Brought to you by Informa Tech

OMDIA

Publication date:
17 Nov 2021

Author:
Adam Etherington, Principal Analyst, Digital Enterprise Services

Service Provider Spotlight: BT Signals Global Security Ambitions with Eagle-i

Omdia view

Summary

BT's ambition is to become the "world's most trusted connector of people, devices, and machines."

To realize this vision, BT has reinvigorated plans to extend cybersecurity growth globally. At a recent industry analyst event, the global telco officially launched a proactive, integrated cybersecurity platform called Eagle-i and accompanying managed services.

The launch of BT's managed firewall and endpoint services complement existing security advisory services. But more importantly, the Eagle-i platform that underpins them leverages BT's unique visibility of customers' networks alongside threat detection, behavioral analytics, and the recent SAFE investment to bolster proactive defense capabilities and future on-ramp releases.

The launch timing is spot on because it coincides with Cybersecurity Awareness Month, the potential of global markets returning to economic growth, and rising advanced cyber threats in addition to the heightened risks these threats pose to multinational corporations (MNCs) and governments as digital roadmaps accelerate.

BT executives updated industry analysts over two days in October. They shared BT's progress, roadmap, and growth strategy for 2021–22. This report shares insights from this event to raise awareness and consideration of BT's capabilities in security among executive decision makers.

The changing role of a chief information security officer (CISO)

What are MNCs' and government CIOs' biggest challenges and priorities right now? What do these mean for CISOs? To set the scene for BT updates, the CEO of BT Global highlighted insights to these pivotal questions from BT's Global Advisory Board (GAB). GAB is a collective of approximately 20 prominent CIOs that meet twice yearly to share and co-innovate around security challenges, opportunities, and best practices.

The CISO role: From technology to business focused, trading a currency of trust

Not surprisingly—but reassuringly—CISOs are tasked with quantifying the risks and benefits of technology to material business outcomes, what BT calls a "business CISO" rather than a technical one. The designative difference is subtle but important. Trust is the modern currency because CIOs seek to protect their organizations and the service providers that support them.

A BT-commissioned white paper noted that 76% of global organizations feel confident about their organizational security position, yet 84% have been breached. This is a serious statistic elevating the importance of network performance, combined with cybersecurity, in underpinning the delivery of business results. This trend means BT needs to engage in a different conversation with large enterprises. For example, how can security improve an organization's marketing penetration, lead generation, and supply chain resilience; increase operational efficiency; and reduce costs?

CIO trends: Accelerating multicloud, cloud native, and rising consumption model acceptance

COVID-19's disruption of business operations forced organizations to accelerate their adoption of multicloud because remote working dominated, market demand levels fluctuated, and business continuity was paramount.

As a result, the use of multiple concurrent clouds—facilitated by "as a service model" maturity—and zero-trust security strategies have accelerated. Cloud-native application development has also sped up through leveraging APIs and broader device connectivity to generate greater value from cloud investments. However, this shift has also raised security concerns. Historically, cloud has not been a massive focus area for BT. Thus, winning security will require the telco to embed itself into cloud-led conversations.

CIO priorities: Realizing business outcomes from technology, mitigating cyber threats, managing network performance, and transitioning to hybrid

There will no doubt be case studies written in times to come of firms that failed or flourished during the recent pandemic. In BT's experience and that of the GAB CIO community, organizations that embraced digital business models were the ones to survive and thrive.

However, CIOs are also increasingly concerned about cybersecurity, now a featured agenda item in most organizations' board discussions. The performance, visibility, and security of core networks that underpin multicloud and hybrid working, for instance, increases the attack surface and highlights a growing need to proactively address security—before an attack turns into a severe incident.

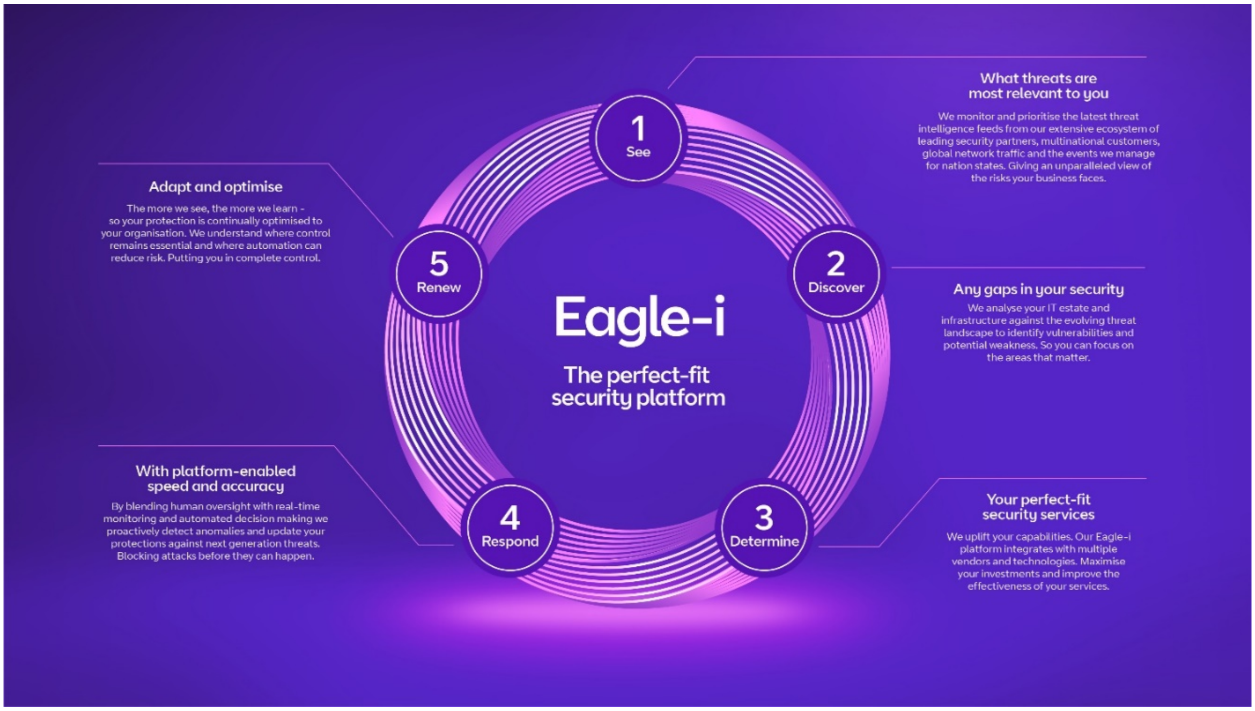
Building a perceptive cybersecurity defense platform with "Eagle-i"

Launching Eagle-i, "the perfect fit security platform"

Against this backdrop—and to meet the changing role of IT security executives head on—BT has officially launched "Eagle-i," an open-architecture, cybersecurity platform that reportedly combines BT's consolidated technology partners (e.g., CrowdStrike) and leverages proprietary artificial intelligence (AI), automation, and orchestration capabilities. It also makes use of BT's extensive breadth and depth of telemetry data and experience as a telco managing massive MNCs and government networks globally.

As a scalable platform, Eagle-i reportedly leverages BT's network management expertise. Building Eagle-i was pivotal to BT delivering its next generation of enhanced managed security services.

1. Figure 1: BT's Eagle-i platform capabilities



What threats are most relevant to you

We monitor and prioritise the latest threat intelligence feeds from our extensive ecosystem of leading security partners, multinational customers, global network traffic and the events we manage for nation states. Giving an unparalleled view of the risks your business faces.

Any gaps in your security

We analyse your IT estate and infrastructure against the evolving threat landscape to identify vulnerabilities and potential weakness. So you can focus on the areas that matter.

Your perfect-fit security services

We uplift your capabilities. Our Eagle-i platform integrates with multiple vendors and technologies. Maximise your investments and improve the effectiveness of your services.

With platform-enabled speed and accuracy

By blending human oversight with real-time monitoring and automated decision making we proactively detect anomalies and update your protections against next generation threats. Blocking attacks before they can happen.

Adapt and optimise

The more we see, the more we learn - so your protection is continually optimised to your organisation. We understand where control remains essential and where automation can reduce risk. Putting you in complete control.

Source: BT

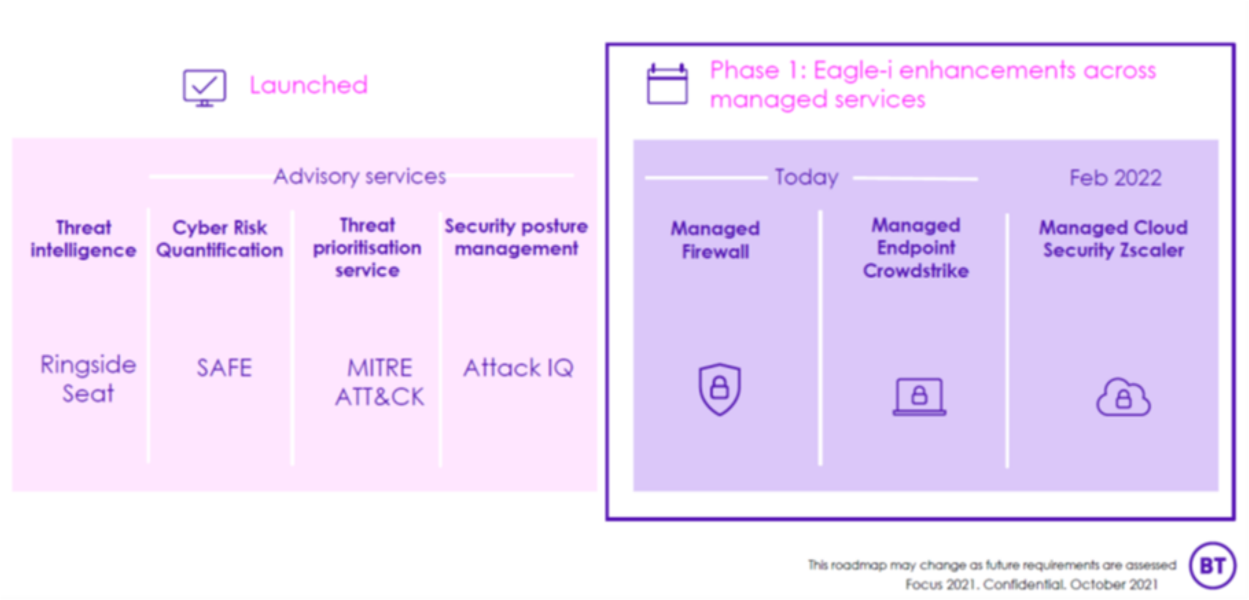
Roadmap Phase 1: Managed firewall, managed endpoint (CrowdStrike) security, and cloud security (Zscaler)

Within the roadmap of Eagle-i developments, the first tranche, which is in Phase 1, was announced for release in October. It consists of two managed services: managed firewall security and managed endpoint security (leveraging CrowdStrike).

The second tranche is also in Phase 1 and will be made available in February 2022. It will launch managed cloud security (incorporating Zscaler), leveraging the same Eagle-i smarts.

These managed services extend advisory services that are currently available through over 300 security professionals globally. These consulting services include threat intelligence (ringside seat), cyber risk quantification (SAFE), threat prioritization, and security posture management services already available.

2. Figure 2: BT's Phase 1 security roadmap



Launched

Advisory services

Threat intelligence — Ringside Seat

Cyber Risk Quantification — SAFE

Threat prioritisation service — MITRE ATT&CK

Security posture management — Attack IQ

Phase 1: Eagle-i enhancements across managed services

Today

Managed Firewall

Managed Endpoint Crowdstrike

Feb 2022

Managed Cloud Security Zscaler

This roadmap may change as future requirements are assessed

Focus 2021. Confidential. October 2021

BT

Notes: *This roadmap shows BT's current intentions to implement the listed products and services. BT reserves the right to change the implementation dates and the products and services shown.*

Source: BT

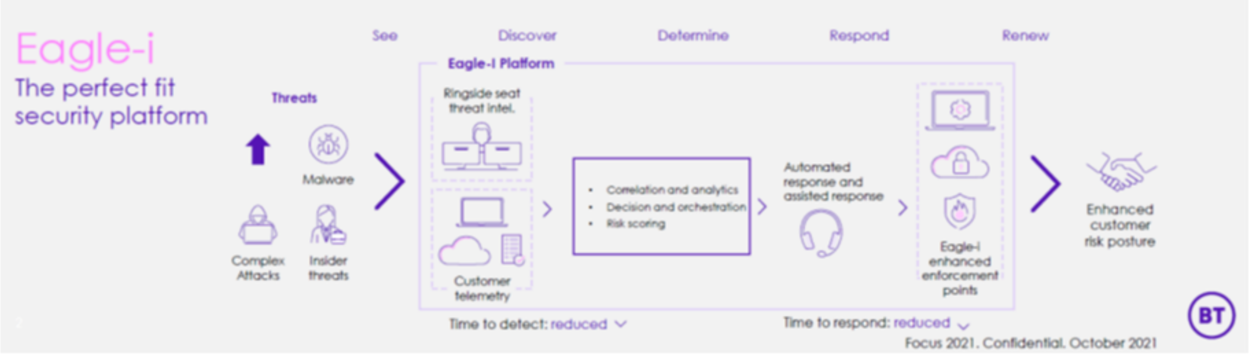
What is ahead: Phase 2 and 3 of BT's Eagle-i roadmap

Future phases of BT security solutions in development include multi-control orchestration, hybrid cloud management, SD-WAN, and firewall policy orchestration. These productizations are designed to overcome the historically siloed nature of cybersecurity solutions present in many MNCs. If done well, the platform offers BT a chance to broaden its cyber portfolio coverage into cross-portfolio remediation and automated posture management, especially as cybersecurity solutions become more interdependent, integrated, and embedded in digital change across industries.

How is Eagle-i any different from other cyber platforms?

While predictive threat intelligence capabilities to support managed security are not new to the market, Eagle-i relies on recent investments in SAFE and significant internal investments in BT's internal operations (automation and security). It also leverages BT's deep network expertise to present an integrated customer proposition. Eagle-i analytics engines can analyze the additional telemetry that BT's network expertise generates to better predict, respond, and learn from advanced threats. Speed is critical for responding to any threats, and BT's visibility across the network, endpoints, and cloud enables security of data in motion.

3. Figure 3: BT’s Eagle-i platform blends automation with human expertise



Eagle-i
The perfect fit security platform

See
Discover
Determine
Respond
Renew

Threats
Malware
Complex Attacks
Insider threats

Eagle-I Platform
Ringside seat threat intel.
Customer telemetry

- Correlation and analytics
- Decision and orchestration
- Risk scoring

Automated response and assisted response

Eagle-i enhanced enforcement points

Enhanced customer risk posture

Time to detect: reduced
Time to respond: reduced

Focus 2021. Confidential. October 2021

Notes: *This roadmap shows BT’s current intentions to implement the listed products and services. BT reserves the right to change the implementation dates and the products and services shown.*

Source: BT

Fortunately, the platform is not a “rip and replace” solution and is positioned as an accelerator for organizations exiting security investments and capabilities.

In essence, Eagle-i unifies BT’s technology partners, internal operations expertise, and experience from managing customers’ networks to offer a proactive, AI-driven, scalable platform that is integrated with BT’s and internal SecOps analysts’ expertise.

From this solution, BT plans to leverage Bayesian AI across extensive customer cloud, network, and endpoint telemetry data to identify threats, quantify their impact, and remediate them more quickly.

Leveraging the SAFE approach to cybersecurity

A foundational component of Eagle-i is intelligence and reporting capabilities acquired through BT’s SAFE company investment. As Omdia reported in an article “BT makes Safe bet on security” back in July, BT made a significant investment in the Silicon Valley cyber risk management firm Safe Security, rapidly boosting the telco’s capabilities to the left of an attack. SAFE offers a methodology and platform that can quickly and accurately assess an organization’s vulnerability to cyberattacks, reported as a SAFE score.

Founded in 2012, Safe Security was formerly known as Lucideus. The company helps organizations measure and mitigate enterprise-wide cyber risk using its security assessment framework for enterprises (SAFE) platform.

In practicality, risk posture and threat tolerance are different for each organization, influenced by their level and integration of prior security investments, cyber maturity, and industry, among other factors. The advantages of the SAFE score are customer-specific assessment, quantification, and prioritization of critical cybersecurity areas to address.

The SAFE score’s ability to pinpoint risk areas and the potential costs could be invaluable in building future business cases for cybersecurity investments within an organization. This is mainly because budgets are tight, and security funding often competes with more lustrous investments in cloud, 5G, and AI/ML.

From BT’s perspective, the investment delivers exclusive rights to embed SAFE within its growing security services portfolio, which should serve as a solid on-ramp for advisory services and, eventually, managed security services for the telco.

The road ahead for BT

Combining these capabilities is an important move for BT, especially for BT customers. Combining the inorganic and organic investments that culminated in 34 product releases in 2020, thousands of cybersecurity awareness training hours invested in frontline staff will favorably uplift BT's integrated security services capabilities from consulting through to managed security. These meshed capabilities are essential to growing market share among large enterprises and governments globally.

BT's challenges from this point are manifold. The first is sustained efforts to bolster awareness and consideration in security to bring in new clients. The second is capturing security service opportunities attached to the cloud, networks, and digital transformation within target industries.

Challenge one: Awareness in security

Omdia will start by addressing the first challenge. BT itself highlighted in its briefing that its security capabilities are often a "hidden asset" in the eyes of its customers. Further, in recent Omdia surveys of global decision makers, BT scored comparatively well against best-in-class providers globally in contract flexibility and delivery models. The telco also has a claim to a solid reputation among clients for delivered services.

However, compared with market leaders in the hotly contested security space, overall awareness needs continued focus to achieve a sustained cut that translates to wallet share. BT's achievements with customer wins, a rising Net Promoter Score, and a solid relationship score among those surveyed will enable currency of trust growth.

Challenge two: Capturing managed security services from network, cloud, and digital transformations

The second challenge builds on the first. According to Omdia's report in May 2021, *Digital Enterprise Services Insights: Global Cybersecurity Market Landscape – 2021–22*, BT scored particularly well in two sub-criteria areas of importance to IT decision makers: the perceived capability of security digital platforms and contract terms. The telco has also secured sizable IT security services deals, provisioning threat intelligence, technology services, consulting, industry solutions, and managed services.

However, future growth potential requires capturing a larger share of new and recontracted deals where security underpins. In April 2021, we noted in our report *Cybersecurity IT Services Contracts Analysis: Global – 2021* that there were fewer standalone managed security services (MSS) deals in 2020. MSS are more often attached to the broader cloud, network transformation, and digital transformation deals.

Achieving this on a global scale requires demonstrable expertise in securing digital technologies within industries and regional contexts while addressing both shared- (often technical) and unique- (often sector or region) based cybersecurity ramifications. For instance, a growing number of regulations and compliance measures across a more elongated, interwoven, and complex third-party supply chain of technologies ups both the potential payoff and risks of technology within each industry.

A path to growth

BT has signaled global ambitions in security. The telco now has sizable core capabilities, experience, partners, roadmap, reference industry experience, and thought leadership. If these are combined well, they will offer compelling security solutions for both the mid-market and large enterprises and governments, which are anticipated to foster BT's growth in coming years.

Appendix

Further reading

Cybersecurity IT Services Contracts Analysis: Global – 2021 (April 2021)

"BT makes Safe bet on security" (July 2021)

Digital Enterprise Services Insights: Global Cybersecurity Market Landscape – 2021–22 (May 2021)

Digital Enterprise Services Insights: Global Cybersecurity Services (Cloud, Edge, MSSP) 2021–22 (August 2021)

Enterprise Services Total Addressable Market Forecast: 2020–26 (September 2021)

Omdia Universe: Selecting a Global IT Security Services Provider, 2021 (March 2021)

Author

Adam Etherington, Principal Analyst, Digital Enterprise Services

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com