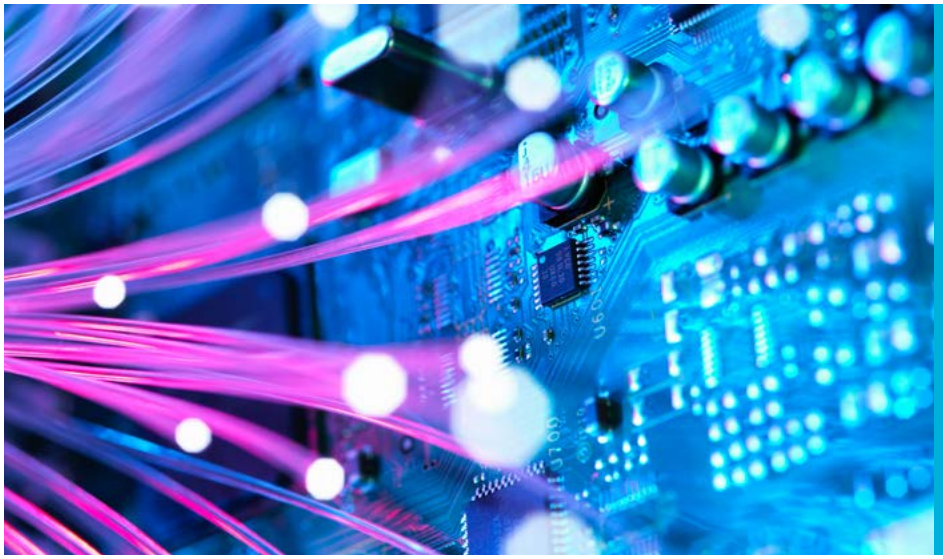

Business challenge

One of the UK's leading broadband providers, TalkTalk needed to continue evolving its security capabilities—including its responsiveness to cyber threats—along with its expanding business.

Transformation

After years of expansion, TalkTalk needed to continue maturing its security operations to keep pace with its growing business. Integrating the IBM Resilient Incident Response Platform® (IRP) with its legacy security systems and applications, the company responds to and contains potential issues more quickly than ever before.

Colin Hardy
Head of Intrusions and Investigations
TalkTalk

Results

Faster resolution
with an eightfold reduction in average containment time

Quicker adjustments
to address changing threats and attacks

Greater visibility
for transparent reporting and communication

TalkTalk

Resolves issues eight times faster with an IBM Resilient solution

Headquartered in London, England, TalkTalk provides broadband, landline, TV and mobile services to more than four million customers in the UK. Initially formed as a telephony reseller in 1995, the company launched TalkTalk as a consumer brand in 2003. Throughout its history, TalkTalk has focused on offering high-value, low-cost connectivity to its customer base.

"Having Resilient at the heart of our security operations is a complete game changer for us."

—Colin Hardy, Head of Intrusions and Investigations, TalkTalk

Share this

Expansion demanding highly tuned security

Launched over two decades ago as a telecommunications service provider, TalkTalk remains true to its founding mission: making connectivity accessible and affordable for people throughout the UK. "We describe ourselves as a value operator," says Colin Hardy, Head of Intrusions and Investigations. "We deliver broadband services at highly competitive rates to more than four million customers."

After years of steady growth that included multiple acquisitions, TalkTalk needed to ensure that its security capabilities continued evolving along with its business. The company decided to bring previously outsourced tasks in house, initiating a long-term plan for maturing its security operations.

TalkTalk's strategy focused on developing three critical security competencies: people, processes and technology. With a newly expanded security team in place, the organization quickly identified the need to bolster its legacy IT with a powerful incident response platform.

"Since we're a business that has been built up through acquisitions, we've got many different kinds of network environments and legacy equipment," says Hardy. "We wanted to be able to use all of the security tooling we've invested in by stitching it together, getting richer data out of it and really honing our response capabilities."

Game-changing incident response capabilities

Experimenting with legacy tools to track and mitigate potential cyber threats led TalkTalk to evaluate more scalable incident response solutions. The broadband provider ultimately chose the Resilient IRP based on the offering's flexibility, vast feature set and ease of deployment.

"The decision to go with IBM was geared around the tool's ability to support our maturity journey," says Hardy. "We needed a product that could develop as we knew we were going to develop over the coming years and we really saw that in the Resilient offering. Also, since it's cloud-based, it was easy to implement in our environment and saved us money in having to stand up resources."

Working closely with an IBM Resilient team, TalkTalk integrated Resilient IRP with its legacy security applications—including its endpoint response and intelligence sharing platforms—and fully incorporated the new technology into its processes.

"Our security analysts know what to do and which workflows to follow in different situations," says Hardy. "Having Resilient at the heart of our security operations establishes an auditable record of what occurs during an incident that we've never had before. It's a complete game changer for us."

An eightfold reduction in containment time

Instead of tracking potential security threats across disparate environments, TalkTalk's analysts now have a centralized hub for viewing notifications. "When an alert comes in, our analysts don't want to investigate ten different systems to work out whether it's a threatening incident or not," says Hardy. "They want the context of that alert to be delivered to them all within a single pane of glass, which is what Resilient provides."

By integrating TalkTalk's security platforms and streamlining its workflows, the Resilient solution speeds issue resolution significantly for the company—TalkTalk's security team now contains potential threats eight times faster on average.

With the Resilient IRP serving as the cornerstone of its security infrastructure, TalkTalk also adjusts more rapidly and agilely to address evolving threats. "Part of the beauty of Resilient is that you can configure it so well," says Hardy. "As the bad guys change and develop new attacks, we can very quickly shift to implement new responses. Resilient allows us to move with the threat landscape."

Finally, the Resilient solution introduces a new level of transparency into TalkTalk's security operations. "The visibility of an incident and how we communicate to our stakeholders is absolutely critical," says Hardy. "One of our great measures of success is being able to tell our Board of Directors that this tool has enabled us to not only see incidents in one place but actually report on how much faster we're responding to them."

Solution component

- IBM Resilient Incident Response Platform®

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

Please Recycle

29025129-USEN-00