iboss™
CYBERSECURITY

Reducing Dwell Time with Behavioral Analytics

THE KEY IS IDENTIFYING HIGH-RISK INFECTIONS FASTER

iboss CYBERSECURITY

Reducing Dwell Time with Behavioral Analytics

THE KEY IS IDENTIFYING HIGH-RISK INFECTIONS FASTER

High-stakes hide and seek

Today's IT environments are complicated, comprised of clouds, virtual machines, BYOD, floods of data, and distributed workforces. These complexities give attackers lots of hiding places. Many security programs hunt for intruders by looking for particular attack signatures, which are distinctive patterns that were known to be used in previous attacks. However, this approach can't find new types of attacks because they aren't in any database yet.

Even if an organization isn't relying solely on signature-based security, intruders can still be hard to detect because attackers adjust their strategies regularly. For instance, a lot of malware now uses encrypted code segments that are hard to turn into signatures. The most dangerous attackers are well-organized and well-funded; they buy all the leading security products in order to replicate a target's environment so they can learn the best ways to slip in and stay as long as possible.

Sheer volume is another reason intruders are able to stay inside networks for so long. The average company experiences over 10,000 events per month, more than half of which are false positives. However, a lot of companies are still relying on manual analysis to score events and lack the capability to see patterns of alerts that would reveal an attack in progress. Attackers have the upper hand simply because they can hide in the crowd.

Attackers are smart, sophisticated, and adaptable. The only way to find them is to analyze massive volumes of data in near real-time and in a way that reduces the false positives that drain resources and distract from true threats.

Attackers don't just want to get inside your network. They want to stay inside your network. The longer attackers can remain undetected, the more time they have to find the locations of the most valuable data and take it away by the terabyte.

For that reason, organizations need security strategies that focus on more than keeping out intruders—they have to think about how to recognize the presence of intruders and end their activities as quickly as possible. In the same way that cancer is treated more effectively when it is discovered early, the damage from an attack is reduced if the time an intruder dwells inside is promptly curtailed.

Dwell time begins when an attacker breaches the network and continues until the attacker leaves on his own or is detected and kicked out. The average dwell time is currently 200 days. Yet an attacker with mid-level skills only needs a single day to map a network and credentials, wipe out evidence of his presence, and set up a back door to make future attacks more convenient. That leaves a window of 199 days to steal data, but even a dwell time of a few short days is long enough to allow an attacker to inflict significant damage. According to the 2016 Verizon Data Breach and Investigation Report (DBIR), only about a quarter of breaches were found in "days or less" after the initial compromise. Breaches are increasingly discovered by law enforcement or third parties and decreasingly discovered by the compromised organizations themselves.

Reducing dwell times does more than limit damage; it can help prevent future attacks. The primary motive of attackers is not to penetrate a target— it is to stay inside for as long as necessary to find and exfiltrate valuable data. When attackers can't stay inside long enough to get all the data they want, they are likely to find a softer target for their next exploit. After all, there's no shortage of soft targets.

The **overlooked metric**

Many organizations do not yet measure dwell time. This happens when an enterprise doesn't recognize and respond to the reality that breaches are inevitable, doesn't understand that attackers disguise themselves as insiders to navigate a target's network freely, and/or because they don't have visibility across all inbound/outbound traffic so they cannot correctly identify the routes attackers follow to access the most valuable data and exfiltrate it from the network.

Determining when an attack was initiated is not straightforward because breaches today tend to be conducted by a combination of techniques, such as hacking, social engineering, and automated attacks. If an organization can't learn when an attack began, it can't measure the dwell time.

Additionally, many attacks now use multiple attack vectors; for instance, in the case of some of the Office of Personnel Management (OPM) breaches, attackers began by hacking companies that provided background checks for OPM employees. Once inside, the intruders were able to enter the OPM's network and continue their activities. What was the dwell time? It's hard to say since attackers that use vendors' credentials to access a target can operate undetected for a very long time.

Another factor making these complexities tough to untangle is the shortage of cybersecurity expertise capable of doing the job. The dearth of talent is a well-known problem and one that can't be solved by turning out newly-certified CISSPs as fast as possible. Security professionals become valuable by learning on the job, so it really takes a veteran analyst to recognize anomalies in complex environments.

Companies that disclose breaches will reveal how many records were stolen and how much the breach cost them, but usually they don't provide data on how long the intrusion lasted. That's because they often just don't know. Even when they do disclose dwell time, in some cases the numbers are best guesses. For instance, in the case of the OPM, there were a series of breaches that are most likely related. In the first, information on network architecture was stolen, and that was probably used in the series of attacks that followed. Those ensuing attacks were against both OPM and its business associates, namely two companies that run background checks.

This chart of recent high-profile data breaches illustrates the connection between dwell time and magnitude of data loss.

ORGANIZATION	DWELL TIME	RECORDS COMPROMISED	CAUSE OF DISCOVERY
Excellus	22 MONTHS	10.5 MILLION	Reviewed network activity after becoming aware of attacks on similar organizations
PREMERA BLUE CROSS	8 MONTHS	11 MILLION	Internal monitoring
HOME DEPOT	6 MONTHS	50 MILLION	Notified by banks and law enforcement after hackers tried to sell data on hacking forum
OPM	3-12 MONTHS	22 MILLION	Informed by contractors (Multiple attacks that appear to be related)
J.P.Morgan	3 MONTHS	76 MILLION	Informed by security company investigating Russian crime ring

Attackers come **with a plan**

Once inside a network, attackers learn the lay-out, move from machine to machine, and scan the network to find remote hosts and exploitable web servers they can use to hop around in search of sensitive data.

They install back doors so they can visit again with greater efficiency, delete event logs to hide their activities from log analysis tools and, of course, steal as many credentials as possible.

Attackers snap up documents and shared drive access from regular users as they search for users with higher privileges that they can use to gain access to the most critical servers and systems while disguising their malicious activities and, therefore, increasing the persistence of the attack.

WHERE STANDARD CYBERSECURITY FAILS

- **Not enough** visibility over hidden ports and protocols
- **Too many** new / morphing / evolving threats slip through
- **Too many** undifferentiated alerts
- **Too few** qualified analysts to investigate and resolve cyber threats

When security slips, **attackers advance**

Most of today's security solutions are fundamentally flawed. Traditional security solutions focus on catching malware but lack the ability to detect an evasive infection that has breached the perimeter and is lurking inside the network.

When it comes to reporting, they are based on what happened yesterday, last week, or last year, but they can't alert a network operator to what is going to happen tomorrow or, often, what's occurring right now. In addition, they rely on a human interpretation of events so they are subject to human fallibility. Human error becomes even more of a problem in the face of massive logs of event data with no distinction between what is benign and what is malignant.

Signature-based approaches have become less effective as threats have become more dynamic. Devices, access points, and use cases have grown exponentially. As a result, the complexity of network architectures has evolved beyond the capacity of even expert humans to understand. Only a formidable team of security analysts can manage most of these solutions with any level of effectiveness, and formidable teams are hard to build and costly to keep.

Organizations have turned to sophisticated analytics platforms, but found them impractical to deploy and manage. Instead of helping to solve the problem, they create choke points when deploying sensors to collect data, and they require mobile users and remote offices to backhaul data to the core network in order to secure it. That places additional pressure on the network while exposing the data in transit to attackers who are listening for it.

Add to these concerns high costs, which make such platforms available only to large financial institutions with mammoth budgets and resources. Only leading financial brands can bear the heavy investment in CAPEX and the burden of increasing TCO that occurs when these solutions are installed on-premises.

Common approaches to dwell time reduction

LOCK THE DOORS

Slow down an attacker's entry with standard security controls like a good patch program and strong identity and access management, and use multi-factor authentication. Just as a burglar will pass by a home with an alarm company sign for a neighbor with an open window, cyber attackers prefer to invest their time and effort in easy marks. Set up extra monitoring around the systems and people most critical to your business—they attract attackers like a flame attracts moths; if an attacker gets inside, that's where he's heading.

NETWORK BEHAVIORAL ANALYSIS (NBA)

Relying on a database of attack signatures to identify threats only protects a network from threats that are already known. However, attackers are always changing their techniques, tactics, and procedures, so organizations need to recognize new threats as they occur. Behavioral analytics start by establishing a baseline of normal behavior and then constantly monitoring for behaviors outside the norm, such as an app containing sensitive data connecting to the port that lets traffic in and out of the network. NBA separates false positives from real threats.

MANAGE INTELLIGENCE TO CALCULATE DWELL TIME

In addition to creating red flags to signal abnormal activities on the network, correlate actions to each machine and user and collect detailed information about all incoming emails so that security staff can trace suspicious messages to their point of origin.

MATCH PEOPLE TO POLICIES

Sometimes events that seem random are actually part of an organized attack. Monitor endpoints to see if user activity adheres to security policies; that creates context, which helps the security team recognize when a real attack is in progress and respond more quickly.

PREDICTIVE ANALYTICS

Predictive analytics take the concept of network behavioral analytics further. Instead of assessing current anomalies, predictive analytics ingest massive amounts of data to find predictors of future behavior. That allows organizations to identify which activity inside the network is about to become dangerous and end it before it can execute its mission.

The best predictor of future behavior is past behavior

This truism is the basis of industries such as insurance, mortgage, and credit services. Now, it is being applied to cybersecurity. Predictive analytics are based on predictors, which are variables that can be measured to predict future behavior. Multiple predictors are combined into a predictive model, which can then be analyzed to create forecasts of future probabilities. The model is revised as new data is collected, becoming iteratively more reliable.

A familiar name
with a fresh approach

As the most targeted of all verticals, the financial sector has the greatest need for security solutions that attackers can't evade. FICO, the organization known to most people as the credit score company, is actually a software analytics company with 25 years of experience in fraud detection. Used in over 90 percent of credit decisions and holding over 100 patents related to streaming behavioral analytics for attack detection, FICO is a proven leader in fighting fraud.

Now, FICO is applying its knowledge and experience to create a predictive analytics model that will help organizations detect attacks with better reliability and accuracy. FICO's model is capable of identifying not only known techniques, tactics, and procedures, but also unknown threats that have not yet been noted by analysts.

Milliseconds
to unmasking

FICO's patented predictive analytics identify anomalous activity within milliseconds, leveraging artificial intelligence to become smarter in real-time. The analytics model creates a threat score that evaluates the level of suspicion associated with the behavior of specific devices, users, or servers on a network, in a manner similar to the way credit scores are created and updated.

The FICO Threat Score is integrated into the iboss Cloud Cybersecurity platform. This integration is possible because of iboss' unique node-based, containerized architecture, which provides more security in the cloud by isolating each organization's data in its own container so it never overlaps with any other in the public cloud. Together, the technologies are able to identify and remediate in real time what other solutions miss. Blind spots are eliminated; even attacks that mask communication with TOR software like the Zeus64 malware Trojan and Locky ransomware can be found and stopped before an infection becomes catastrophic or data is abducted en masse.

SECURITY AMPLIFIED BY ANALYTICS

- **Enhance** your security posture instantly by extending security across all users, devices and locations with minimal resources
- **Reduce** CAPEXTCO, and eliminate backhauling of traffic to HQ
- **Gain** single pane of glass reporting across all users, enhancing visibility while shortening incident response times
- **Eliminate** choke points created by traditional sensors
- Flexible deployments allow for nodes to be hosted locally

Stop attackers
in their tracks

Perimeter security and intrusion detection solutions are no longer adequate protection for organizations that value security—which should be every organization. Only companies that are measuring dwell time can gain a true understanding of the levels of risk they must manage and the level of exposure to which their customers, business associates, and employees are subjected. Reducing dwell times not only safeguards data more effectively, it also helps organizations control the costs of data loss, since data loss either doesn't happen or is at least minimized by the shorter duration of the attack.

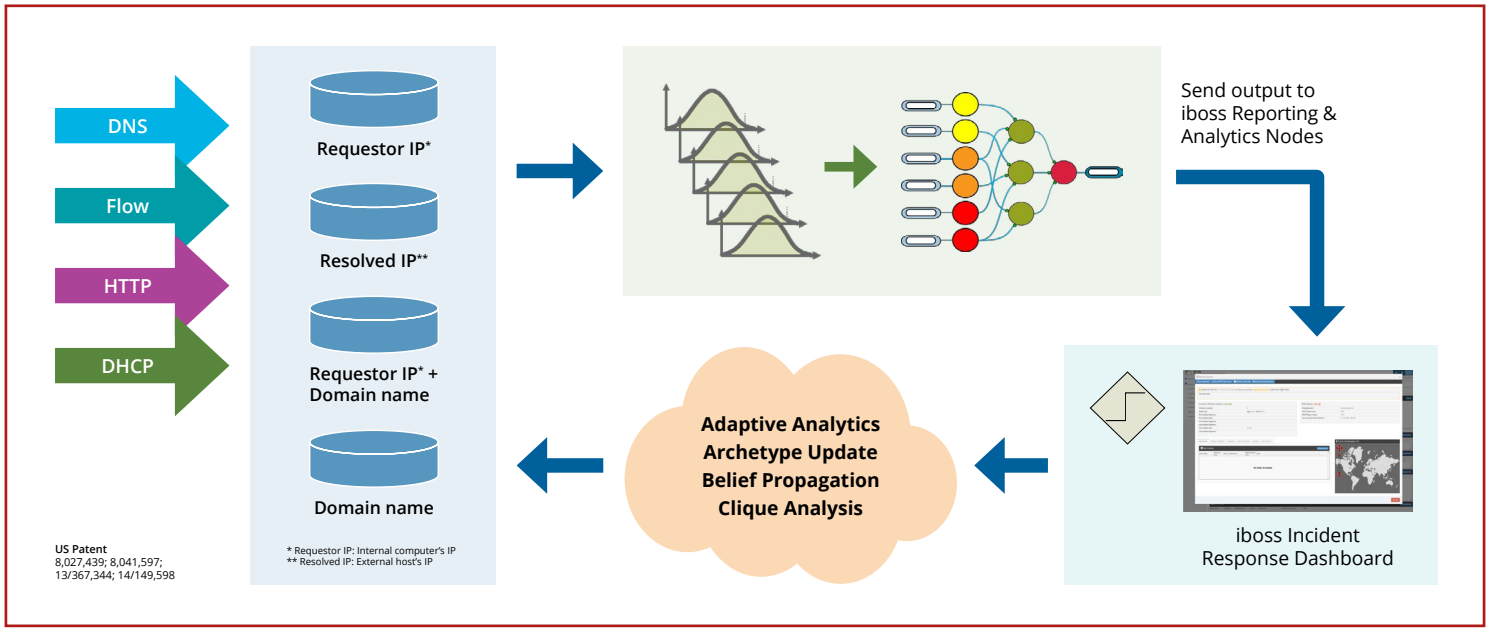
Attackers are smart, agile, and often equipped with technology that is better than that of their targets. Most businesses can't be as agile as attackers simply because they have processes and controls in place that make experimentation difficult, which is reasonable and proper. However, predictive analytics built on AI and running in an innovative secure containerized cloud is a way for businesses to level the field.

The fabric of the **FICO Cyber Threat Score**

iboss uses its proprietary secure containerized architecture to deploy FICO in distributed organizations. Fundamentally different from conventional security cloud architectures, iboss relies on a virtualized architecture that uses nodes to deliver an infinitely scalable, dynamic, and elastic cloud.

Predictive analytics running on iboss's containerized architecture can detect even previously-unknown infections faster, reducing data loss during an attack. Event log noise is reduced, allowing the threats that pose the highest risk to be pinpointed in real time. Security analyst teams are alerted to threats with the highest scores, while iboss auto-containment stops any data being exfiltrated mid-stream. The behavioral-based Cyber Score gives security teams quantifiable intelligence about which threats they should tackle first, accelerating response times to the most dangerous incidents and dramatically reducing data loss.

When new exploits are detected, the containerized cloud architecture updates all iboss users in minutes, better positioning them against the latest attacks. The same level of security is extended to all devices, users, and remote sites on the network, so the organization is completely protected.



About **iboss Cybersecurity**

iboss Cybersecurity defends today's borderless networks against malware, advanced threats and data loss with an innovative direct to cloud, containerized, node based approach. Unlike legacy technology focused solely on keeping malware out, iboss offers a balanced cybersecurity approach with equal emphasis on prevention, detection and containment to reduce damaging loss from data breaches. Backed by patented, next-generation technology and unparalleled visibility across all inbound/outbound data channels, iboss next-gen technology provides better security weapons to reveal blind spots, detect breaches and minimize the consequences of data exfiltration. Leveraging leading threat protection and unsurpassed usability, iboss is trusted by thousands of organizations and millions of users.

www.iboss.com

About **FICO**

FICO (NYSE: FICO) powers decisions that help people and businesses around the world prosper. Founded in 1956 and based in Silicon Valley, the company is a pioneer in the use of predictive analytics and data science to improve operational decisions. FICO holds more than 165 US and foreign patents on technologies that increase profitability, customer satisfaction and growth for businesses in financial services, telecommunications, health care, retail and many other industries. Using FICO solutions, businesses in more than 100 countries do everything from protecting 2.6 billion payment cards from fraud, to helping people get credit, to ensuring that millions of airplanes and rental cars are in the right place at the right time.

www.fico.com