Traditional email protection platforms and appliances sit between a network and the outside world, shielding that critical gateway and chokepoint. They filter incoming email to weed out spam and viruses, and sometimes also prevent things like personal or confidential information from leaving a network the same way. They are good at what they do but are becoming increasingly ineffective against things like advanced phishing and targeted impersonation attacks. And they do nothing to prevent some new kinds of attacks, like when a hacker takes over an email account and then sends their malware or phishing attacks internally to other users.

The effectiveness of these so-called gateway appliances is well known. Review bakeoffs often have the top competitors performing at 99.5 percent accuracy or higher. It’s unlikely that any email with a malicious package, a link to a malware site or other forms of traditional attacks are going to make it through those defenses. The problem is that hackers know this and have started to develop email attacks and new techniques designed to circumvent gateway protection.

They do this in a variety of ways, but one frequently used technique is to send a highly targeted email that is void of any links or malicious payloads that the gateways will detect. Sometimes they pretend to be a colleague or business contact and simply ask for the targeted victim to write them back, but at an account that the attacker controls, which is often camouflaged to look like something else. They can then run their cons using the established channel or by leading a victim to another, unprotected communication platform. Or they can include a call to action in their first email, such as a request for a money transfer, but with bank details provided in plain text to fool filters. And in the newest form of attack, hackers first work to compromise an internal email account and then use that to launch their attacks, avoiding the network gateway entirely.

One of the biggest shortcomings of gateway appliances is that they rarely have any insight about the network they are protecting. Sure, they can find malware or malicious links in incoming mail, but they don’t know that a seemingly innocuous email sent from a Gmail account isn’t really coming from the company CEO. Another shortcoming is that, because they sit at the gateway, they have no control over internal emails and are in no position to ever come in contact with them.

Because of this, everyone from the private sector to government agencies are urgently searching for some way to boost their email security. It may well be the next big push in cybersecurity.

The Barracuda Sentinel email protection platform could be a big part of that solution. Instead of sitting at the gateway, Sentinel connects at the API level to any cloud-based email program like Microsoft Office 365, which was used for this review. It integrates with every inbox from a protected organization, giving each one individual attention, whether or not the mail came from the outside or the internal network.

Sentinel is offered as a service, with pricing based on the number of employees being protected. That way employees can have more than one inbox without raising the price. Barracuda calls this new form of email protection Inbox Defense. It’s designed to work in conjunction with a gateway appliance or other email protection (Barracuda itself offers several gateway defense appliances and platforms) and mostly concentrates on the aforementioned gaps in all gateway platforms.

Setup: Training the AI

Installation of Sentinel could not be easier. Once employed, the service will simply need permission from the email administrator to integrate with every existing mailbox at the API level. After that, it will dive into the email archives using an artificial intelligence to learn about the people, patterns and programs used by authorized users. (Finally, a good use for all that archived email that piles up on the servers of most organizations.)

Sentinel can go back a year into email archives to discover how users communicate, down to their preferred linguistic patterns and any outside accounts they send mail from. Depending on the size of the organization, it can take up to a day for the Sentinel AI to digest and process all of that information, though nothing is required of
human administrators in the meantime.

Sentinel learns how users communicate so that it can spot anomalies that might be an indication of an attack later on. In an extreme example, if the company CFO always uses complete sentences and proper grammar in his email and suddenly using slang it might mean that his account has been compromised.

Interestingly enough, it’s very possible that Sentinel will spot attacks that have already occurred over the past year as part of this learning process. This was tested using an email archive that was protected for over a year with a gateway mail security appliance. It allowed a surprising number of targeted attacks through its defenses. These archived attacks were pointed out in the dashboard interface.

Historical attack data is both interesting and potentially useful. For example, if something like a hostile account takeover is discovered by Sentinel, that might be the first indication that something is wrong, and the attack could still be ongoing if the hacker behind it is moving very slowly to avoid detection or is using the compromised mailbox to recon for other attacks.

The AI that powers Sentinel is advanced enough to be considered a second-generation AI, as it is able to explain all of its actions in plain language. For example, it was extremely easy to see why the program quarantined an email that supposedly came from a company official in our testbed. The email was stopped because of several factors: The from address had never before been used by that person; the mail itself makes an urgent request, in this case to transfer funds internationally; the mail asks the recipient for her availability, something many impersonation attacks do to keep the intended victim off-guard; and it used language and keywords that don’t match the historical mail archive that the AI previously observed.

The report is also helpful because, by only focusing on mail that actually made it into an inbox, it will clearly identify the holes in any existing mail gateway security. Information gained from the historical report can also be exported to a CSV file for further analysis.

Testing Barracuda Sentinel

Once the AI is trained up and ready to go, Sentinel can be fully activated. Administrators can program what actions the program will take in response to various threats. For example, phishing emails could be immediately deleted, while email coming from a new account might be quarantined for more analysis by human administrators. Users can be notified about blocked or quarantined email using a template of configurable automatic responses — or they can be kept in the dark about Sentinel’s actions. That all depends on the organization’s policy and attitudes about email security and how much they want to bother users with information about security actions taken on their behalf.

The dashboard for Barracuda Sentinel is very clean, and in our testing contained almost no false positives. It relies on up to a year of email archives to learn about organizational mail, so is highly accurate.

Sentinel can protect inboxes without users ever even knowing that it’s there. But if you want to keep your users in the loop, a set of messages can be configured to explain why specific emails were blocked or quarantined.

The AI that powers Sentinel is advanced enough to be considered a second-generation AI, as it is able to explain all of its actions in plain language. For example, it was extremely easy to see why the program quarantined an email that supposedly came from a company official in our testbed. The email was stopped because of several factors: The from address had never before been used by that person; the mail itself makes an urgent request, in this case to transfer funds internationally; the mail asks the recipient for her availability, something many impersonation attacks do to keep the intended victim off-guard; and it used language and keywords that don’t match the historical mail archive that the AI previously observed.

Because Sentinel integrates with inboxes at the API level, it only flags mail that bypassed gateway protection. Here it explains why it suspects that a cleared email is actually malicious.
included in the report. Sentinel is extremely good when making determinations. Most humans could probably do the same thing if they were concentrating on the task at hand and not distracted by a million other daily problems. But for an AI to get it right almost every time is impressive. It’s clear that studying the yearlong archive of mail gives Sentinel a lot of insight into how valid users communicate.

The newest and possibly most dangerous form of attack, an email account takeover, can also be spotted and flagged by Sentinel. It does this in several ways, including looking at where supposedly valid users are logging in to their account. If an authorized user is connecting to their account from North Korea or Nigeria, that could indicate a problem even if the passwords are correct. Sentinel also knows what hackers performing account takeovers do to maintain their secrets, like changing inbox rules or setting it up so that certain mail is automatically forwarded out of the network.

In the case of a suspected account takeover, Sentinel notifies the local IT team instead of taking direct action. This is done for a couple reasons. First, the fact that an email account has been hijacked may also indicate that the user’s endpoint is also compromised — or that this was just one step in a larger attack or campaign. Also, where accidentally blocking or quarantining an email in the event of a false positive probably is not a big deal, making a bad call and locking someone out of their account could be very bad, especially if that user is the CEO.

However, it’s worth noting that Barracuda plans to slowly add automatic actions in response to account takeovers, once current users get a little more time with that feature, just to be sure it’s working at maximum efficiency.

As an extra feature, Sentinel is able to check all email for Domain-based Message Authentication, Reporting and Conformance (DMARC). The DMARC protocol is used, in conjunction with other technologies, to ensure that a sender’s domain can’t be spoofed. While this would be more helpful for users outside a protected company, it would ensure that an organization’s brand is not abused by a hacker trying to use it as an authenticator for phishing or other attacks.

As an extra but highly useful feature, Sentinel can check email for Domain-based Message Authentication, Reporting and Conformance (DMARC) compliance to ensure that domains can’t be spoofed, enabling scams in your company’s name.

The last word

Gateway email protection devices have been employed for years at enterprise organizations. And that won’t stop anytime soon. However, organizations need to recognize that while they are highly efficient, they contain inherent flaws and can be circumvented by skilled hackers employing highly targeted attacks. A platform like Barracuda Sentinel, which sits at the API level well back from the gateway to protect individual mailboxes, is needed to ensure total security in today’s more dangerous threat environment. Thankfully, it’s extremely easy to use, and almost ironclad in terms of its effectiveness at filling in those dangerous gaps.