KCOM ENSURES GDPR COMPLIANCE AND STRENGTHENS ITS SECURITY POSTURE WITH ABSOLUTE

KCOM

kcom.com

"The safety of our information is very important, especially from a GDPR perspective. With Absolute, we are sure that our data is safe at all times. The key thing that Absolute gives us is the confidence to know and prove that no data was lost. We can confidently say that no sensitive information is compromised or accessed, and all records and data on any PC are completely safe, no matter what."

Steve Williams
Manager, IT Operations
KCOM

INDUSTRY:

COMMUNICATIONS

PLATFORM:

⬤ CUSTOMER SUCCESS STORY

KCOM provides a wide range of IT and communications services to enterprises and public-sector organizations and is listed on the London Stock Exchange. With 2,000 employees working across nine different locations, securing and keeping track of laptops and desktops and protecting the sensitive information they contain is difficult at best. At worst, it becomes a drain on company resources and a big data security risk.

BACKGROUND
KCOM's IT Operations team recently made the decision to refresh the company's IT estate, which included leasing 2,000 new machines, and they are looking to significantly raise the bar of their security profile across the entire group. They intend to protect endpoints more aggressively against malware, make sure VPN is always on, see the big picture by integrating information from different tools, and ultimately respond to threats effectively and efficiently.

THE CHALLENGE
A high percentage of KCOM employees work remotely, which used to weaken their security posture. For example, when an endpoint was infected with a virus and a VPN connection was not active at the time, Steve's team was not able to manage that device remotely. Someone had to physically drive to the location of the device. Because they are a small desktop team, such a limitation caused a significant waste of time and undermined KCOM's ability to respond to threats in a timely manner.

Protecting information is another major cause for concern, especially with the GDPR regulation already being enforced. Whether it is company or customer personal data, regulated personally identifiable information (PII) could easily be present on any of KCOM's endpoints due to the nature of the business. The IT Operations team needs to be able to prove that any regulated data residing on their devices was never compromised if an incident occurred.

THE SOLUTION
With Absolute's Application Persistence, powered by patented and embedded technology, Steve's team now has the ability to make their VPN agent resilient on all their endpoints. Consequently, they remain in a position to remotely manage any endpoint and fix it if it has an issue. "Everyone sees the benefit; this is a really good place to be," Williams said.

In order to increase overall efficiency and productivity by adding more automation to its processes, KCOM is currently looking to have more mission-critical applications deployed and self-healed on its machines through Application Persistence.

---

absolute.com

/ABSOLUTE®
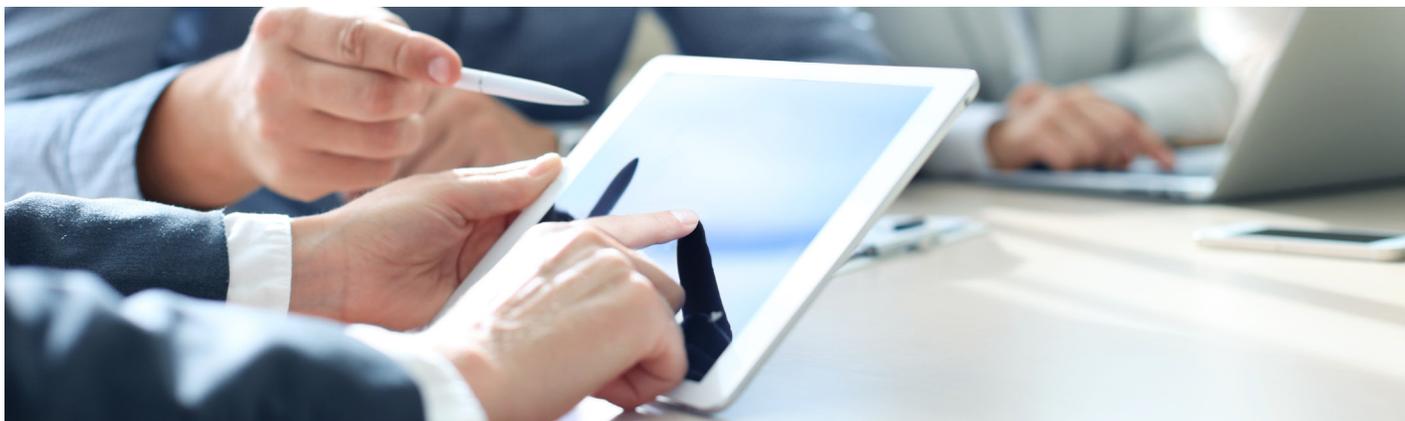
When it comes to responding to incidents, KCOM has a security event triggered automatically every time an endpoint is stolen, lost or misplaced. "If we can't see it, there's a risk to it," Williams said. "The first step is remotely locking a device by using Absolute so nobody can get access to it."

Steve's team is now also confident that KCOM's data is secure at all times. "The safety of our information is very important, especially from a GDPR perspective. With Absolute, we can confidently say that no sensitive information is compromised or accessed, and all records and data on any PC are completely safe, no matter what," he explained.

According to Williams, Absolute provides the full and deep visibility that the IT Operations team needs to prove compliance. "The key thing that Absolute gives us is the confidence to know and prove that no data was lost, even if a device is in unauthorized hands," Williams said. "We are able to tell the complete story of what has happened to the machine, guarantee that encryption was always on throughout the entire process and, later, confirm that the disk has been securely and remotely wiped, so there is absolutely no way anyone could have access to it."

RESULTS

STRENGTHENED SECURITY POSTURE
Automatic self-healing of failing endpoint security applications, on or off the network

INCREASED OPERATIONAL EFFICIENCY
Ability to see, control and secure all endpoints remotely, no matter what happens

PEACE OF MIND AND PROOF OF COMPLIANCE
Total confidence that any sensitive data is safe at all times and the ability to prove GDPR compliance

For more information about Absolute solutions please visit: **absolute.com**

/ABSOLUTE®