deep instinct™

CASE STUDY

FINANCIAL SERVICES
BANKING INSTITUTION

Taking a prevention-first approach to protecting critical banking services and customer data

<99%
THREAT DETECTION ACCURACY

0
ENDPOINT SECURITY EVENTS

GAINED VISIBILITY INTO HIDDEN THREATS

The Company

A financial institution that provides correspondent services to community banks.

Industry: Financial Services

Company size: Mid-Enterprise

Existing security solution: Endpoint prevention, detection, and response

This bank provides correspondent, lending, and operations services to community banks in the U.S. Operating in a highly regulated and competitive sector, the bank has a unique understanding of the challenges associated with the compliance, regulatory, and audit needs of the banking community it serves.

The Challenge:

The Changing Threat Landscape Requires a Prevention-First Approach

As the bank continued to mature its security operations and threat posture, it wanted to shift from a reactive approach of detecting and mitigating threats to a full prevention-first cyber strategy to maintain the highest level of security.

Cybersecurity is a boardroom issue, and business-critical services are protected through a robust security ecosystem and strong cybersecurity awareness training for employees. Endpoint protection is a critical threat protection layer and predicting, detecting, and responding to threats before they enter this layer is necessary to guard against breaches.

"We wanted something that we could put into place and have the peace of mind that if anything got to that layer of defense, we would be confident that it would be stopped—even if it was a zero-day threat," says the bank's information security manager.

With layers of effective security in place, the bank had no intention of changing its endpoint protection platform. But the prospect of adding a more sophisticated prediction and prevention layer to extend the security stack led to a demo of Deep Instinct.

Deep Instinct's pioneering use of deep learning—the most advanced subset of artificial learning—was a driving factor in choosing Deep Instinct™ Threat Prevention Platform. Deep Instinct's neural network algorithms can detect and prevent previously unseen and unknown threats, such as zero-day and advanced persistent threats (APTs). The techniques used to disguise and deploy malware evolve quickly, requiring a security solution that does not rely on historical user or entity behavior and heuristics to determine if something is suspicious.

Deep Instinct delivers greater than 99% unknown threat accuracy with less than 0.1% false positives. Endpoint protection is provided with no impact to the user experience: every file, script, and macro is checked pre-execution in less than 20 milliseconds. Deep Instinct also protects against ransomware, providing a $3 million warranty in the event of a ransomware breach—three times the amount offered by any other vendor.

During the demo, Deep Instinct detected dozens of the very latest malware samples and successfully scanned every file type, whether on the drive or over the wire. It quickly became clear to the IT security team that Deep Instinct could prevent advanced threats in pre-execution, not only better protecting its business-critical banking services and customers' data, but also freeing up the IT team from labor-intensive incident response, false positive alerts, and remediation work.

The Results:

Complimenting an existing platform with a prevention-first approach

Deep Instinct is a key element in the financial institution's efforts to proactively protect its business operations, safeguarding customer personal information, data, and trust, and enabling the IT team to respond to fewer false positives and stay focused on priority security demands.

Prevent threats in zero time

Deep Instinct automatically detects and blocks malicious content, without any manual effort from the IT team and without connecting to the cloud, greatly increasing detection speed and threat prevention. A prevention-first approach means there are fewer serious security events to address, and when events do occur, there are more resources to respond to the incident with immediacy.

IT teams also have greater visibility into endpoint risks. For instance, Deep Instinct alerted the IT security team to files that weren't necessarily malicious, but that IT didn't know were there. Identifying these types of files and scripts that were running as part of software tools gave the IT team greater awareness of its software supply chain.

Ongoing operations are smooth. Deep Instinct updates are infrequent and automatic, and within 20 minutes of an update, all endpoints have the latest protection. Adding new endpoints and servers is a simple and straightforward exercise.

"It's super nice to know we can do that and have that peace of mind that all of our endpoints are on the newest version, and we don't have to touch it, or worry about whether we have the latest protection," says the information security manager.

Safeguard customer trust

Any cyber-disruption—especially from ransomware—could have a high impact on hundreds of community banks and their customers. Members count on the bank for check clearing, cash management, access to a Federal line of credit, and bond accounting.

With Deep Instinct protecting its endpoints, IT leadership has an even stronger security posture, with the most advanced threat prevention technology used to guard against cyber threats. The financial institution can confidently assure its members that their business-critical data is protected, and that business continuity is protected. Customer trust is essential to retaining business and acquiring new members in a highly competitive sector.

Reduce IT management time

When malware is detected, Deep Instinct automatically blocks the attack in pre-execution, ensuring it never enters an endpoint. By predicting and preventing threats while also delivering extremely low false positives, incident response is streamlined, and the security team only needs to investigate where the attack came from or if a user caused it. The need to remediate the damage is avoided.

Deep Instinct detects what other solutions can't find, and prevents threats others can't stop, protecting the bank from business disruption, expensive breaches or data theft, a loss of its members and compliance issues. Deep Instinct saves the IT team's time, allowing them to focus on other security considerations.

> *"Endpoint protection is one of the most critical layers in any organization's threat posture and has to be considered a top priority. Even if an endpoint platform is just installed and works in the background, using an advanced threat prevention solution will ensure that your stack is fully extended and enhanced to immediately stop threats. To ensure your endpoints are fully protected, then I'd say Deep Instinct is a great fit. You install it and it just works right away."*
>
> ***– Information Security Manager***

Request an online demonstration of the Deep Instinct Platform

See how Deep Instinct can help protect your organization in this live demonstration of our solution capabilities against unknown threats.

REQUEST A DEMO

deep instinct

www.deepinstinct.com | info@deepinstinct.com

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack—providing complete, multi-layered protection against threats across hybrid environments.