INDUSTRY FOCUS:
HEALTHCARE
5 INDUSTRY NEEDS:

1. Hacking incidents and ransomeware attacks have increased and are the biggest threat to protected health information (PHI) security. Malware threats are a driving force behind a rise in IT expense.
2. Healthcare organizations often have limited IT budgets, IT resources, and ineffective security technologies that create an environment vulnerable to security breaches.
3. The move towards the digitization of patient record have introduced greater security risks to PHI and have led to the increased number of data breaches. Many hospitals are replacing legacy systems with legacy integration products and some with less expensive integration platforms. IT departments need to review their current technology platforms with an eye toward the changing security environment instead of addressing new healthcare requirements.
4. IT departments face mounting pressure to address and meet compliance requirements and are spending less time monitoring network traffic and applications, implementing user data access controls, fixing network vulnerabilities, improving security posture, and protecting patient privacy. Data loss incidents are overwhelmingly caused by failure to implement and monitor data access control. Employees are accessing records that should have been out of reach.
5. Healthcare providers need effective security technology and risk management practices that are capable of pinpointing security risks with both external and internal security threats.

PERSPECTIVE

2016 could be the worst year for healthcare data breach fines. Poor cybersecurity for patients’ healthcare records could cost hospitals, clinics, and medical centers a significant amount in financial settlements. The U.S. Department of Health and Human Services since last
November obtained more than $16 million in settlements from just five entities related to electronic patient data breaches. According to Healthcare IT News, “as data theft, ransomeware, network attacks, and accidental privacy violations continue to plague healthcare organizations of all sizes, the HHS has announced plans to devote more resources to investigate smaller breaches. Whether it’s simply noncompliance with HIPAA regulations or victimization at the hands of shadowy cyber crooks, providers, payers, and business associates - irrespective of size - are all vulnerable to breaches.”

Many healthcare providers have embraced the move toward the digitization of electronic health records due to regulatory pressure, security, as well as the convenience and efficiency of accessing patience information and improving patient care. Unfortunately, the promotional efforts to attract providers in bringing patient records into the digital world have not kept pace with the efforts to promote computer network security and to advance the cause of investing the most capable IT security technology in order to protect the security of large volumes of sensitive data now stored in databases. The movement towards the digitization of patient records in reality has introduced greater security risks to protected health information (PHI) resulting in higher incidences of data breaches and the proliferation of aggressive cyber attacks each year. The healthcare industry has become a gold mine for both financially-motivated hackers and insider thieves alike as medical records, contact patient information, addresses, birth dates, social security numbers, insurance information, detailed physical information, and beneficiaries. According to the Identify Theft Resource Center Breach Report, last year the Health/Medical sector came in second place for the highest number of breaches publicly reported. This year the healthcare data breaches are continuing at an alarming pace with more breach incidents occurring per month. Hospitals have been hit with 88% of all ransomware attacks as patient data is worth more than any information on the back market. Some of the most high profile hospital data breaches this year are results of ransomware attacks.

The healthcare industry is a constant target for cyber attacks and has been named as the most breached industry. The industry’s reputation as being a soft target for hackers and insider thieves alike are due to a number of factors. IT departments operate with limited IT budgets and lack the crucial resources to effectively manage and maximize security operations. All of healthcare IT is aware of cyberattacks and the potential danger of losing patient data, and yet IT budgets remain stuck. In addition, IT departments are subject to using outdated and ineffective security technologies, making it more difficult for IT departments to pinpoint security risk. IT departments are also experiencing mounting pressure to address and meet compliance requirements and are spending less monitoring network traffic and applications, implementing user data access controls, fixing network vulnerabilities, improving security posture, and protecting patient privacy. Furthermore, healthcare facilities are also facing an aggressive threat with the growing problem of targeted malware which is more difficult to detect and prevent. Malware incidents such as ransomeware exploit kits have become the biggest threat to PHI security and are a driving force behind a rise in IT expense.
WHY LEADING HEALTHCARE ORGANIZATIONS RELY UPON AANVAL:

- To proactively monitor and respond to all security breaches, including malware and ransomware exploits which can help reduce IT expenses.
- To deliver a market-leading network security solution that will also provide substantial cost savings while improving risk management practices and meeting regulatory requirements at the same time.
- To proactively monitor and respond to both external and internal security breaches including malware exploits in real-time.
- To drive operations efficiently through the intelligence use of automation technology. Aanval’s automated database management simplifies the security tasks of capturing and managing a large number of security events as well as creating valuable user and database activity reports to monitor insider threats and delivering real-time alerts.
- To obtain real-time situational awareness in order to quickly and accurately summarize network event information and provide IT departments with the resources they need to identify actual risks and make sound decisions during critical moments.
- To effectively deliver crucial scalability to accommodate additional network growth and to also manage, archive, and store more than 1 billion events.
- To improve network security posture across all networks including WLAN network devices, thereby protecting PHI information.

TACTICAL FLEX, INC. SOLUTIONS

Most of the data breaches in 2015 were due to third-party cyber attacks. Consistent studies conclude that security threats facing both large and small healthcare organizations are both equally high and damaging. Security experts predict that there will be more organization hacking attempts that are already confronting the entire medical industry. The biggest challenge facing the healthcare industry overall is to find the most capable information security tools to implement and manage both security measures and security requirements. IT departments need to assess and review their security technology tools with an eye toward the evolving security threat environment instead of addressing new and changing healthcare requirements. Healthcare organizations in turn need to ensure that they are taking every
precaution to safeguard their patients’ confidential information and provide sufficient resources for IT departments to operate more effectively.

Tactical FLEX, Inc. understands that healthcare organizations need a comprehensive and affordable real-time threat management solution that gives IT departments the technological power and operational efficiency to accelerate the accurate detection of security threats as well as pinpoint security risks in order to safeguard the privacy of PHI and maintain regulatory compliance. Aanval’s SIEM and IDS solution provides around-the-clock monitoring of all in-bound and out-bound network traffic including both user and database access activities and the effective detection and prevention of malware exploits. Aanval’s next-generation technology features include a unique situational awareness engine which allows IT departments to quickly identify which specific devices, services, and approximate areas of the network that are most at risk and which are more likely to be a problem in the future. In addition, Aanval also delivers multiple source event collection, correlation and archiving, and false positive-reducing event validation which further delivers advanced event analyses, making it simpler to investigate and prevent anomalous behaviors including advanced threats.

Additionally, Tactical FLEX, Inc. is a trusted security vendor, with its products and services operating within dozens of healthcare organizations throughout the world in full compliance with HIPAA and other associated regulatory requirements.

Review Aanval products and Aanval services or contact us at 800-921-2584 to speak with our knowledgeable staff immediately.