LOGPOINT

SECURING THE DIGITAL TRANSFORMATION IN THE PUBLIC SECTOR

For public organizations operating at large scales, increasing efficiency is a constant requirement. Digital systems and applications are helping to meet that need, providing easier communication, accessibility, mobility, convenience and productivity for the administration and citizens. But with that connectivity comes the increased risk of data breaches.

Securing The Digital Transformation In The Public Sector

For public organizations operating at large scales, increasing efficiency is a constant requirement 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 citizens. But with that connectivity comes the increased risk of data breaches.

Public IT infrastructure are facing an unprecedented threat level, stemming from actors as diverse as nation-states, cybercriminals, hacktivists, trill-seekers and insiders.. Adding to the problem, many public organizations use off-the-shelf products that are connected to the Internet – exposing nations and organizations alike to cyber terrorism and criminality.

With software and operating system vulnerabilities becoming a cornerstone of modern cyber warfare, the public sector IT infrastructure is more vulnerable to unexpected attacks than ever before. Public cybersecurity relies on the right solution – now, more than ever.

Public institutions are facing a number of challenges, including:

- **Compliance requirements are increasingly difficult to meet (GDPR, ISO, NIS and NIS2 etc.)**
- **Increased complexity in the infrastructure makes it challenging to obtain centralized analysis across the organization**
- **Difficult to detect advanced persistent threats, data loss and insider threats**
- **Increased privacy requirements have to be met while maintaining smooth IT operations and secure data of citizens**
- **Rising data amounts means more expensive analysis- and cybersecurity operations**

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? SIEM. Logpoint's seamless, quick reporting on unusual behavior in the network easily adapts to compliance requirements specific to your agency or institution. By keeping an eye on everything going on in your network, Logpoint positions you to address a possible breach quickly, limiting potential damage.

With User Entity Behavior Analytics (UEBA) Logpoint provides extensive machine learning and anomaly detection capabilities for advanced threat detection.

Extensively Proven In The Public Sector

Logpoint has been providing its Converged SIEM platform to customers in the public sector for years. Hundreds of public authorities, institutions and organizations across the world rely on Logpoint for cybersecurity, compliance, IT operations and Business Analytics.

Public sector customer categories include:

- **Ministries and Government agencies**
- **Defense, Police, Intelligence and Security authorities Regions, Cities, County Councils and Municipalities**
- **Universities, Colleges and Research institutions**
- **Public Hospitals**
- **National Banks**

The Logpoint SIEM solution allows the public sector 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.

Our SIEM solution collects and aggregates log data generated throughout the network, 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.

Logpoint's Converged SIEM comes with one SOAR seat for free to reduce cybersecurity risk and automate the investigation, containment and removal of threats. SOAR tackles the alert fatigue suffered by SOC teams and help them increase their efficiency with out-of-the-box playbooks and guided decisions. In addition, the Converged SIEM platform includes a native endpoint agent called AgentX for precise detection and fast remediation of threats in endpoints. In combination with SIEM and SOAR, AgentX provides Logpoint's Converged SIEM with EDR (Endpoint Detection and Response) capabilities.

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 cyberattacks immediately by spotting unusual patterns of activity and eliminate false positives.

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 everincreasing number of alerts.

In a nutshell, SIEM allows public sector 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 network – creating value from the sum of data which is worth much more than the individual pieces.

A single alert from an antivirus filter may not be a cause of alarm on its own, but if it correlates with other anomalies, e.g. from the firewall or data export at the same time, this could signify that a breach is happening.

As public organizations deal with very sensitive data, not only have to be extra careful but they often are the target of many cyberattacks too. With User Entity Behavior Analytics (UEBA) Logpoint provides extensive machine learning and anomaly detection capabilities for advanced threat detection, whether they are consequence of an external actor or come from within the organization.

Public Sector Use Cases

GDPR Compliance And Security Convergence

Personal data held by public sector organizations often includes Personally Identifiable Information (PII): medical conditions, tax documents, doctor appointments and other sensitive information. Within the majority of these organizations, we've seen the efficient handling and access to this information as a key factor in the public drive towards digital transformation.

In the future, the amount of digitized data is only set to increase and in 2018 the European Union implemented the General Data Protection Regulation (GDPR) to protect PII from unlawful processing and loss or destruction.

With Logpoint you can:

- Detect and report illegal access of personal data (GDPR Article 24, 32)
- Provide pseudonymization and encryption of personal data (GDPR Article 32)
- Provide tools for detecting proper processing of personal data (GDPR Article 24.32, NIS2)
- Provide tools for detecting and reporting incidents (GDPR Article 33, NIS2)
- Detect illegal transfer of personal data within a reasonable time (GDPR Chapter V)

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 prior to 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

Public Sector Use Cases (Continued)

Cyber Espionage

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 such as SAP and Oracle, often storing key information subject to sabotage and espionage.

With Logpoint, you can:

- Protect essential business 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 such as state-affiliated actors or possible espionage
- 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

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, mis delivery 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 personal 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

Healthcare Cybersecurity Use Cases

Automating Compliance Reporting While Saving 50% On SIEM

Durham County Council (United Kingdom) is a local government organization that employs 18.000 people and represents a population of more than 500.000. The capital funding for SIEM is primarily justified by the council's extensive compliance burden, and as a local authority that holds public data and collects revenue, the Durham County Council is subject to multiple compliance and accreditation requirements, including PSN, NHS IG Toolkit, HSCIC, PCI-DSS and BACS.

The benefits of the Logpoint solution includes:

- Compliance reporting automated, providing the info needed rapidly and comprehensively
- Much more cost effective than the last SIEM
- Data loss issue resolved
- Greater variety of systems integrated, giving more extensive reporting context
- Extended to a far greater number of users in the ICT team, creating time efficiencies and freeing team members up

"The outstanding offering – in terms of features, look and price – was Logpoint"

Paul Woods,
Information Security Officer, Durham County Council

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 to the legal requirements of effective log auditing"

Joakim Bengtzon,
IT Security Manager, Region Värmland

Healthcare Cybersecurity Use Cases

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 the 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

Strengthening Security And Eliminating False Positives

For the University of Bedfordshire (United Kingdom), protecting IT infrastructure is a round-the-clock responsibility. With campuses in Luton, Bedford, Milton Keynes and Aylesbury, the university welcomes more than 14,000 students each year from over 120 countries. It serves international learning communities via education partners in China, the Middle East, Europe and South East Asia. Logpoint helps the University Systems Infrastructure department to convert data into actionable intelligence, greatly improving the cyber security posture. This is done by:

- Simplifying management of network alerts
- Improving ability to identify incidents requiring actions
- Ingesting logs from its numerous IT Systems and then correlating to find indicators or compromise/attack or patterns of threatening behaviour
- Significantly reduced workload associating with correlating security logs

" The operational cost savings we've seen have been impressive, and the support we've received from Logpoint before, during and after implementation have really been fantastic. We're now upgrading to the latest version of Logpoint and looking to leverage it's analytic as to assess other areas such as asset utilization and more detailed profiling of the devices, applications and operating systems users bring to the network"

Chris Newby,
Systems Infrastructure Manager, University of Bedfordshire

Why the Public sector choose Logpoint

1. Public Sector 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 are 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 an end-to-end security operations platform delivered on-premises, as SaaS, in a private cloud or through a managed security service provider (MSSP). 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 public sector tell us, that time-to-value is a huge factor for why they choose our solution. Logpoint gives you a full security operations platform that includes SIEM, SOAR, UEBA, EDR capabilities and business-critical applications security monitoring. You can have it up and running providing your security team 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.

Our customers tell us that time-to-value is a huge factor for why they choose our solution

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information, visit logpoint.com

LOGPOINT