LOGPOINT

IT SERVICES

STRATA

HOW LOGPOINT IS HELPING STRATA INCREASE
SECURITY AND IMPROVE OPERATIONAL EFFICIENCY

STRATA

FACTS	
Customer	Strata Service Solutions Ltd.
Industry	IT Services for local authorities
Location	Exeter, UK
Objectives	Increasing Security and improving Operational efficiency

LOGPOINT

- Provides increased Security
- Improves operational efficiency
- Comes at a Predictable cost

Strata Service Solutions Ltd. are delivering transformational IT services to three local authorities in the South West of England. A key tool in enabling this transformational change is the Logpoint SIEM solution, which allows Strata to increase Security and improve operational efficiency across East Devon District Council, Exeter City Council, and Teignbridge district Council.

BACKGROUND

Strata Service Solutions Ltd., based across three sites in the South West of England, is a unique organisation. It focuses on delivering transformational IT Services into three local authorities, East Devon District Council, Exeter City Council, and Teignbridge District Council, while aiming to reduce costs, reduce risk and deliver the capability to support change. Strata started its life in 2014 and had been a huge success story. Strata operate with the commercial acumen of a business but without the profit incentive.

Strata is embedded in the three councils and enjoys close working relationships in all making it easier to deliver exemplary services to the citizens throughout the associated districts. This collaboration also facilitates flexible working among the council's staff and improves their individual interactions with technology, this makes for a more progressive and innovative working environment.

Strata support approximately 1,800 end user council officers and 300,000 citizens across the three councils.

THE CHALLENGE

Once Strata had been established in 2014, the task started on consolidating three IT environments and teams into one. The decision was taken to adopt a VDI environment to enable users to access their work from any building or terminal within the three councils and at any time. The challenge for this is managing an environment that is both complex and susceptible to change.

Due to the nature of this complex environment, Strata identified that they needed a log management system to identify events happening across the systems and network, in order to learn from new incidents and then put proactive monitoring in place to identify reoccurrences in advance, offering end to end Continual Service Improvement.

"As an IT Director, the thing that helps me sleep at night is knowing that when the users of the three councils come into work in the morning, they have access to the systems they need to support the 300,000 citizens resident within the area. We have 1,800 users across the three authority sites, and we have calculated that for each hour users are unable to access the systems and service their citizens, the cost of lost productivity if £30,000. Hence, Strata Service Solutions Ltd. need to be aware 24 hours a day and 7 days a week of any risks to our networks that can impact our users and our citizens," says Laurence Whitlock, IT Director at Strata.

Strata decided that the best way of managing these risks in a complex environment was to bring onboard a SIEM system to track all the activity that was going on across all different systems. Not only did Strata want this solution to manage logs from a security perspective, but also to provide proactive operational management, delivering information to other areas of the business such as infrastructure and support that could impact the business systems and systems availability.

THE SOLUTION

Strata started looking for a SIEM solution in November 2014 and due to their specific requirements, dismissed many SIEM vendors straight away.

"We needed a SIEM solution that could cope with a huge amount of logs; VMWare alone produces thousands of logs per minute. As we also wanted to use the SIEM tool for operational purposes, we needed to bring in a wide range of other sources, substantially increasing the amount of data that was going through the solution. Most of the solutions that we initially looked at were licensed by the amount of data consumed. As we were potentially looking at either reducing the number of sources we were tracking or having a very expensive solution, neither option was viable," says Robin Barlow, Head of Security and Compliance at Strata.

On further investigation, Strata came across Logpoint and were immediately impressed with the licensing model, which is priced by nodes rather than data input. This enabled Robin Barlow and his team to decide on the number of nodes that they had and then predictably budget for what they needed.

For an organisation whose key principle was saving money for the local authorities this model both made Logpoint cost- effective and also fixed the costs of the logging system regardless of any peaks of log traffic.

Another Logpoint key differentiator for Strata was the ability of the solution to react to changes and upgrades, particularly with VMWare, who are constantly changing the types of logs that they produce. Logpoint could keep up with that as they provide new log "normalization" as part of the contract but also importantly allow the customer to undertake this activity if they wish.

CONTACT LOGPOINT

If you have any questions or want to learn more about Logpoint and our modern SIEM solution visit www.logpoint.com

"Strata can produce up to 4,500 logs per second, and we usually store these for between 6 months to a year. With this huge amount of data coming from such a variety of sources, including our VDI environment, we needed to easily take the logs and get them configured so they can be easily managed. [...]Logpoint has certainly met my expectations."

Robin Barlow
Head of Security and Compliance

THE RESULTS

"Strata can produce up to 4,500 logs per second, and we usually store these for between 6 months to a year. With this huge amount of data coming from such a variety of sources, including our VDI environment, we needed to easily take the logs and get them configured so they can be easily managed. This process is known as normalization, and through this, we can produce an equal amount of reports and alerts from both a security and operational side. Logpoint has certainly met my expectations," says Robin Barlow.

One example of where this has been used from an operational perspective in Strata is when Logpoint can alert when there have been issues within VDI environment. Logpoint is then able to pre-warn the Strata Service Desk that they will be receiving a significantly higher number of calls from end-users.

After successfully using Logpoint for the past few years, Strata are now working with the Logpoint team to take Logpoint to the next stage, looking at the new UEBA module to see how Machine Learning can help Strata be alerted to the "unknown unknowns" and continue to support the business both operationally and securely.

"Over the last 3 1/2 years, our use of Logpoint has grown considerably. We do not see it as a point product, but a solution that has grown with our business. And the fact that it is not only deployed for security makes it all the more valuable. Over the last few years, we have cut the number of IT suppliers from 400 to 190, so we are heavily invested with the organisations we have chosen to partner with. Logpoint is with us for the long run", says Laurence Whitlock.

"Over the last 3 1/2 years, our use of Logpoint has grown considerably. We do not see it as a point product, but a solution that has grown with our business. And the fact that it is not only deployed for security makes it all the more valuable."

Laurence Whitlock
IT Director