

Experian

HP Enterprise Security Customer Case Study

“ArcSight ESM brings intelligence to log management, allowing us to do much more than we imagined – and with a much smaller team than we anticipated.”

—Tom Jacobsen, Director, Global Security Operations Center,
Experian



Customer Brief

Experian is the leading global information services company, providing data and analytical tools to clients in more than 65 countries. The company is a constituent of the FTSE 100 index, with annual revenues reaching \$3.9 billion. Experian employs approximately 15,000 people in 40 countries and has its corporate headquarters in Dublin, Ireland. Operational headquarters are located in Nottingham, UK; Costa Mesa, California; and São Paulo, Brazil.

Product(s)

- ArcSight ESM
- ArcSight PCI Protection Suite

Business Benefits

- ArcSight ESM gives Experian the ability to identify external threats and detect suspicious events before they can cause damage
- Experian can now optimize its security process while increasing operational efficiencies and cost savings
- ArcSight ESM has shifted the security paradigm for Experian, allowing it to conduct behavior and pattern analysis across all its systems



The Experian Challenge

As a trusted information provider, Experian is fully committed to ensuring the integrity and safety of its data. Four years ago, the company realized it needed an enterprise security management system that would allow it to monitor threats and vulnerabilities in an automated fashion.

“We needed a more efficient method for monitoring event logs from our disparate systems,” says Tom Jacobsen, Director of the Global Security Operations Center at Experian.

The problem, he explains, was that systems administrators – such as the Unix administrator or the Microsoft Windows administrator – were responsible for managing and monitoring their individual logs for security events, even though this was not their primary role.

“Trying to add security to their job functions was simply not effective,” says Jacobsen. “It was unfair to ask network or engineering staff to be responsible for vulnerability management or intrusion detection on top of everything else.”

HP Enterprise Security Customer Case Study:

Experian is committed to ensuring the integrity and safety of its data. The company sought a solution that would allow it to monitor threats and vulnerabilities.

Industry: Financial Services



Experian understood that those critical security functions had to be integrated and managed in a central location. The company required a system that could automatically pull log information from its various systems and allow Jacobsen and his security team to monitor and analyze the data within a single view. That's when it discovered ArcSight ESM.

The ArcSight Solution

Experian looked at several enterprise security management vendors, but it was clear that ArcSight ESM was one of the most sophisticated solutions on the market. "ArcSight ESM isn't just some simple logging mechanism," says Jacobsen. "It actually brings intelligence to log management, allowing us to do much more than we imagined – and with a much smaller team than we anticipated."

In particular, Jacobsen and his team were excited by the ability of ArcSight ESM to intelligently analyze log data. Typical log management solutions are primarily focused on historical analysis. ArcSight ESM, however, features robust capabilities that can proactively detect a vast range of threats and compliance violations, and respond to them in a timely manner.

"In the past, we looked at things in a static mode. You almost had to know what was going to happen in advance," says Jacobsen. "But ArcSight ESM allows us to take our security to a whole new level. We now have the ability to do behavior and pattern analysis across all our systems, a practice which has fundamentally shifted the paradigm of how we approach security."

What's more, Experian receives billions of log events each month from thousands of systems. ArcSight FlexConnector technology enables Experian to efficiently collect logs from a multitude of different devices and then convert the data to a common format, which enables reporting and analysis across the entire organization.

Experian must also comply with a number of regulations, including the payment card industry (PCI) data security standard. The company implemented the ArcSight PCI Protection Suite, additional functionality available with ArcSight ESM that proactively protects against data breaches, insider threats and non-compliance risks across all 12 PCI requirements.

"We had a very aggressive timeframe for rolling out our PCI compliance," says Jacobsen. "The training provided by ArcSight professional services was customized to our needs and the entire process went very smoothly and easily. We had it operational within 30 days."

The ArcSight Impact

With the ArcSight platform, Experian has greatly enhanced its capacity to mitigate external threats and detect suspicious events before they can cause damage. "ArcSight ESM has given us an approach that we never had before, for actually finding sophisticated threats like zero-day attacks," says Jacobsen. "This increased protection gives us a greater peace of mind."

ArcSight ESM correlates all incoming events across the entire Experian network, enabling the organization to intelligently identify, prioritize and respond to security threats. That Experian can better judge the severity of an event and immediately know what level of response is required is a great relief to security personnel, who deal with a multitude of events each month and need to prioritize and act accordingly.

In terms of cost savings, Jacobsen estimates that the company has saved thousands of dollars by centralizing the log management function. "It would be very expensive if we had to send each of our systems administrators out to training conferences to learn how to monitor logs and read signatures for their individual systems," says Jacobsen. "Now I can bring an ArcSight specialist in-house and train 12 people for a fraction of the cost."

Jacobsen also relies on the annual ArcSight Protect Conference to gain up-to-date information, training and best practices, as well as network with peers and ArcSight employees. He and his team look forward to attending each year, and have been presenters themselves. "The brain trust that goes into ArcSight Protect is just fantastic," he says. "This year, at the end of the first day we sat down to review the content we felt was valuable, and it took over two hours."

Going forward, Jacobsen sees ArcSight ESM as being used not just for security; the company is already starting to leverage the solution for business and operational intelligence as well. For instance, with new insight into network traffic flows, when pattern anomalies surface they have a good idea something is happening operationally that needs to be investigated.

"ArcSight ESM is essential to our organization," says Jacobsen. "It's an integral part of what we do every day. I couldn't imagine doing my job without it."

