Securing the Human Layer

Natural language understanding to assist humans in protecting enterprise data

Armorblox

Security Powered by Understanding

Securing the Human Layer: Natural language understanding to assist humans in protecting enterprise data

The last decade has seen a tremendous creative force that brought humans and machines closer, weaving connected-machines into the very fabric of a new global economic engine. At the heart of this engine is data that represents our businesses, our values, and even ourselves. In this new connected world, we have access to data that is spread across geographies, clouds and data centers.

While companies today reap the benefits of this connected world, reaching new heights of productivity and scale, their valuable data is continuously under siege. Most employees work and collaborate by exchanging emails, instant messages, documents, presentations, etc., and bad actors are targeting them in the enterprise.

As a result, employees have become the weak link in securing the enterprise. Sophisticated attacks exploit basic human nature with social engineering and phishing. From emails intended to deceive naive users[1] to plain-vanilla data-theft, attackers are getting through by targeting employees – and these attacks have cost businesses upwards of 12 billion dollars in less than 5 years[2].

Organizations are heavily invested in traditional solutions like URL filtering, DLP and anti-phishing solutions, but they are not effective in today's rapidly-evolving environment. The attacks mimic human interactions among other sophisticated tradecrafts and are increasingly harder to detect. Traditional security solutions are unable to intelligently process and reason about textual communications to protect employees as they communicate and share data.

We are at one of the most interesting inflection points in the evolution of deep learning that can be used to address the missing layer in security: the human layer

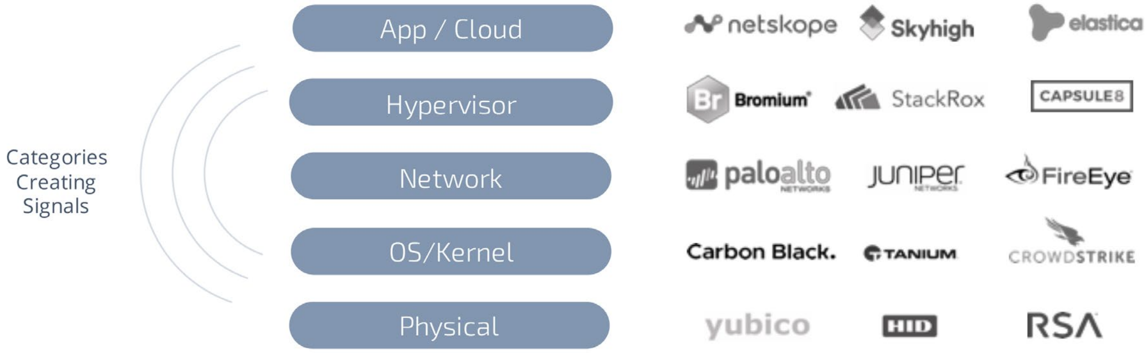
This paper describes how Deep Learning can help analyze textual communications and data to secure a new signal for enterprise security that addresses the top attack vector of global enterprises today.

[1] 94% of Cybersecurity attacks start as an email phishing campaign - Verizon Data Breach Report 2018

[2] FBI estimates $12B lost due Business Email Compromise - FBI Field Office

Today's Current Solutions Lack Understanding

In the past, security could be controlled by perimeters. But today, with data distributed across datacenters, clouds, and geographies, organizations are applying and inserting security solutions at various layers to protect their core resources. For example, you have cloud security solutions to give you visibility into what is in the cloud, or network security products to monitor and control network traffic.



The problem is that these solutions are fragmented and compartmentalized across multiple product categories that do not communicate with or learn from each other. Security professionals are constantly trying to consolidate their solutions for more control and clearer views of their security postures. But configuring and integrating these products often requires expensive and time-consuming professional services engagements.

After investing millions to create thousands of policies, organizations are terrified to make updates because it is impossible to understand the impact of any changes or risk losing important policies. As a result, policy evolution remains elusive as organizations instead invest in thousands of additional policies to protect against different evolving scenarios.

Detection efficacy is also problematic across these product categories because they generate a mountain of alerts that require armies of tier-1 analysts that have little to no context about the generated alerts. Even siloed responsibilities lead to product stack fragmentation. Overlapping pain points but disparate budgets result in different products purchased by the CIO, CISO, CDO, or the Chief Risk Officer.

The Missing Layer: the Human Layer

Organizations struggle to define the perimeters of protection for their core resources. Compromises that involve information or money can easily be engineered today by attacking the weakest, yet most important, part of an organization - its people.

Securing this human layer involves rethinking enterprise security in a fundamental way. Email continues to be the single biggest attack vector, responsible for 94% of all attacks. Attacks have evolved from older techniques such as phishing URLs or malicious payloads to simple text-only emails that are engineered to manipulate human trust.

> ***Email continues to be the single biggest attack vector, responsible for 94% of all attacks.***

New product categories have emerged and matured while trying to address this fundamental problem. Some of them describe themselves as addressing the human layer. But each of those categories grapples with its own sets of deficiencies.

- Email security products struggle with identity and identity-related attacks.
- Identity and authentication focused products act as gatekeepers in verifying identity to let users into a network but struggle to monitor and authenticate behavior on a continuous basis, often resulting in data leaks.
- DLP products stop at simple regex-based string matches and document-level signature detection, while missing more intelligent compromises that involve copying parts of documents or rephrasing content. What is considered confidential also changes with title, department and time.
- Often IT departments are not best placed to classify data without sufficient information, but the non-IT departments that can make the decision do not have access to, or understand the complex tools in their organizations.

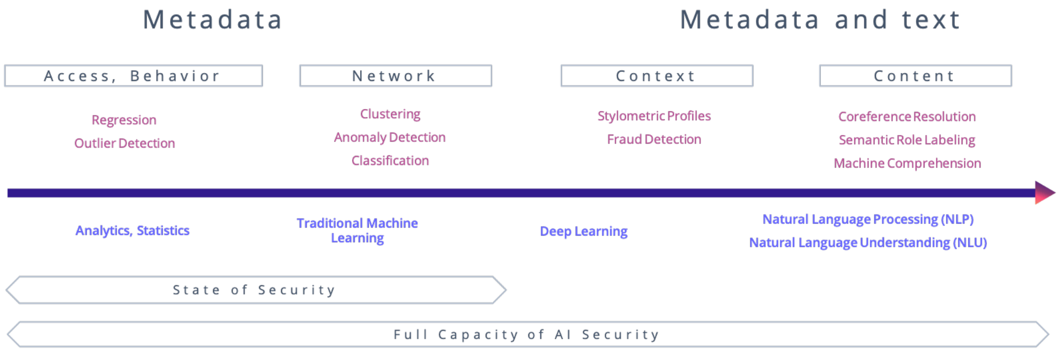
While some vendors in these categories offer employee training to address the human factor, it has been proven to be ineffective. Organizations need a solution that can understand and reason about textual communications, and automate security actions that reduces risk.

AI to the rescue

Security tools classically attempt to stitch together incidents across different channels, but fail to provide timely insights into the attacker's intent. This failure is largely due to the lack of focus on modeling human behavior and the massive mundane workflows required to catalog good ones from the bad.

“Privacy and data breaches are top of mind. However, extortion and fraud attacks are becoming more prevalent as well,” according to the Gartner 2019 Planning Guide for Security and Risk Management.[3]“ Common attacks include ransomware, business email compromise, and credential phishing and stuffing. A particular challenge is increased exposure to attackers, for example, by the move to cloud-based services, which can make previously firewalled users and administrative functions accessible via the internet. Because many traditional security controls don't encompass these newer environments, it is easy for an organization to incorrectly use or configure them, or miss their existence altogether. Newer business technologies, such as increased use of robotic process automation (RPA) and the emergence of AI and machine learning (ML) in business processes and applications, are by and large uncharted cybersecurity territory.”

Evolution of AI for Security



Historically, machines have accelerated human potential by automating tedious processes. From using punch cards for a national census, to autonomous flights redefining human locomotion, machines enable us to better understand our environments.

Recent advances in deep learning show that we are entering a new era of *Natural Language Understanding*[4] that advances machine comprehension of textual data

[3] “Gartner 2019 Planning Guide for Security and Risk Management,” October 5, 2018
[4] https://en.wikipedia.org/wiki/Natural-language_understanding

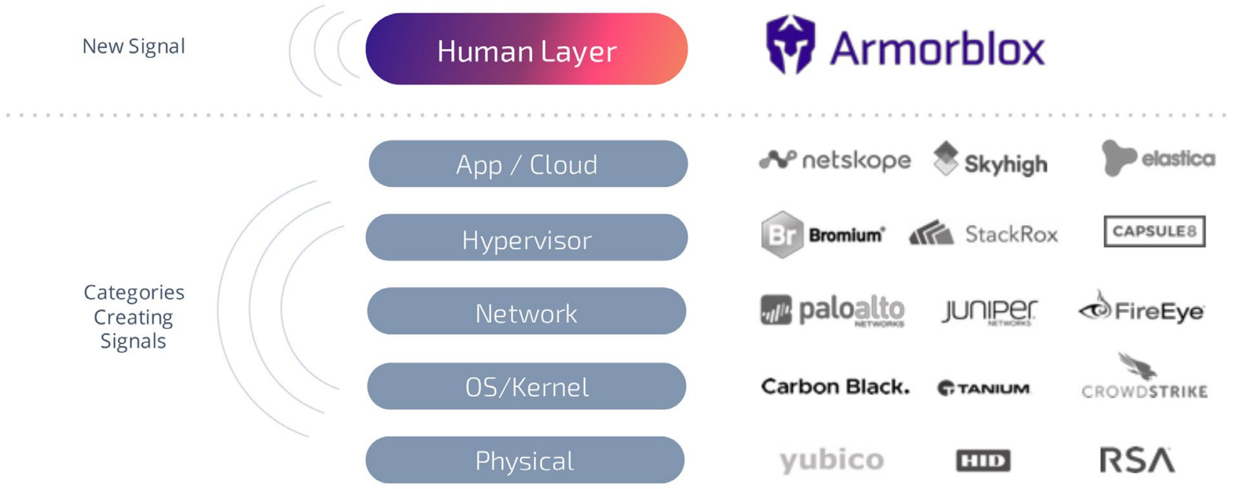
to new frontiers. These advances have the potential to power the next-generation of security tools that can reason about textual data with the ultimate goal of accelerating detection and remediation.

Natural Language Understanding (or NLU) combines context with post-processed[5] text to summarize structured or unstructured data. An ensemble of techniques, such as Named-entity recognition, Coreference resolution, and Semantic role-labeling among others, augments the signal required to determine if a document or an email posed a potential threat.

The Armorblox Platform

Armorblox has built the world's first natural language understanding (NLU)-powered security platform that fully leverages the spectrum of AI to secure the human layer. It enables organizations to replace one-time security gates with context-aware, adaptive, programmable security. It continuously discovers, monitors and prioritizes risk - proactively and reactively. It uses analytics, AI, and automation to speed time to detect, respond and scale.

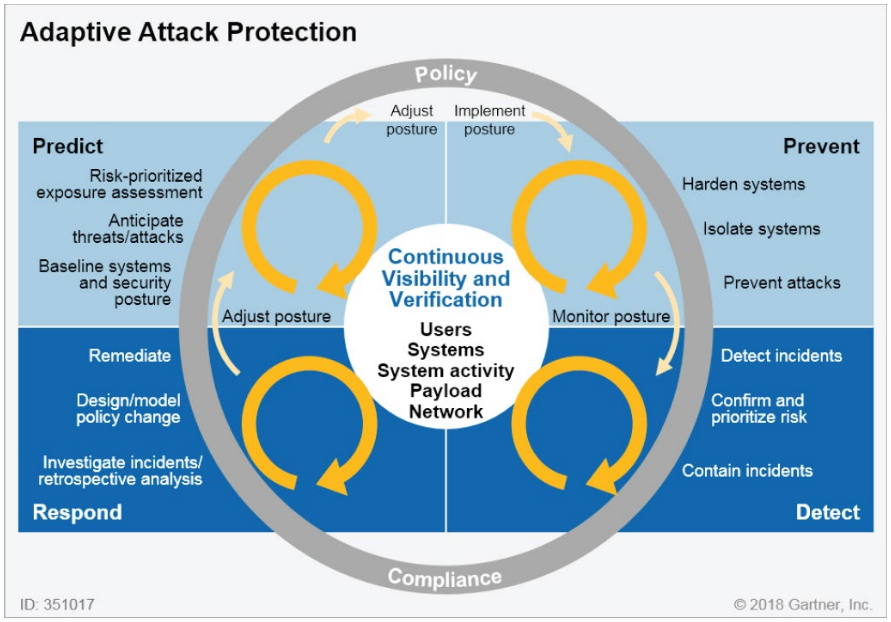
[5] Post processed using NLP



By analyzing and comprehending user data using NLU and machine learning, Armorblox provides a security platform that adapts to evolving threats. It helps them continuously:

1. **Detect:** The natural language engine derives unprecedented insights from enterprise communications and data by combining best of breed natural language understanding (NLU) and deep learning algorithms.
2. **Predict:** The policy learning and recommendation engine requires no pre-configuration and learns what is important for the organization to automatically create and recommend policies.
3. **Respond:** An alert remediation framework that reduces security team workload by reducing the number of false positive alerts and distributing context-sensitive alerts to relevant users for validation.
4. **Prevent:** A policy enforcement framework that integrates with your app to label, tag, encrypt or block access to sensitive content.

Security and risk management leaders need to embrace a strategic approach where security is adaptive, everywhere, all the time. Gartner calls this strategic approach "continuous adaptive risk and trust assessment," or CARTA.


Adaptive Attack Protection
Policy
Adjust posture
Implement posture
Predict
Risk-prioritized exposure assessment
Anticipate threats/attacks
Baseline systems and security posture
Prevent
Harden systems
Isolate systems
Prevent attacks
Adjust posture
Monitor posture
Continuous Visibility and Verification
Users
Systems
System activity
Payload
Network
Remediate
Design/model policy change
Investigate incidents/ retrospective analysis
Respond
Detect incidents
Confirm and prioritize risk
Contain incidents
Detect
Compliance
ID: 351017
© 2018 Gartner, Inc.

Source: Gartner (April 2018)

Armorblox brings understanding to security, helping customers with:

Email security

In addition to analyzing the metadata and the URLs, Armorblox analyzes the content, sentiment and tone of emails. Armorblox uses these signals to identify phishing, spear phishing, ransomware and social engineering attacks at scale that other security solutions can't catch.

Data protection

As employees share important documents and communicate through collaboration, content management, and workflow automation tools, Armorblox provides a context-aware, adaptive security platform to secure the textual communications and data shared between your employees, customers, and partners. Armorblox instruments the data across your infrastructure for comprehensive, full-stack visibility, including sensitive data handling, to identify when data is being improperly shared.

Insider threats

Insider threat detection poses a security risk and a challenge as it requires adaptive measures to protect confidential and proprietary information from leaving your organization. Typically such risks manifest from malicious employees, ex-employees or employees mistakenly sharing confidential or proprietary information across or outside of organizational boundaries. Armorblox classifies data appropriately and provides a context-aware adaptive security platform to secure textual data shared between your employees, customers, and partners.

Armorblox

About Armorblox

Armorblox has built the world's first natural language understanding platform, providing a new way to intelligently detect, alert and protect against identity-related attacks and data loss. Enterprises use Armorblox to automatically create and adapt policies, continuously measure risk exposure, and reduce alert fatigue. Founded in 2017, Armorblox is headquartered in Sunnyvale, CA and backed by General Catalyst. For more information, please visit https://www.armorblox.com.