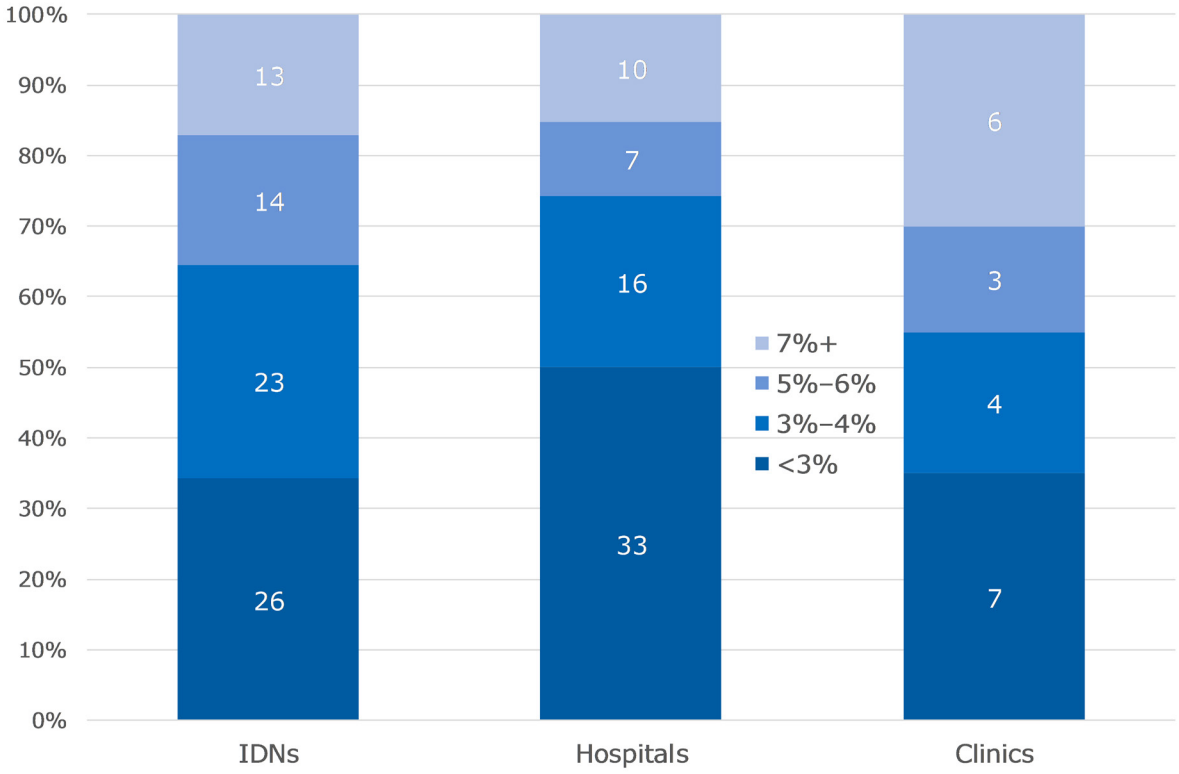
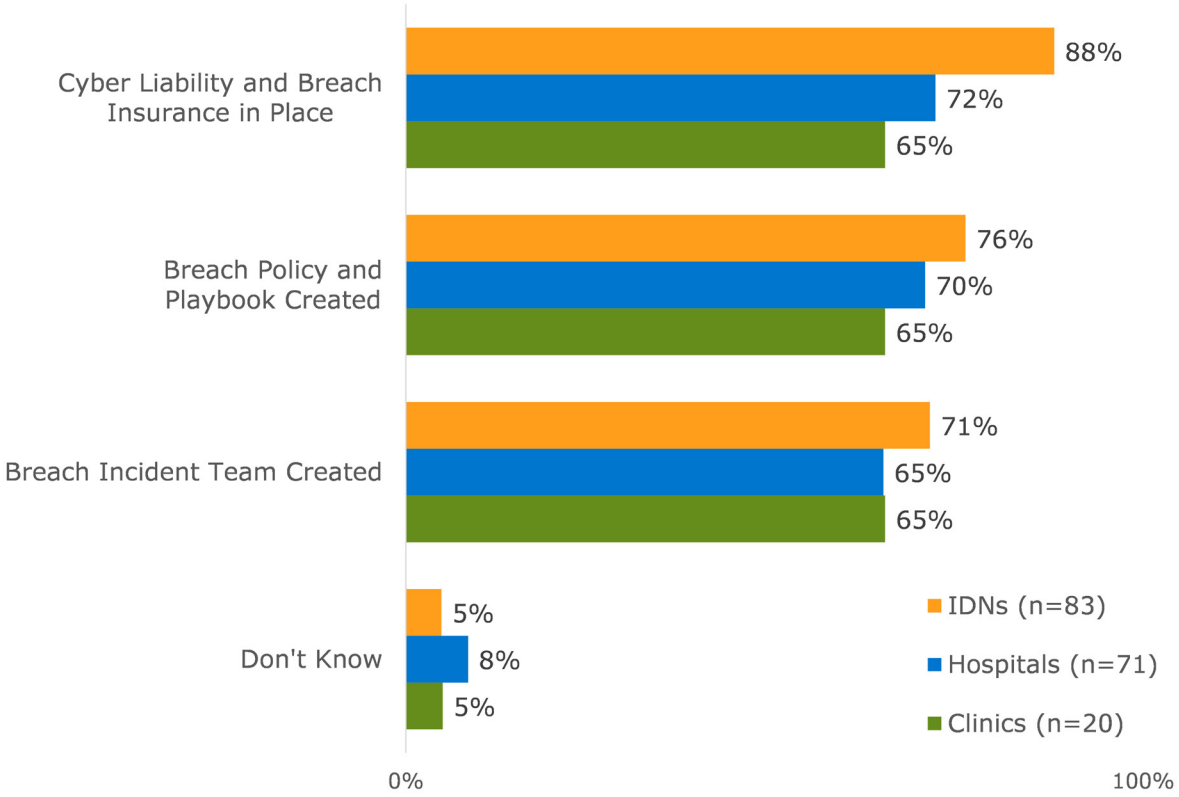


Figure 7 **What Is Your Breach-Readiness Level?**

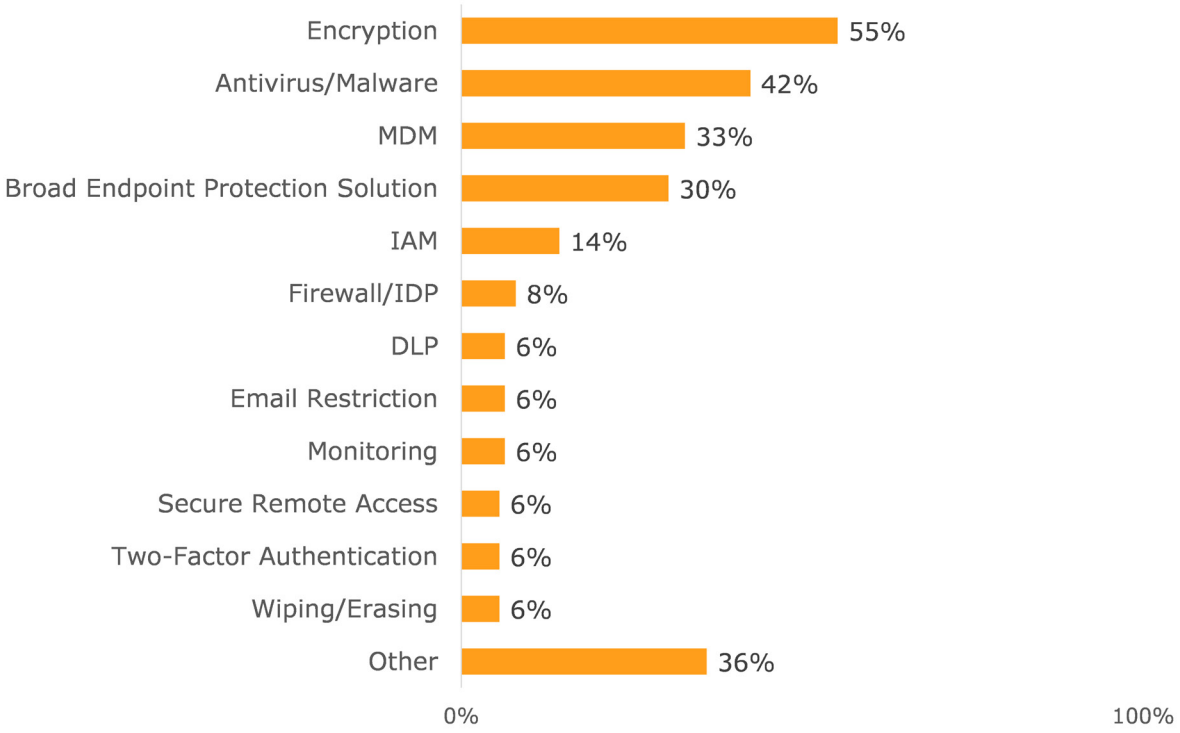


ADDITIONAL INDUSTRY SECURITY INSIGHTS

KLAS asked each organization the following questions related to their security practices.

How Are You Securing Endpoints?

Figure 8 **How Are You Securing Endpoints Connected to Your Network?**
n=125



"Other" includes Advanced Threat Protection, Anomalous Behavior Detection, Configuration Management, Device Location, Device Locking, DHCP Reservations, Domain Credentials, Filtering, Guest Network, Hardening, Life-Cycle Approach, Network Authentication, Password Protection, Patching, Restricting Privileges, Secure Messaging, Segmentation, Time Outs, Update Management, USB/Removable Device Protection, VPN, and Whitelisting.

The majority of organizations use a combination of methods to ensure the security of their endpoints, which include both laptops and mobile devices. Security professionals find themselves trying to control for end-user behavior or mistakes, which often cannot be tackled through software alone. Rarely do organizations have single-threaded strategies for endpoint protection.

An organization's approach to security can often depend on the organization's size:

- Clinics use all of the methods shown in the chart above but use the following more frequently than large organizations: MDM, firewalls, restricted use of emails on devices, and remote wiping. Clinics rarely use other methods outside of the core methods shown above.
- IDNs and those organizations that self-report as having a fully functional security program are more likely to use device encryption as a method of securing endpoints.

In general, organizations often feel that specific MDM solutions help them do better with securing mobile devices; laptops and devices wired into the network are a bigger challenge. One CISO stated,

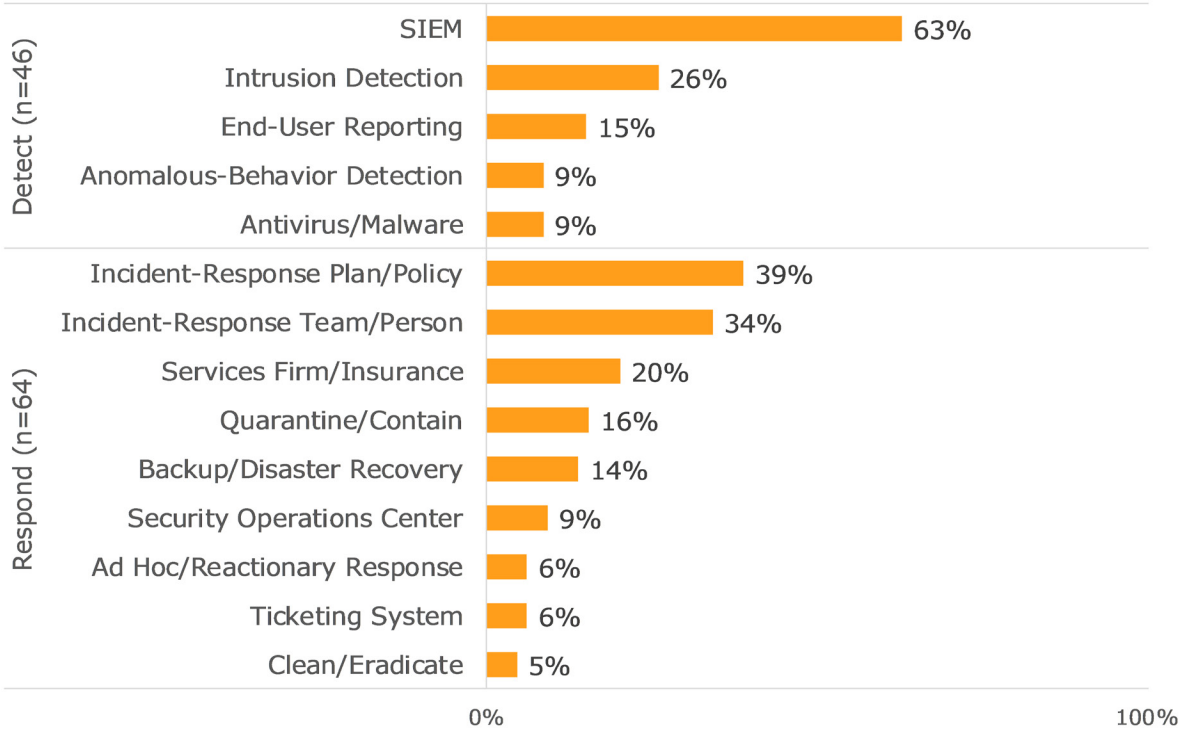
There are two levels we consider in securing our endpoints. One is whether we allow people to connect to our network that aren't known and managed. I think we are doing a good job on the wireless side, but we are not on the wired side. The other thing to consider is the managed devices. We are doing a good job of patching up things with antivirus programs. We could take that security to the next level with endpoint tools. I think we are doing a good job, but the end users are our weakest point, so we really have to work on restricting administrative privileges to the end user. We are doing well, but we could take the security up another level.

What Are You Doing to Detect and Respond to Attacks?

Numerous organizations don't have any formal protocols for dealing with incidents. Those who do have protocols in place and who talked about how they detect attacks most frequently cite SIEM as the method for doing so; SIEM is followed distantly by intrusion detection software in frequency of mentions. 15% of organizations rely on end-user reporting for things like phishing attacks.

When it comes to responding to specific threats and attacks, those organizations who have protocols in place most often point to their own self-created incident-response plans or policies. Another third have tasked specific individuals or teams with evaluating and responding to the attacks. One-fifth turn to outside insurance companies or services firms to provide guidance and come up with a plan.

Figure 9 **What Are You Doing to Detect and Respond to Phishing, Ransomware, and DDoS Attacks?**



IDNs rely relatively less on end-user reporting and are much more measured in their approach: about 80% report using a SIEM solution to detect issues. These larger organizations with more resources are also more likely to have a security operations center to handle incidents than they are to rely on a specific team or individual.

Clinics, on the other hand, rely more heavily on intrusion-detection, antivirus, and malware-protection systems to identify incidents. A lack of resources means these organizations are much more reactive to incidents rather than proactive about watching for them.

What Measures Are You Taking to Ensure Adherence to Security Policies and Procedures?

When it comes to ensuring adherence to security policies, the key is training, training, training, including a mix of in-person and online trainings (through a learning management system or other web portal) that cover HIPAA, phishing, and other security-specific topics. Organizations say new hire trainings and ongoing manager trainings are also critical. One-fifth specifically mention that they include a test or certification process with their ongoing training and education.

One-quarter of respondents run phishing campaigns, and they generally require those who are caught to undergo additional training. Two main vendors were frequently used to provide phishing testing. Other organizations do general employee awareness campaigns through email, security fairs, or intranet notifications.

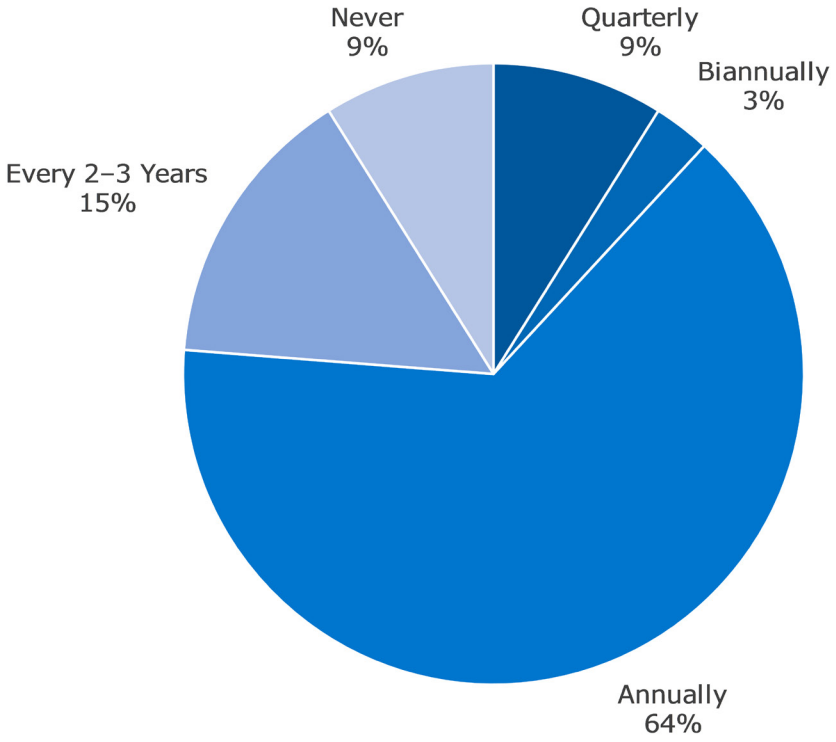
Figure 10 **How Do You Ensure Employees Understand and Follow Security Policies and Procedures?**
n=114

Some differences exist in how organizations of different sizes drive adherence. Clinics almost exclusively focus on training and don't do many awareness campaigns. They are also more likely to just require employees to review the organization's security policies and manuals. Almost all organizations with security programs self-described as fully developed do ongoing training, but they also focus on even more proactive campaigns to keep cybersecurity policies front of mind for their employees.

How Often Do You Conduct an External Risk Assessment?

Most organizations conduct an external risk assessment annually through a third-party firm and then have a team or individual follow up and address any vulnerabilities. Those that don't conduct external assessments have internal assessments. There are no significant differences in this area based on organization size or type.

Figure 11 **How Often Do You Conduct an External Risk Assessment?**
n=101



WHAT SECURITY TECHNOLOGIES ARE HAVING THE GREATEST IMPACT?

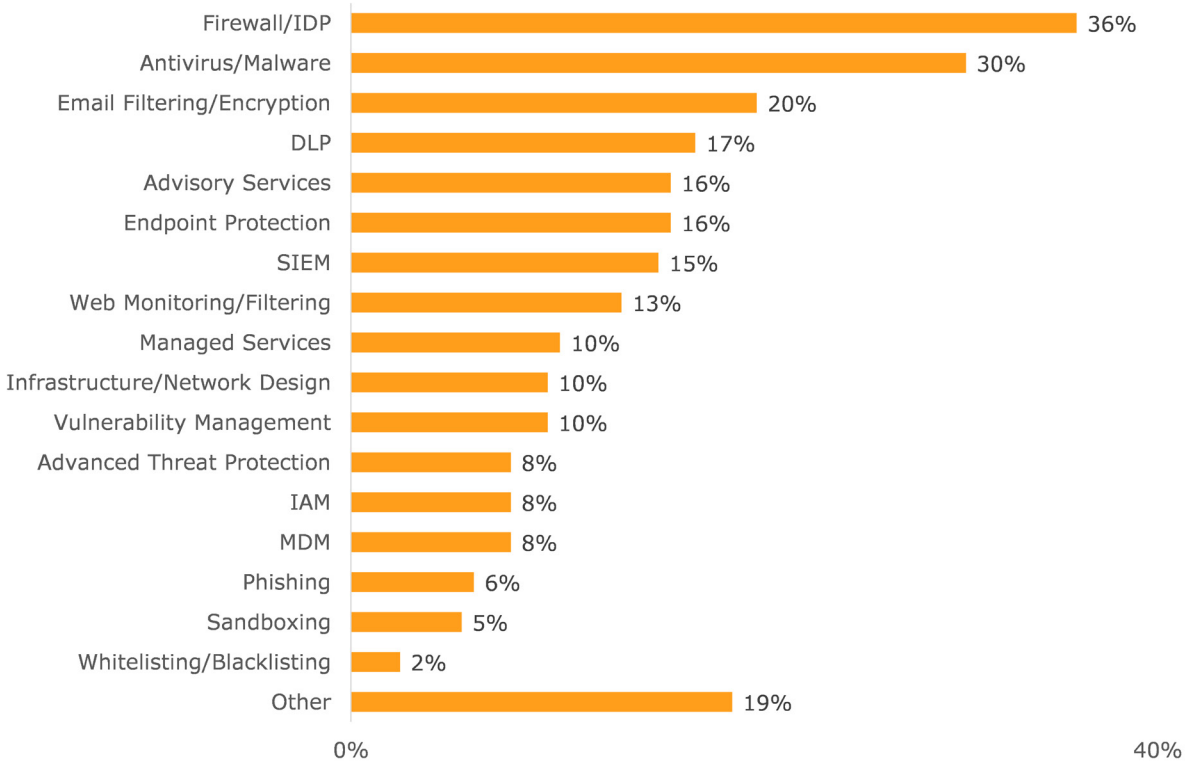
As the data above illustrates, healthcare organizations are taking varied approaches to cybersecurity. Unfortunately, cybercriminals are not slowing down in their attempts to breach systems, whether via viruses, malware, phishing, ransomware, or other targeted attacks. It is not surprising that healthcare organizations often cite foundational technologies as the most valuable in helping them build up defenses.

For example, KLAS asked security professionals at IDNs, hospitals, and clinics what technologies are having the greatest positive security impact, and the two technologies most frequently mentioned were (1) firewall and intrusion-protection software, and (2) antivirus programs and malware protection. Other technologies organizations are using to prevent data from leaving the organization include email and web filtering, encryption and endpoint protection, and DLP. Healthcare organizations also engage consulting firms in various advisory or managed services roles to help them strategize and execute on their plans. While some organizations are looking at more futuristic software that can analyze and detect anomalies in user behavior, only a couple of organizations out of the nearly 200 interviewed said they are using it today.

The larger the organization, the more complex the environment. While all types and sizes of organizations say firewalls and antivirus/malware-protection programs are having the biggest impact, larger organizations also mention using more sophisticated software. Large, multihospital organizations with more robust security programs point to solutions that help manage their complex environments. They highlight SIEM and vulnerability-management solutions as having the greatest impact much more frequently than do small organizations. They also more frequently outsource pieces or even large portions of their security portfolio to managed services firms for help handling the sheer volume of data gathered on a daily basis. Clinics more frequently say they get the greatest impact from antivirus solutions, malware-protection programs, and solutions that tackle phishing. Hospitals—both standalone and within an IDN—point to solutions that protect them from data leakage (DLP solutions) or from specific attacks (firewalls and intrusion detection and prevention solutions).

Figure 12 **Technologies with Greatest Impact on Cybersecurity**

Which technologies are you leveraging from your two most impactful security vendors? (n=164)



Note: Organizations are often using multiple technologies from their most impactful vendor. "Other" includes analytics, anomalous behavior, anti-bot, asset tracking & scanning, breach detection, cloud hosting, end user training, forensic analysis, gateway access, incident response, log monitoring, multitiered architecture, patch management, phishing training, secure messaging, virtualization, and web proxy.

WHICH SECURITY VENDORS ARE HAVING THE BIGGEST IMPACT?

There is little consensus among healthcare organizations when it comes to which vendors are having the greatest impact. A few vendors stand out, but in total, the healthcare organizations interviewed for this report mentioned 89 different vendors. Two vendors with broader portfolios rose to the top, offering a wide array of products and the ability to fill a number of gaps for healthcare organizations. Additionally, many niche vendors that focus primarily on a single aspect of security, like firewalls or email filtering, were noted by healthcare organizations as having the greatest impact.

To gain additional insights into which vendors healthcare organizations report as having the greatest impact, please refer to the full report: "Cybersecurity 2017: Understanding the Healthcare Security Landscape."

MOBILE DEVICE MANAGEMENT (MDM)

MDM is one of the most widely adopted security strategies in healthcare. Over 80% of healthcare organizations have already implemented or are in the process of implementing an MDM solution. At its core, MDM is about securing and locking down mobile devices (laptops, cell phones, tablets, etc.) so that sensitive information doesn't walk out the door with an employee. MDM is a foundational capability of enterprise mobility management (EMM), a more expansive strategy that includes MDM as well as the ability to control applications, documents, and email.

MDM solutions achieve the overarching goal of securing mobile devices in a number of ways. Some solutions encrypt mobile devices and emails. Others segment or containerize sensitive data, making it possible to remotely wipe only sensitive information from a device. Others enable organizations to manage content, allowing them to whitelist or blacklist specific applications and also push out proprietary applications. These solutions are widely used to lock down both company-issued devices and personal devices used in bring-your-own-device (BYOD) environments. These devices are most frequently iOS and Android devices.

Figure 13 **How Are You Addressing Mobile Device Management?**
n=184

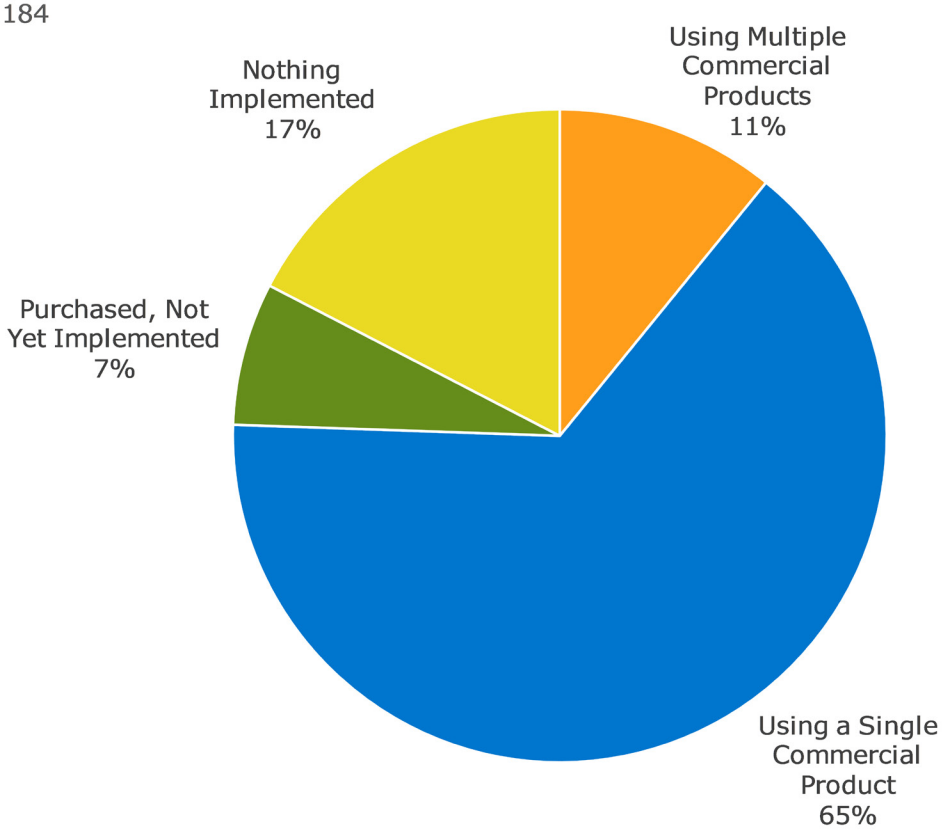
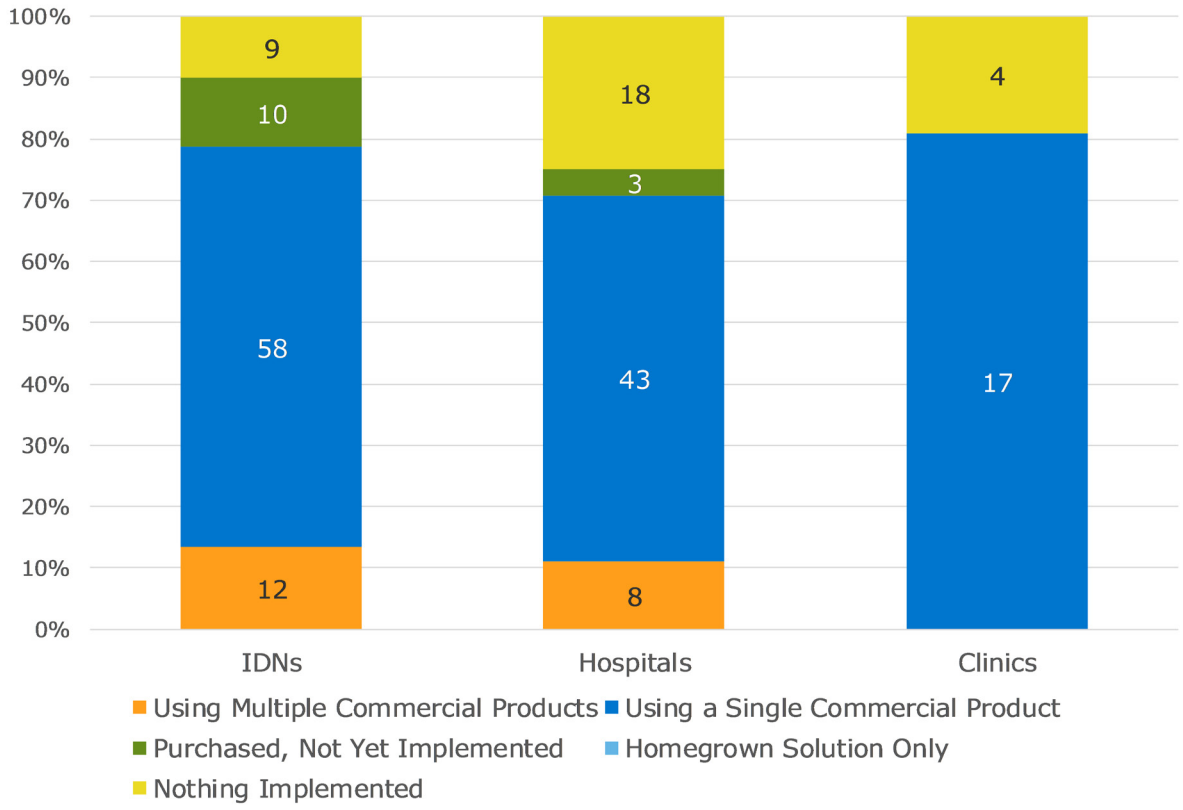


Figure 14 **Mobile Device Management—By Organization Type**



IDENTITY AND ACCESS MANAGEMENT (IAM)

Only about one in 10 healthcare organizations report that IAM is one of the most impactful strategies helping them with their security goals. The tasks healthcare organizations consider as IAM range from basic provisioning/deprovisioning with Active Directory to single sign-on, two-factor authentication, and biometric scanning in more complex environments. Even though using Active Directory is a more basic approach to IAM, healthcare organizations do count it as an IAM strategy. A number of organizations report that they use only Active Directory or use it in conjunction with other solutions. It is likely that other organizations also use Active Directory as an underlying piece of their IAM strategy but did not mention it when asked about IAM due to its simplicity.

Figure 15 **How Are You Addressing Identity and Access Management?**
n=183

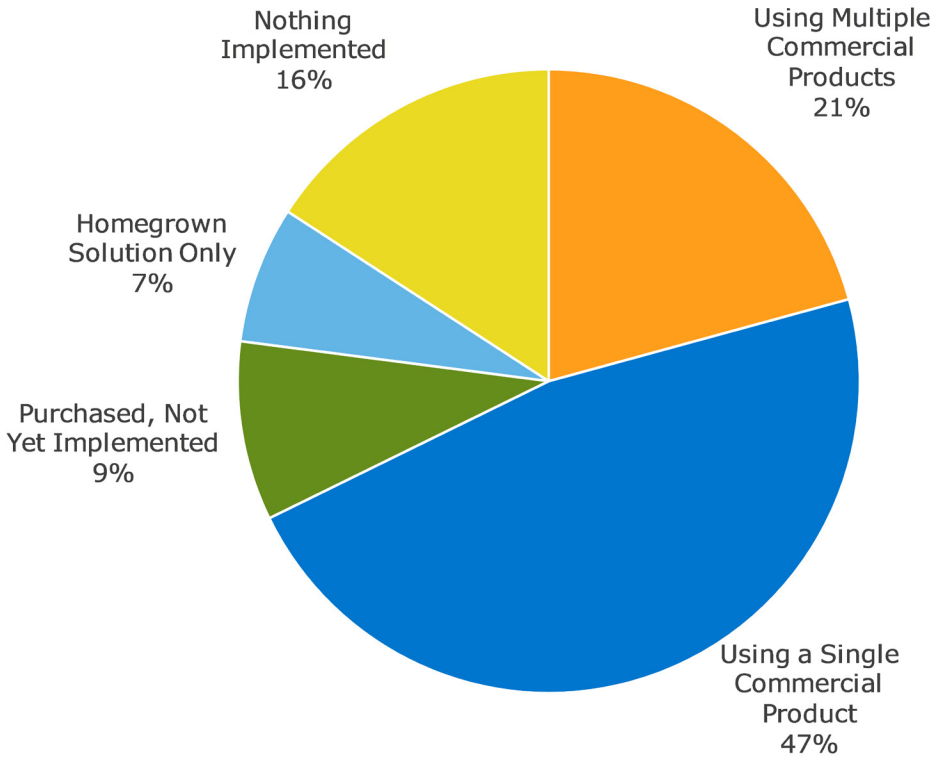
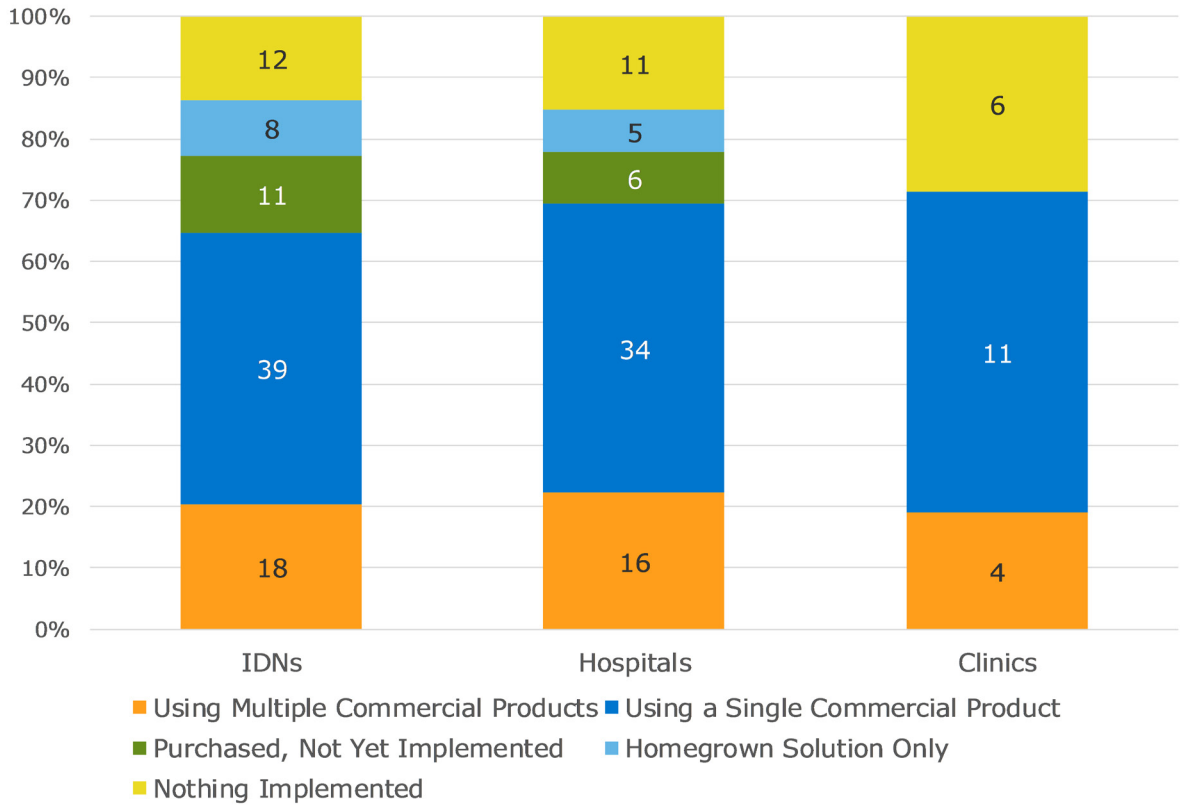


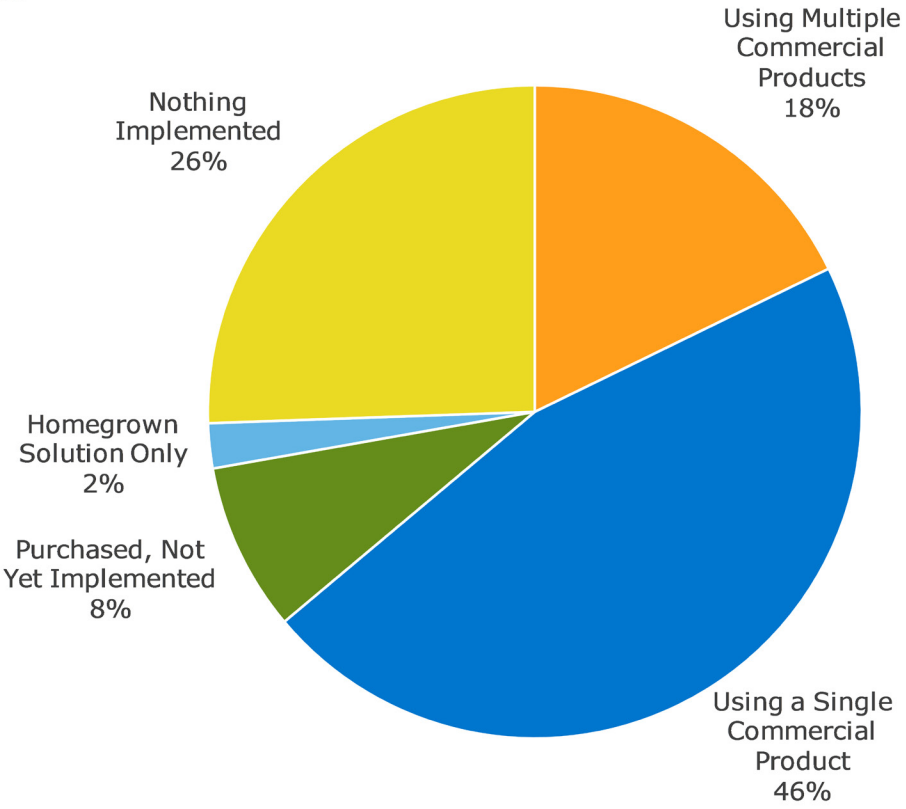
Figure 16 **Identity and Access Management—By Organization Type**



DATA LOSS PREVENTION (DLP)

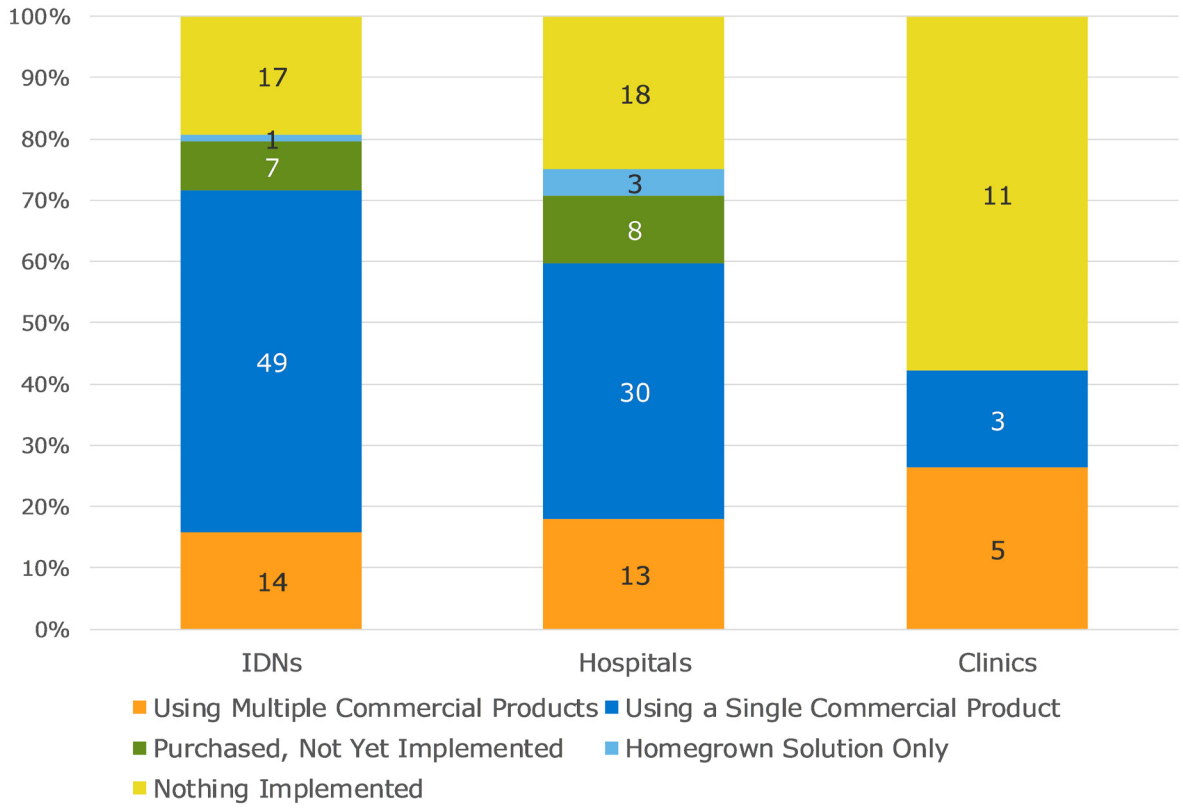
DLP focuses on preventing protected health information (PHI) or other sensitive information from leaving an organization. Nearly one-fifth of healthcare organizations say DLP solutions provide the biggest security benefit to their organization. These solutions are used in a variety of ways, the most common today being filtering and encrypting sensitive emails or preventing emails containing PHI or other sensitive information from being sent outside of the organization. Other organizations use solutions to lock down or encrypt endpoints or prevent individuals from saving sensitive information to USB drives or other discs. Based on conversations with healthcare organizations, KLAS' definition of DLP does not include data backup, disaster recovery, or inbound efforts to hijack sensitive information (like phishing attempts). Rather, for the purposes of this research, KLAS defines DLP solutions as solutions that prevent employees from sharing sensitive information, such as PHI, with unauthorized individuals, either inadvertently or on purpose.

Figure 17 **How Are You Addressing Data Loss Prevention?**
n=180



The majority of organizations (with the exception of clinics) have at least one commercial solution in place today, and about one-fifth of organizations leverage multiple commercial solutions to help lock down their sensitive information.

Figure 18 **Data Loss Prevention—By Organization Type**



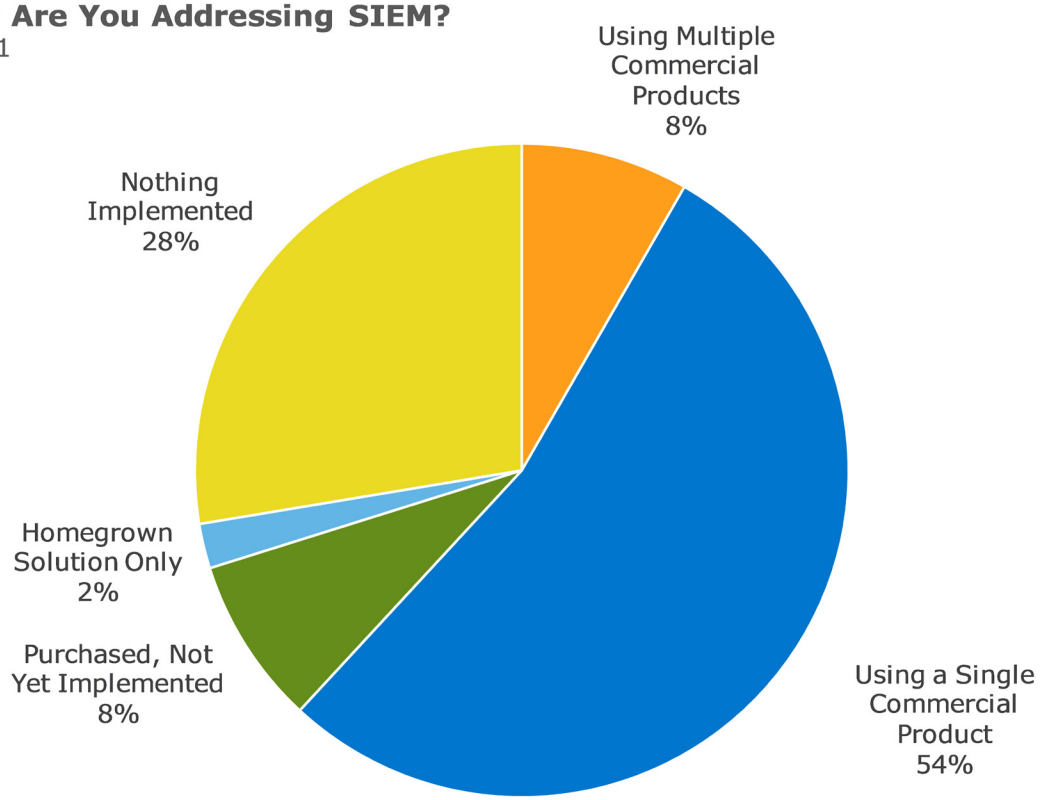
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM solutions focus on the storage, organization, and correlation of event logs gleaned from network equipment, end-user devices, servers, and other sources like antivirus applications. This data can then be monitored, analyzed, and reported on so that organizations can flag suspicious behavior, catch anomalies or other network problems, thwart dedicated attacks, and perform forensic and other compliance audits.

SIEM solutions are designed to automate the monitoring of this information, a task that would otherwise be impossible given that some organizations generate gigabytes or even terabytes of log data on a weekly to monthly basis. This sheer volume of data is the biggest challenge that organizations face in regards to SIEM. Organizations experience problems such as system slowness due to underestimating requisite storage needs and a lack of dedicated full-time employees or internal expertise to cull through all the information being generated.

As a result, few organizations are trying to tackle SIEM through homegrown methods, and it is not uncommon for organizations to outsource SIEM services. In some cases, organizations have their own SIEM solution and outsource only the 24/7 monitoring. More frequently, however, organizations outsource both the software and the ongoing monitoring to a managed services firm. Other organizations take a more measured approach by not initially including all logs, limiting their event monitoring and alerting to just network activity so that they can detect issues, such as slow servers, that could indicate a potential attack or failing disk. Only one interviewed organization is using their SIEM solution to monitor anomalous behavior, although multiple organizations say their SIEM solution opened the door for this type of analysis in the future.

Figure 19 **How Are You Addressing SIEM?**
n=181



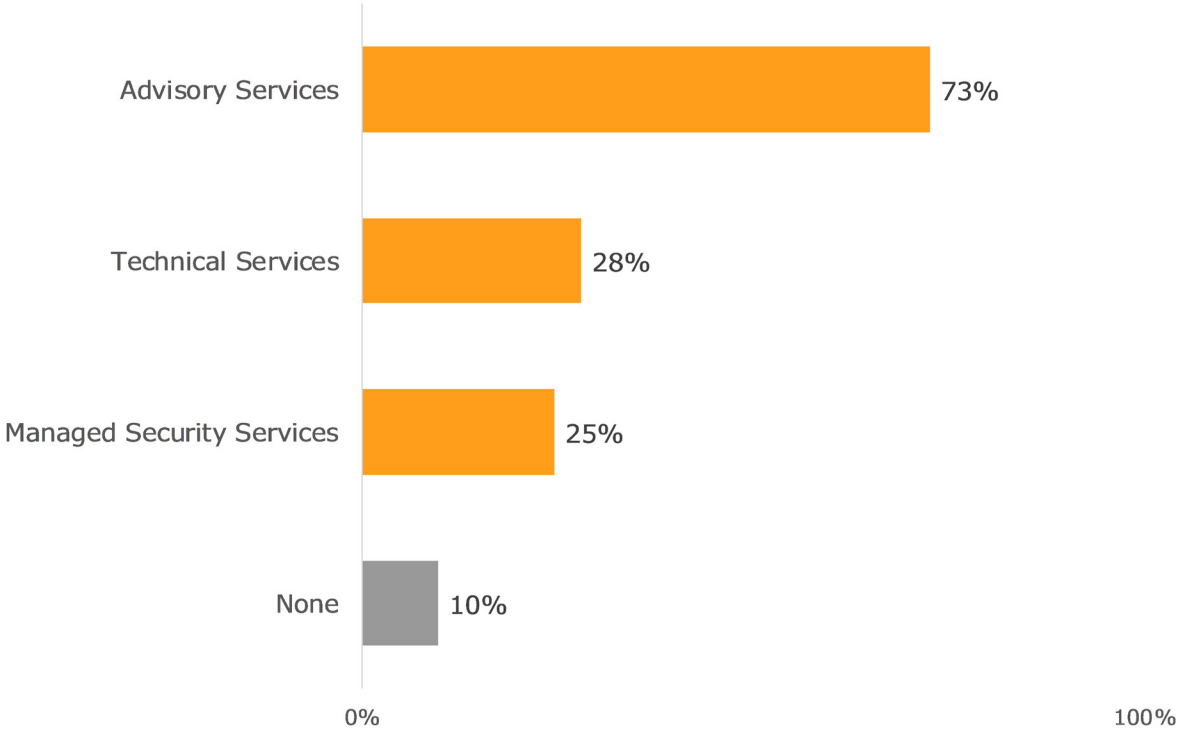
According to the healthcare organizations queried by KLAS, SIEM is currently the least mature of the four security applications covered in this report, though not by a wide margin. In all, about 60% of organizations have a solution at least partially operational today, and over 60% say that SIEM is the primary way they detect threats within their organization. Due to the sheer volume of data being produced and the complexity of these systems, few organizations have multiple solutions, and those that do use each product to monitor specific logs (for example, they might have one SIEM solution for network activity and another to help with firewall or antivirus monitoring or forensic analysis). Larger, more complex organizations are more likely to be leveraging a solution, but organizations of all sizes realize the importance of and expressed a need for a solution that can help them with HIPAA compliance reporting.

Healthcare organizations have just begun to scratch the surface of what SIEM can do for them. Most SIEM deployments are not yet mature enough for organizations to be able to gain the additional value they could from aggregating logs and data from other security software. Deep, overarching SIEM deployments have a lot of potential for more advanced uses, such as user-behavior analytics and anomalous-behavior detection, which in many regards is a missing element in healthcare IT security today. One CISO noted, *"[Our SIEM solution] is what we use to understand what is going on in security in our environment. The product is where we collate and respond to all of our security events. All of our security events go to the system, but we have to work through a process of categorizing those based on urgency and impact. We use that to react and respond."*

SECURITY SERVICES ARE FREQUENTLY USED—MANY GOOD OPTIONS EXIST

Healthcare organizations frequently turn to outside firms to gain guidance and cross-industry expertise. Only 10% of organizations have not enlisted any outside security consulting help in the past two years. Nearly three-quarters of organizations have turned to consulting firms for advisory work, such as risk/gap assessments. Often these larger advisory engagements involved more technical aspects, like penetration testing, though only just over one-quarter of organizations have consulted with a cybersecurity firm for just technical services work. One-quarter have also outsourced a large portion of their security program to a managed services firm. These outsourced agreements often make sense for organizations who feel unprepared or unequipped to handle the burden of the increased analytics and 24/7 monitoring necessitated by SIEM solutions and other applications.

Figure 20 **What Type of Cybersecurity Service Engagements Have You Done in the Past Two Years?**
n=175



HOW DO THE EMR VENDORS FIT INTO THE SECURITY LANDSCAPE?

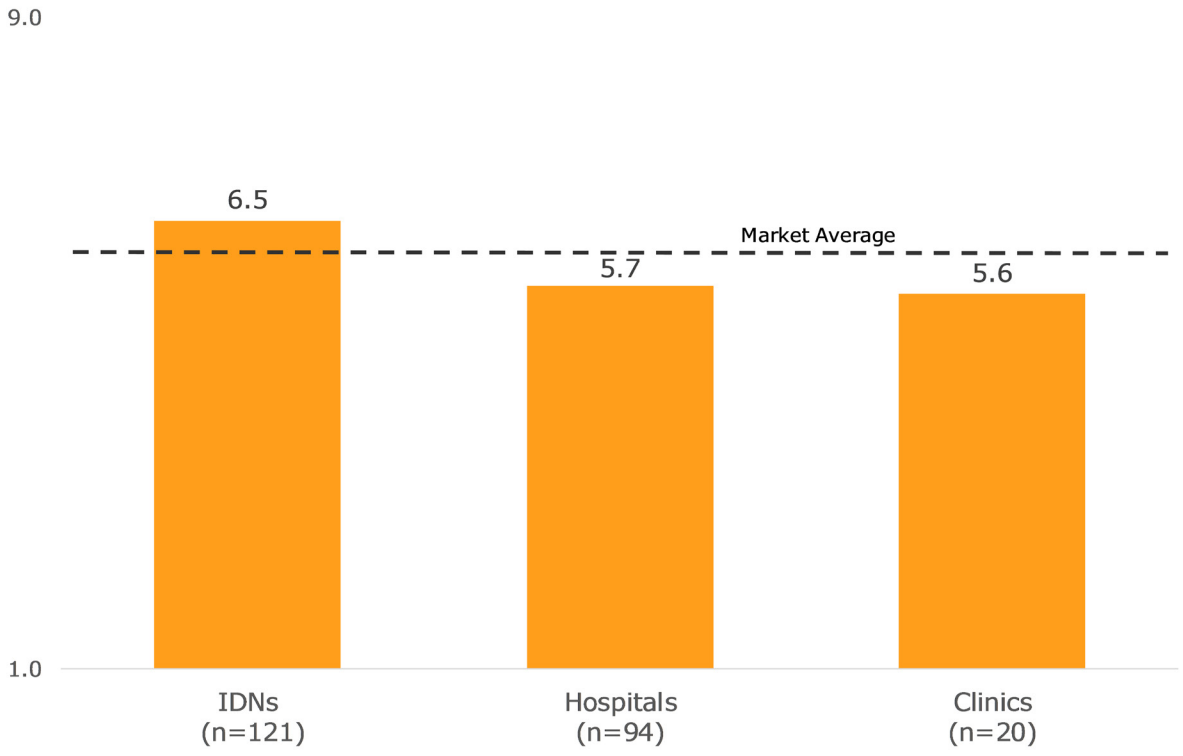
Security professionals are largely underwhelmed by their EMR (electronic medical record) vendors' focus and strategy around security. Many note that their EMR vendor is very slow to respond to their questions or does not discuss security with them very frequently. Even customers of the leading EMR vendors in the US market report that security is not a top focus for their vendor. The study did not indicate that EMR solutions are vulnerable or that the EMR vendors are not addressing security. EMR vendors all ensure that their data is secure according to HIPAA (Health Insurance Portability and Accountability Act) regulations, and customers note that most vendors are starting to think about security more regularly.

However, according to those interviewed, there is still a long way to go before healthcare organizations will be confident that their EMR vendors are helping them properly protect sensitive PHI. Organizations who assume their EMR vendor has done everything necessary on the security front are likely more at risk than they think. A security director explained,

> *All healthcare vendors have started to improve in regard to security. Everybody gives lip service to the fact that security is their top concern, but in the reality, when people are working in a technical environment and trying to troubleshoot things or work through issues, people get sloppy. That is just inevitable. That is not specific to our healthcare vendors; all of the vendors have a long way to go. I am starting to see a change in behavior. Vendors are trying to go as fast as they can to get to a point where they are doing things right.*

Figure 21 **Security Ratings for EMR Vendors—By Organization Type**

How well does your core EMR vendor support your organization's security goals? (1–9 scale)



CONCLUSION

As this report highlights, healthcare providers are using multiple approaches to shore up their cyber defenses. Importantly, cybersecurity seems to be garnering more attention from the C-suite and boards of trustees. Yet we also know that cyber criminals are continually finding new and more sophisticated tactics for breaching a network. Also, securing information systems will become increasingly complicated as delivery system reforms create greater connectivity between providers, payers, and patients. Recognizing that information is power, KLAS and CHIME will continue to measure industry practices in cybersecurity both individually and collectively. KLAS will continue to monitor the cybersecurity market with targeted, more in-depth studies focused on vendor performance in areas such as DLP, MDM, IAM, and SIEM.

To gain additional insights into how the security, services, and EMR vendors perform and to view customer commentary, please refer to the full report: "Cybersecurity 2017: Understanding the Healthcare Security Landscape."