LOGPOINT

Securing the digital transformation in the healthcare sector

The healthcare sector is going through a rapid digital transformation. Electronic Medical Health Records are being implemented everywhere, and the volume of sensitive records is soaring. The number of users accessing sensitive data is exploding and medical technology is increasingly relying on an interconnected network of devices.

The complexity is increasing, and so is the risk of cyber attacks disrupting vital services, or breaches leading to massive privacy infringements. At the same time, compliance requirements such as GDPR, HIPAA, and ISO2700X are increasing. The LogPoint SIEM solution is a key tool in ensuring the digital transformation in the healthcare sector.

Cybersecurity challenges of a vital sector

Not long ago, it was reasonable to think that the financial industry would be the most prominent and most profitable targets of cybercrime. After all, the rising volume of electronic payment transactions and the vulnerability of credit card information, made this industry an attractive target. However, today it's the healthcare industry that is facing the brunt of cyber attacks.

As an example, Ransomware attacks have grown dramatically over the past years, with healthcare organizations being a very common target. These incidents range from low-key and barely noticeable to large-scale hacks that have taken down hospitals for weeks at a time. In the UK, the 2017 WannaCry cyberattack disrupted more than 80 hospitals and 8% of all general practices. 19.000 appointments were canceled across the one week of the attack, with an estimated 1% of all care disrupted.

A 2018-report by the UK Department of Health and Social Care revealed that the WannaCry ransomware attack cost the UK National Healthcare Service (NHS) a total of GDP 92 mill. through services lost during the attack and IT costs in the aftermath. The report estimates around GBP 20 mill. was lost during the attack mainly due to lost output, followed by a further GBP 72 mill. from the IT support to restore data and systems.

The value of healthcare data

Part of the cybersecurity problem in the healthcare sector has to do with the enormous value of healthcare data, made increasing accessible by the rapid deployment of Electronic Medical Health Records (EHR) in hospitals and national healthcare services all over the world. EHRs offer significant benefits and have been adopted by over 96% of critical care hospitals and over 83% of regular hospitals in the US.

While the digital transformation overcomes many of the inefficiencies and fragmentation that has plagued healthcare providers previously, patient records are now also more susceptible to hacking and theft. On the US black market, the going rate for a social security number is 10 cents. A credit card number is worth 25 cents. But an EHR could be worth hundreds or even thousands of dollars.

The EHR contains a wealth of exploitable information which attracts hackers. This includes demographic information, names, historical information of where you live, where you worked, the names and ages of your relatives, past medical history, including every doctor's visit you've made and diagnosis you've received. The medical record is likely the most comprehensive record about the identity of a person that exists today, and while you can cancel credit cards and change social security numbers, an EHR remains.

Lives are at stake

However, in the healthcare sector, it's not the monetary value of records or the logistical annoyances of recovering from a cyber-attack that is the main concern. People's lives could be at stake. A 2019-study from Cornell University documents, that even if the quality of care patients are receiving isn't directly affected by a cyber attack, 30-day mortality rates rise significantly after a hospital data breach. As hospitals are stretched thin with resources, and staff members are more stressed than usual in the wake of a cyber attack, the quality of care naturally goes down.

Hospitals are also vulnerable because their systems are becoming increasingly complicated. Medical technology is increasingly relying on an interconnected network of devices. In hospitals, this means nurses and doctors rely on tablets and mobile devices in addition to computers and monitoring equipment. In patients, this means sensors, monitoring equipment, and sometimes even prosthetics that collect information or provide treatments.

This complexity isn't limited to the security or integrity inside hospitals and among professional medical staff. As our healthcare systems increasingly rely on digital self-service interfaces for patients, much of the security burden is placed on patients. Patients are the ones responsible for creating, maintaining, and protecting their passwords and login credentials. All it takes is one lapse in security from a patient, a doctor, a nurse, or another staff member to cause serious harm.

Using LogPoint SIEM to secure the digital transformation in the healthcare sector

For healthcare organizations operating at large scales, increasing efficiency is a constant requirement, often driven by political demand. Digital systems and applications are helping to meet that need, providing easier communication, accessibility, mobility, convenience, and productivity for the administration and patients. But with that transformation comes the increased risk of data breaches.

Healthcare IT infrastructure is facing an unprecedented threat level, stemming from actors as diverse as cybercriminals, hacktivists, thrill-seekers, and insiders. Adding to the problem, many healthcare organizations use a complex mix of specialized devices, proprietary applications, and off-the-shelf products that are connected to the Internet, increasing their exposure to cyber threats.

As the cybersecurity challenges in the healthcare sector has only been increasing in the past years, and the amounts of sensitive data have been increasing, government authorities and regulators, have responded with legislation and requirements for compliance with security standards. And while Compliance requirements is an extremely valuable driver in increasing cybersecurity and privacy protection, implementing standards is difficult and consumes vast amounts of resources.

Healthcare organizations are facing a number of challenges, including:

- Increased privacy requirements have to be met while maintaining smooth IT operations and secure data of citizens
- Increased complexity in the infrastructure makes it challenging to obtain centralized analysis across the organization
- Difficult to detect cybersecurity threats across complex IT infrastructures, including advanced persistent threats and insider threats
- Rising data amounts means more expensive analysis- and cybersecurity operations
- Compliance requirements are increasingly difficult and resource consuming to meet

Many public organizations tasked with securing data may not have the right solution to do so. It's a problem – but one with a solution. That solution? Security Information Event Management or SIEM. LogPoint SIEM.

LogPoint's seamless, quick reporting on unusual behavior in the network easily adapts to compliance requirements specific to your organization. By keeping an eye on everything going on in your network, LogPoint positions you to address a possible breach quickly, limiting potential damage and protecting privacy.

Extensively proven in the healthcare sector

LogPoint has been providing our modern SIEM solution to customers in the healthcare sector for years. Dozens of public and private hospitals, elderly- and psychiatric-care institutions as well as universities and life science/ medical research institutions rely on LogPoint for cybersecurity, compliance, IT operations, and Business Analytics.

Our SIEM solution collects and aggregates log data generated throughout the IT infrastructure, from systems and applications to network and security devices, such as firewalls and routers. The SIEM identifies, categorizes and analyzes incidents and events to deliver real-time alerts, dashboards or reports to the cybersecurity teams.

Cybersecurity without restricting access to digital resources

The LogPoint SIEM solution allows healthcare organizations to immediately detect cyberthreats, without severely restricting access to digital resources. LogPoint provides monitoring, detection, and alerting of security incidents. It provides a comprehensive and centralized view of the security posture of the infrastructure and gives public cybersecurity professionals detailed insight into the activities within their IT environment.

With User Entity Behavior Analytics (UEBA) LogPoint provides extensive machine learning and anomaly detection capabilities for advanced threat detection. Leveraging advanced Machine Learning enables you to detect cyber attacks immediately by spotting unusual patterns of activity and eliminate false positives.

Supports all aspect compliance

The LogPoint SIEM solution is an invaluable tool for compliance auditing and reporting, especially when there are disputes involving digitally stored data and potential fraud. LogPoint's SIEM solution provides compliance for all major healthcare regulatory domains such as HIPAA, GDPR and ISO2700X. LogPoint supports Forensic analysis and investigation, making it effortless to present compliance evidence and determine the root cause of the breaches, improving the overall security posture.

In a nutshell, SIEM allows healthcare Cybersecurity teams to see the bigger picture by collecting security event data from any application, the cloud and core infrastructure to learn exactly what goes on within the infrastructure – creating value from the sum of data which is worth much more than the individual pieces.

This ultimately can assist cybersecurity teams to increase their effectiveness and reduce the resources required to run security operations – which is important in a time where there's a shortage of security skills and an ever-increasing number of alerts.

Healthcare Cybersecurity Use Cases

Data theft/Extraction

Being able to detect suspicious activity around sensitive and classified information is an important step to secure your infrastructure against data exfiltration. LogPoint monitors your organization's infrastructure by observing behaviors around enterprise applications, often storing key information subject to theft and extraction. With LogPoint, you can:

- Protect essential processes, sensitive data, and intellectual property by tracking behavior around and access to privileged information
- Track unauthorized network or system access linked to malicious actors
- Monitor admin rights of external parties to ensure the confidentiality and integrity of sensitive information
- Identify potentially malicious inbound communication from suspicious domains or identified threat sources to secure your organization from phishing attempts

Privilege misuse

What if the threat is coming from inside the four walls of your organization? The ability to detect lateral movement and suspicious or abnormal behavior in the network before exfiltration can defend against an insider threat. LogPoint uses UEBA and exhaustive compliance regimens to monitor and detect fraud within enterprise applications, infrastructure including Active Directory and cloud-based services such as Azure, AWS, and Salesforce. With LogPoint, you can:

- Monitor administrative accounts to alert and report on unauthorized access attempts
- Get notified of new or disabled accounts that doesn't have the appropriate approval levels
- Track access to mailboxes and identify potential misuse
- Detect sudden changes in user, entity or server behavior by combining anomaly detection with advanced correlation
- Detect unauthorized privilege escalation
- Uncover and audit configuration and policy changes
- Identify attempts to exfiltration data quickly and efficiently

Human error

Unintentional data breaches are common in healthcare, and in some cases, institutions have left the patient's sensitive data wide open to the public. Simple employee mistakes can become expensive incidents that can damage your organization's finances and reputation. LogPoint monitors network access, policy changes, file system activity, and file access to help you identify misconfiguration, misdelivery, and disposal errors. With LogPoint, you can:

- Employ retention policies to guarantee that sensitive patient data isn't kept longer than necessary
- Ensure disposal of sensitive data on a granular level by applying routing policies directly to your logs, and limiting access to sensitive information such as personally identifiable data with data privacy mode.
- Review your system configurations from a single pane of glass to rapidly identify misconfigurations that have the potential to render classified information public
- Identify policy misconfigurations before classified information is rendered public

Malware/Ransomware

Advanced cyber threats like Malware, and in particular the Ransomware subcategory, are highly sophisticated threats that can cause extensive operational, reputational and financial damage. Standard anti-malware controls and endpoint solutions often fail to block or prevent these attacks as detecting them requires a powerful analytics tool combined with Threat Intelligence and behavioral analytics. With LogPoint, you can:

- Use Threat intelligence to identify critical threat indicators matched against the threat intelligence database or based on threat categories or threat scores
- Define cybersecurity risk posture by comparing threat indicator scores and understanding the geographical distribution of attacks
- Statically enrich any threat indicator (IP address, domain name etc.) to get an instant overview of potential risks.
- Perform advanced analytics correlation and pattern recognition to provide real-time alerts on risky behavior, and anomalous activities

Healthcare Compliance

The LogPoint SIEM solution enables compliance monitoring of your entire organization. It also provides easy access and overview of data for auditors and regulators to prove compliance, preventing you from being needlessly tied up in long processes. It helps you meet the day-to-day requirements of the most demanding regulatory standards, makes the workload of audits less intensive, and provides a clear picture of whether or not you have the right security measures in place. LogPoint supports compliance by:

- Streamlining data collection to LogPoint, making it convenient to gather data from your infrastructure
- Storing event logs for easy access to complete and secure audit trails
- Enabling rapid threat response for identification, remediation, and reporting
- Alerting of policy and compliance violations
- Validating that controls are in place and optimized
- Resolving critical issues before they jeopardize your compliance posture by correlating diverse events from across your infrastructure
- Documenting incidents, including detailed, auditable records
- Providing out-of-the-box and customizable compliance reporting

LogPoint supports compliance with prominent healthcare standards such as GDPR, HIPAA, and ISO2700X, but are also extensively used in support of other standards such as FISMA, BASEL-II, GPG13, and PCI-DSS. Additionally, compliance reports can be modified or new reports can be created from scratch using our intuitive Report Wizard.

GDPR

The GDPR, short for General Data Protection Regulation, is Europe's unified data protection framework which applies to any EU or non-EU organization processing personal data of individuals based in the EU. The increased data security requirements of GDPR mean that all healthcare organizations have to seriously consider how to ensure compliance as the effects of non-compliance can lead to severe penalties. LogPoint helps by:

- Automating Reporting and audit through an extensive range of pre-defined GDPR reports right out-of-the-box providing you with critical insights helping you to ensure confidentiality, integrity, and availability of your data
- Spotting and tracking unauthorized network or systems access using Data Privacy Module functions under the Four Eyes Principle, meaning that at least two users are required to handle critical information in an organization at all times
- Spotting and tracking unauthorized network or systems access by enabling you to detect any suspicious and/or unauthorized network behavior such as connection attempts on closed ports, blocked internal connections, etc.
- Monitoring international data transfers by using LogPoint's intuitive visualization, providing any organization with a detailed overview of cross-border data flow, ensuring lawful data transfer complying with the GDPR.

HIPAA

HIPAA, the US Health Insurance Portability and Accountability Act, aims to reduce concerns for health insurance coverage, provide good access to health insurances, increase in health industry efficiency and protect health information data in electronic form. The Act makes it mandatory that health care providers, clearinghouses, health care plan providers, departments of healthcare, and other agencies, to patients that their data is secure along all dimensions of security. LogPoint helps by:

- Monitoring File Integrity (FIM) using LogPoint's native FIM module, that calculates the hash value of files, before and after changes could have been made. This way, you will always be in control of your sensitive assets and get alerted whenever a new directory or file is created, deleted, renamed or altered in its content.
- Detecting Access to Systems by users or other systems along with other important contextual information such as the actions performed, the final status, or other entities used like IP addresses. Monitoring access control helps to verify users viewing systems and resources.
- Providing Authentication and Transmission Control, ensuring that users are who they claim to be. This can include password-based authentication, public-private authentication, or two-factor authentication.

ISO2700X

ISO 2700X (ISO27001 and ISO 27002) is an information security standard published by the International Organization for Standardization (ISO). It specifies a management system intended to bring information security under management control and gives specific requirements. ISO 2700X deals with all aspects of Information security including Access control, Operations security, and Communications security. LogPoint helps by:

- Management of privileged access rights by monitoring and logging successful and failed login events to assets across your on-premises and cloud environments
- Protecting log information by storing logs in an safe format and monitoring all activity, including the access and actions performed on log data. In this way, logs are protected against tampering by unauthorized personnel
- Provides Network security management by monitoring and correlating events from the entire IT infrastructure, from systems and applications to network and security devices, such as firewalls and routers to identify anomalous network traffic, such as communication to a known malicious server

How is LogPoint working with the Healthcare sector

Protecting patient integrity

Region Värmland is one of 21 Regions in Sweden. The region is responsible for the healthcare and dental care of approx. 280.000 citizens Usually SIEM is about monitoring and analyzing log data coming from the IT infrastructure such as firewalls, routers, applications, and the like. But in Region Värmland, LogPoint is at work logging medical record views. This helps Region Värmland to better comply with patient data laws, and safeguard citizens' integrity. LogPoint helps by:

- Monitoring and analyzing access to patient data and reduce false positives
- Protects patient data integrity
- Ensures compliance with the Swedish Patient Data Act

"The strength of the LogPoint solution is that we don't have to spend unnecessary time on investigating false positives and that we check all logs. Not only logs chosen at random. This way, we comply with the legal requirements of effective log auditing."

Joakim Bengtzon, IT Security Manager, Region Värmland

Supercomputer Cyber Security and Compliance

Computerome (Denmark), the Supercomputer for Life Science is a collaboration between Technical University of Denmark (DTU) and University of Copenhagen (UCPH), two of Denmark's leading public education and research institutions. LogPoint was chosen by Computerome as a key security platform to ensure the highest level of security and compliance. This was done by:

- Offering a full custom integration services – LogPoint's single taxonomy allowed for easy integration with the Computerome systems
- Enabled real-time monitoring of security controls, providing real-time data analysis.
- Early detection of possible data breaches, data collection, data storage, and accurate data reporting.
- Built-in log analysis is configured to automatically detect and notify all critical events in the Computerome system before as happen.

"LogPoint allows Computerome administrators to quickly detect unusual behavior in the system and to prevent misuse and data breaches. It provides that extra layer of security on top of the established security controls, which is required when handling vast amounts of data. It also allows us to provide our users with full insight and transparency."

Peter Løngreen, National Life Science Supercomputing Center

Achieving super-compliance in healthcare IT services

RAM Infotechnology is a Dutch IT services company, specializing in IT outsourcing, managed services and cloud-based services. Headquartered in Utrecht, the company is primarily serving the public healthcare sector and is handling more than 15 million electronic patient records. To ensure the highest possible standards in handling sensitive information, RAM Infotechnology selected LogPoint to support compliance with an array of certifications, including ISO 9001, ISO 14001 and ISO 27001 as well as the EU General Data Protection Regulation (GDPR). Also, LogPoint enables RAM Infotechnology to provide managed SIEM services to end-customers. LogPoint helps by:

- Supporting compliance with a vast array of industry standards
- Reducing time spent on compliance reporting
- Providing superior time-to-value
- Enabling delivery of managed SIEM services to RAM Infotechnology customers

"LogPoint enables us to document compliance with a wide variety of standards and boost security as well. The SIEM solution enables us to provide our customers with better services and support. We are already delivering LogPoint-based services to two customers and are planning on expanding the installation. LogPoint is now a part of our service offering and is generating revenue"

Frank Waarsenburg, CISO, RAM Infotechnology

Why the healthcare sector chooses LogPoint

1. Healthcare cybersecurity professionals prefer LogPoint's intuitive analytics and advanced threat hunting capabilities

LogPoint's unique taxonomy harmonizes data from cloud applications, core infrastructure, security products, and proprietary applications, among other sources. By leveraging this taxonomy, analytics is consistent across all data sources and use cases, enabling analysts to focus on the output of behavioral analytics, machine learning, and correlations use cases. The taxonomy extends to the integration layer, allowing easy consumption of threat intelligence, adding business context to events and integration with the rest of the infrastructure.

2. A flexible security analytics platform to fit the Public sector digitalization strategy

LogPoint provides healthcare organizations with a SIEM solution that are delivered on-premises, in the public cloud or through a managed security service provider. By supporting more than 400 of the most critical security data sources, Universities can ingest data from virtually any source – from databases to cloud applications.

3. Unmatched time-to-value makes it resource efficient to implement and expand LogPoint

Our customers in the healthcare sector tell us that time-to-value is a huge factor for why they choose our solution. LogPoint gives you a full SIEM solution that provides valuable analytics within a matter of days. Adding UEBA capabilities to enhance the SIEM takes no more than 6 hours, which brings customers unmatched time-to-value.

4. Predictable and transparent total cost of ownership

LogPoint works with your infrastructure, and we believe that the licensing model should not be a limiting factor when planning how and which data sources you would like to ingest data from. Our node-based pricing for SIEM is straightforward, and unlike other SIEM vendors, it covers all servers and data ingested – giving you the control and predictability to know exactly what the total cost of ownership will be.

5. Large partner community enables maintenance-free security operations

LogPoint takes a 100 percent customer-centric approach. You can join an ecosystem of some of the best global integration and technology partners, as well as 700+ customers, including hundreds of public sector organizations across Europe and the US. We provide 24/7 service and enjoy a consistent 97 percent satisfactions among customers for our support.

About LogPoint

LogPoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value.

Our advanced modern SIEM, UEBA and Automation and Incident Response solutions, simple licensing model, and market-leading support organization empower our customers to build, manage and effectively transform their businesses.

We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations, and business decisions. Our offices are located throughout Europe and in North America.

Our passionate employees throughout the world are achieving outstanding results through consistent customer value-creation and process excellence. With more than 50 certified partners, we are committed to ensuring our deployments exceed expectations.

Contact Chess

If you have any questions or want to learn more about LogPoint please contact the Chess Team on **0344 770 6000** or email **marketing@ChessICT.co.uk**

131443 JM 11/19