451 Research | Business Impact Brief

Modern Analytics: Illuminating and Transforming Enterprise Security

The 451 Take

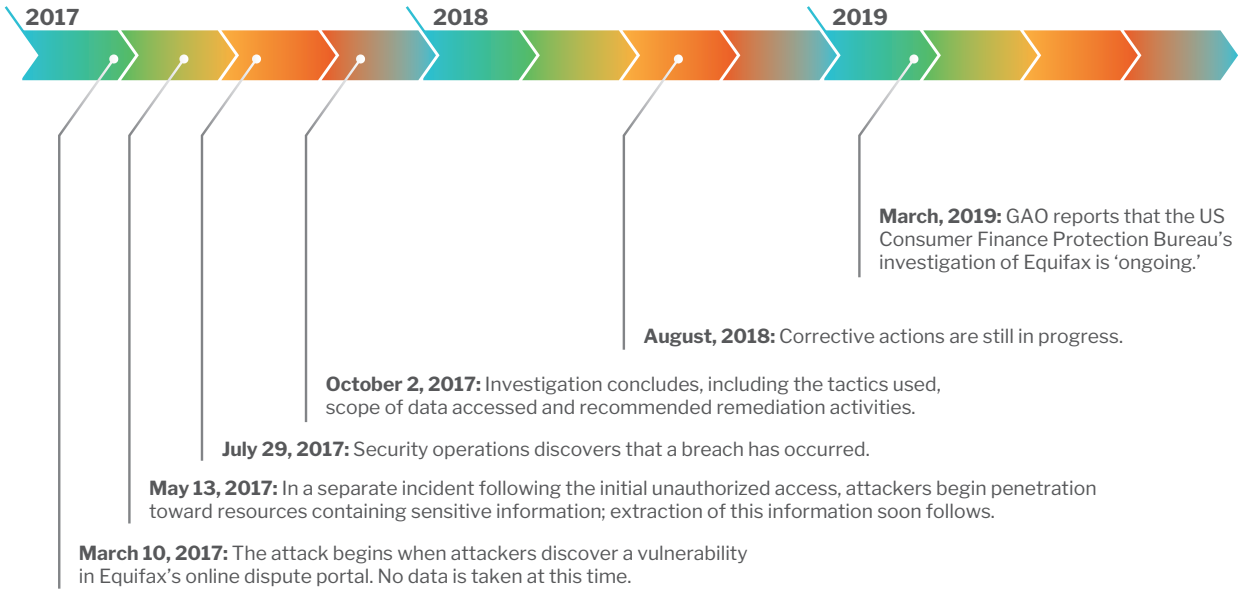
IT is complex and continuously evolving, and keeping it secure has never been trivial. Billions have been spent to protect it, but in spite of that investment, attackers continue to find ways to penetrate defenses and compromise targets. These attacks are often successful because of three major factors:

- **Inability of defenses to identify existing compromise.** When sources of information that reveal aspects of compromise cannot be well and timely correlated, organizations can miss important signals and fail to distinguish normal activity from threats already present within their environment.
- **Lack of ability to recognize new compromise.** Without the ability to baseline the current environment and recognize existing compromise, organizations may be challenged to identify the activity of new threats and respond appropriately.
- **Inability to contain compromise before it has consequences.** With response, time is of the essence, and the tactics applied to a new event may be very different from response to existing compromise. When longer-term compromise cannot be distinguished, or its full extent cannot be recognized, organizations may respond as if it were a new event and fail to contain it fully.

These factors contribute to compromise measured in hundreds of days as evidenced in the timeline reported by the US Government Accountability Office's investigation of the 2017 Equifax breach (below) – but the adversary may have achieved their objective within hours, if not minutes.

Timeline of Equifax Breach

Source: 451 Research, 2019, and US Government Accountability Office, 2018



451 Research® | Business Impact Brief

Business Impact

The good news for enterprises today is that technology is arising to help them overcome these persistent blind spots in compromise recognition, containment and response:

ADVANCED COMPROMISE DETECTION CAPABILITIES ARE MORE WITHIN REACH THAN EVER, SO ORGANIZATIONS SHOULD TAKE ADVANTAGE OF THEM. The scale and performance of cloud-based computing and developments such as machine learning can help organizations identify anomalous activity using statistical methods and proven algorithms. Organizations should remain open to innovations and evaluate their potential. Legacy technologies, including SIEM, may not have been equipped with the capability to learn from observed behavior. Organizations should weigh the value of these advanced capabilities in their comprehensive strategies, and consider how automation can complement them to apply appropriate response, strengthen defenses and help relieve overstretched personnel.

ARM THIS CAPABILITY WITH DATA FROM THE *RIGHT* SOURCES. This means better equipping organizations with tools that leverage modern techniques. Legacy analytics correlate log data from network and security point products, but these sources may overlook network metadata, which can provide the insight needed to recognize compromise and distinguish existing threats. Too much focus on log data may cause users to overlook other valuable sources of threat data that could provide more solid identification of malicious activity or compromise. For example:

- Spam filters can provide intelligence on attack sources, targets and methods used to penetrate defenses.
- DNS provides insight into domains connected with malicious activity and can be correlated with other activity observed within the organization.
- Suspicious IPs and domains can be cross-checked, revealing attack sources that may not have been properly correlated and identified, as well as sources that may remain dormant for some time, but become reengaged in more recent attacks.
- Web gateways and proxies can provide insight into malicious content as well as threat sources.

IMPROVE THE FIDELITY OF THREAT RECOGNITION AND RESPONSE. As sophisticated analytics and learning and detection capabilities become more prevalent, organizations must be open to innovation. For example, behavioral analytics can create large numbers of false positives, but feedback loops can help solve this problem. Initial analytics create a baseline. Subsequent analysis can recognize deviations, acknowledge legitimate changes and distinguish new threats from previously recognized activity. Each successive iteration helps refine findings to allow more recent suspicious activity to be better recognized. This strengthens the system, improves its fidelity of detection, and aids in more effective response.

Looking Ahead

One of the most persistent challenges enterprise security teams face is sourcing and retaining security expertise. Organizations must harness technologies that not only meet the scale and overwhelming detail of the security challenge, but that can also relieve people of tasks that technology can handle more efficiently. Modern analytics can tackle scale, speed and detail, but to be truly effective in helping close expertise gaps, they need high accuracy. This becomes even more important when they provide input that triggers automation for mitigating threats and containing their impact – and as organizations become increasingly dependent on these technologies to close security gaps. Accuracy will, therefore, become not just a benefit, but a vital necessity for organizations that have relied primarily on personnel to discover threats and deliver effective response.

Organizations will require greater visibility across a wider variety of network and IT terrains – analytics will need to go beyond legacy environments to 'see' within emerging, cloud-native architectures. Visibility across the hybrid enterprise will be required to encompass both legacy and on-premises environments, as well as IaaS, PaaS and SaaS resources. At the network edge, defense must be extended to mobile assets. This requirement is rapidly expanding to include an even greater influx of non-traditional IT resources, such as operational technologies, industrial controls, and entirely new (and 'smarter') IoT technologies. The rise of 5G will likely push more sophisticated computing capability even closer to the network edge, driving sophisticated analytics for security to tackle more distributed demands much closer to threat sources.