How the Cognito platform secures and accelerates mergers and acquisitions

Real-time, automated threat detection and response finds attackers before damage is done

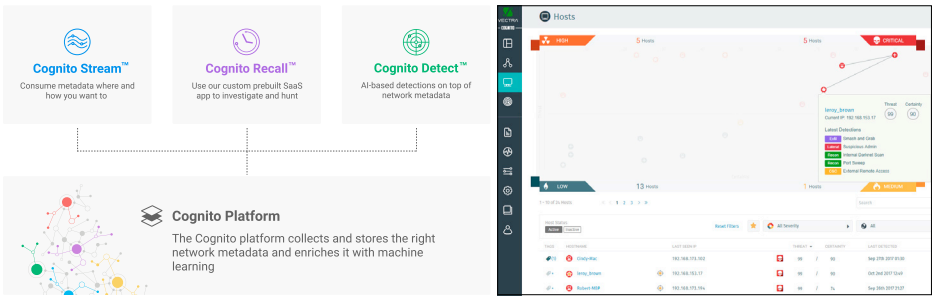
Acquiring a company is a massive undertaking and requires a significant amount of planning and flawless execution. Time is of the essence. The quicker an integration materializes, the faster the time to value.

However, in a survey by West Monroe Partners, 52% of executives discovered post-deal cyber problems. And 41% said post-merger integration is their main cyber concern. According to the study, cybersecurity is the primary reason a company walks away from a deal, and a common reason for regretting a deal.

It is now common for M&A agreements to include a clause that the target company might risk up to 30% devaluation if it falls victim to a cyberbreach during the 12-month period after an acquisition. These impacts significantly increase the stakes well beyond the cost of an actual data breach and the recovery process.

The Cognito® platform from Vectra® is instrumental in accelerating the M&A process using AI-driven network threat detection and response for cloud, data center and enterprise environments.

The Cognito platform speeds-up due diligence and integration by automating threat hunting and prioritizing detected threats based on certainty and risk. This enables faster response and mitigation of in-progress cyberattacks and highly conclusive incident investigations.



The Cognito platform automatically correlates threats with host devices under attack, presenting security operations teams with an intuitive view of the highest-risk threats. It also provides trail of forensic evidence to launch conclusive incident investigations.

There are several critical cybersecurity challenges to overcome and manage during an M&A:

- Merging two companies creates a broader attack surface. This expanded attack surface leaves the networks of the acquiring company and target organizations exposed and vulnerable.
- Inherited or imported threats. It is imperative to have 360-degree visibility into attacker behaviors that exist inside networks. Adding a new organization to your cloud, data center and enterprise networks can introduce hidden threats.
- The risk of insider threats is especially high during the M&A process. Potential threats from insiders can occur for various reasons, including job uncertainty.
- Third parties, such as business and technical consultants who are commonly employed during M&As, can knowingly or unknowingly become pawns in a cyberattack.
- The burden on understaffed IT and security teams during M&As increases the chances of misconfigurations that can unintentionally introduce vulnerabilities that sophisticated cyberattackers can exploit.

In the M&A process, the Cognito platform from Vectra can be leveraged by the target company to conduct a security assessment as well as by the acquiring company to assess risk and compliance of the target organization.

Whether it's an insider threat or an external threat, the Cognito platform automatically detects malicious behaviors in every phase of the attack lifecycle – command and control, internal reconnaissance, lateral movement, data exfiltration and botnet monetization.

This enables security operations teams to respond with unparalleled speed, accuracy and efficiency to detect and mitigate threats to head-off catastrophic data breaches.

Cognito automates manual threat-detection processes and consolidates thousands of security events and historical context in real time to surface compromised workloads and host devices that pose the biggest risk in the cloud and on-prem.

These capabilities are crucial to ensure that cyberthreats are not inherited by the acquiring company or the target company while eliminating attack surface vulnerabilities and accelerating network and data integration as a result of M&As.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai