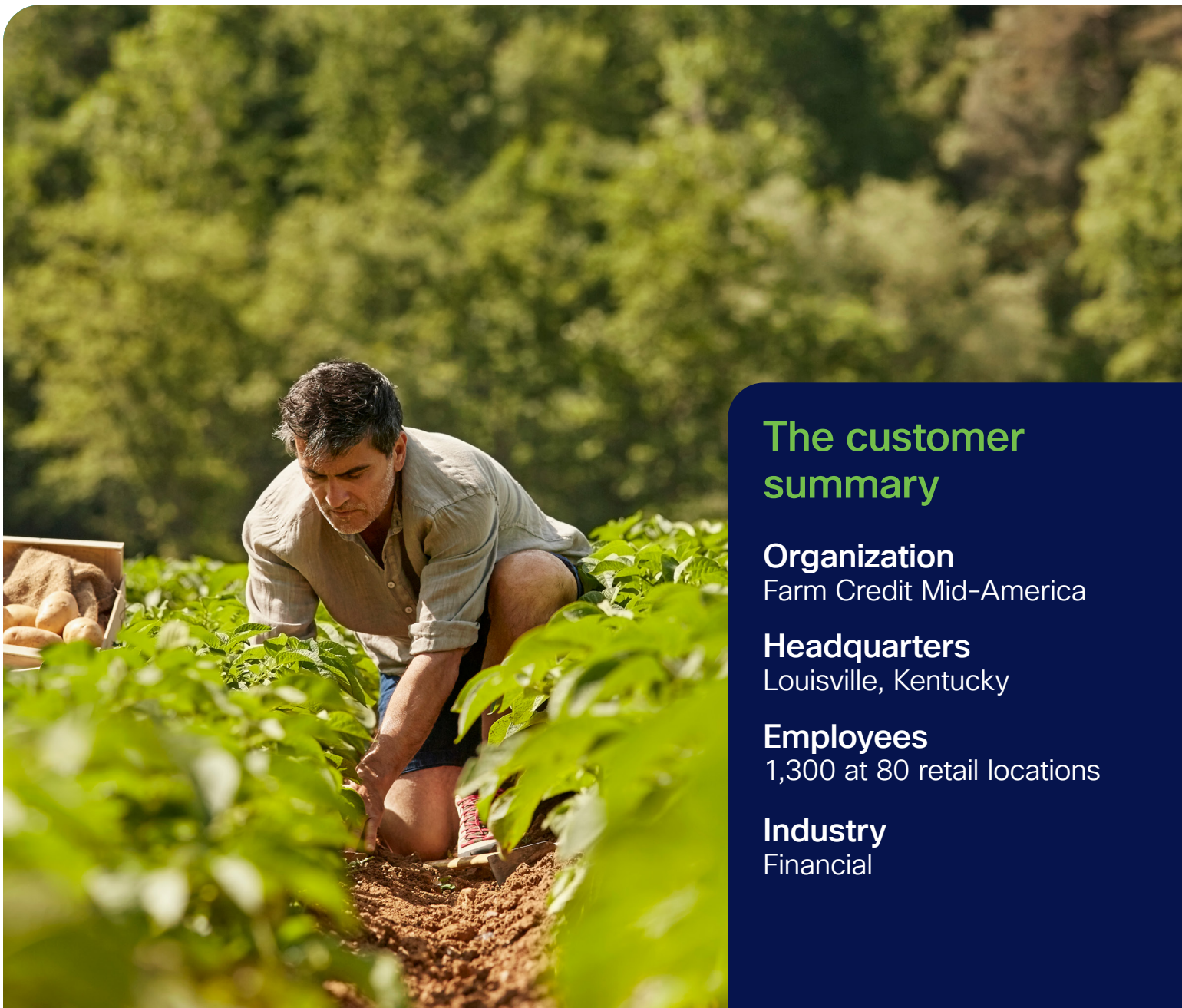




# How a financial cooperative secures customer data while protecting its distributed workforce



## The customer summary

### Organization

Farm Credit Mid-America

### Headquarters

Louisville, Kentucky

### Employees

1,300 at 80 retail locations

### Industry

Financial

## The Challenge

### Protecting customer data and a distributed workforce

As a customer-owned cooperative, Farm Credit Mid-America provides loans and crop insurance to farmers in the rural communities of Kentucky, Tennessee, Indiana, and Ohio, as well as home loans throughout the country. The focus of the \$25 billion financial institution is on “securing the future of rural communities and agriculture,” and protecting customer data is a top priority.

“We’re helping the farmers who are feeding America,” says Mike Mills, security engineer at Farm Credit. “As a financial institution for rural America, we really have our customers at heart, and it’s critically important to safeguard their personal information.”

To achieve this objective, the organization needed a robust solution for protecting its increasingly mobile workforce, distributed at 80 retail locations, from internet-based threats. The security team wanted a suite of controls that provided consistent enforcement of web-based protections, regardless of where the employees used their devices. When the COVID-19 pandemic struck, it accelerated that need since most employees started working from home.

“In a web-centric world, in a work-from-home-world, the threats are web-based,” Mills explains. “Therefore, the controls need to be largely web-based.”

The cooperative had been considering a cloud-based, full web proxy for some time. When Farm Credit’s existing solution, Cloud Web Security (CWS), approached end-of-life, Mills and his team saw an opportunity for implementing a more holistic solution with broader capabilities. Blocking threats early in their lifecycle – before they turned into security incidents – was especially critical. An additional priority for the team was to find a solution that would integrate tightly into the security ecosystem.

**“We’re stopping a lot of attacks with Cisco Umbrella before they are capable of being weaponized at the application layer.”**

### Mike Mills

Security Engineer, Farm Credit

## Objective

Farm Credit needed to keep customer data secure while protecting its distributed, highly mobile workforce from web-based threats, no matter where employees use their devices. The organization wanted a holistic secure web gateway solution that has robust capabilities, can mitigate threats earlier in their lifecycle, and integrate seamlessly into their environment.

## Solution

[Cisco Umbrella](#)

[Cisco Threat Response](#)

[Cisco AMP for Endpoints](#)

[Cisco Threat Grid](#)

[Cisco Email Security](#)

[Cisco Firepower 4100 Series](#)

## Impact

- Gained ability to respond to threats faster and more holistically
- Improved visibility into the entire chain of security events
- Blocked threats earlier in the attack lifecycle before they impacted end users
- Saw a 799% increase in security blocks and an even larger increase in phishing blocks in just 30 days

## The Solution

### A holistic solution that leverages integration

Farm Credit had a good relationship with Cisco and understood its technologies. In addition to Cloud Web Security, Mills' team had integrated several Cisco solutions – AMP for Endpoints, Threat Grid, Email Security, and Firepower 4100 – into Cisco Threat Response, which automatically aggregates data and threat intelligence from multiple security tools into a single console to accelerate investigations.

“We are fully integrated with the other Cisco security products,” Mills says. “In fact, Cisco Threat Response gives us that single pane of glass and visibility into the entire chain of events, from beginning to end, regardless of where a threat originates.”

In addition to Cisco Umbrella, the security team evaluated several secure web gateway solutions. “Cisco Umbrella emerged as the clear winner,” Mills says.

“As an existing Cisco customer, we leverage their solutions across the board, from our data center to our workstations,” Mills says. “The ability to extend that into web proxy makes a lot of sense to us. The Threat Response integration is a very compelling component for me.”

Mills also recognized that thanks to capabilities such as malware blocking, sandboxing, and granular application controls, Umbrella's secure web gateway (SWG) would provide Farm Credit a more holistic solution compared to Cloud Web Security (CWS). “For all of its benefits, CWS had limitations,” he says. “Umbrella's secure web gateway is a much more holistic tool.”



**“The level of integration that we have with Umbrella's full proxy and Cisco Threat Response gives us better visibility which has proven to be very valuable.”**

### Mike Mills

Security Engineer, Farm Credit

## The Results

### Blocking threats before they turn into incidents

Since deploying Umbrella, Farm Credit has been able to respond to threats faster and block them before they reach employees. Mills noted that in one 30-day period, Umbrella showed a 799% increase in security blocks and an even larger increase in phishing blocks, with 2,321 malware requests blocked in 24 hours.

“We’re stopping a lot of attacks with Cisco Umbrella before they are capable of being weaponized at the application layer,” Mills says. “We’re blocking tens of thousands of connection attempts on a regular basis. We are certainly blocking more than we were before.”

In addition to providing a first line of defense with its DNS-layer enforcement, wherever employees connect to the internet, Umbrella allows Farm Credit to block nearly 800 applications, block specific file types with just a few clicks to protect sensitive data from being shared, detect hidden threats by decrypting HTTPS traffic, and make security-policy changes faster.

“The level of integration that we have with Umbrella’s full proxy and Cisco Threat Response gives us better visibility which has proven to be very valuable,” Mills says.

Cisco Umbrella’s integration with Threat Grid is another important feature for Mills. Farm Credit was already heavily using Threat Grid to denotate links and attachments through AMP for Endpoints and the Email Security Appliance. “When it does find something that’s threatening, we are automatically blocking those links inside of Umbrella,” Mills explains.

For Farm Credit, Umbrella provided an agile solution for protecting its mobile and remote workforce across locations and devices. The ability to quickly and easily scale off network protection was essential during the COVID-19 pandemic, when almost all of Farm Credit’s workforce had to work from home and internet threats were rapidly evolving. “Being able to protect our association and our customers in an unpredictable world is an essential business goal,” Mills says. “Cisco Umbrella helps us to achieve this goal.”

**“Being able to protect our association and our customers in an unpredictable world is an essential business goal. Cisco Umbrella helps us to achieve this goal.”**

#### Mike Mills

Security Engineer, Farm Credit