ExtraHop

CUSTOMER STORY

BAC CREDOMATIC

BAC Credomatic Meets Compliance Standards, Safeguards Against Ransomware with ExtraHop

Holistic visibility provided one comprehensive view of security landscape

Optimized resources saved time and money

Integration amplified impact and bolstered security posture

Executive Summary

The largest financial institution in Central America, BAC Credomatic, serves more than 4.5 million clients and 200,000 merchants. Founded in 1952, the organization's 22,000 employees operate across Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panama, Grand Cayman, the Bahamas, and in the United States.

THE BEGINNING

Challenge

As the leading provider of consumer financial services in Central America, BAC needed to comply with PCI DSS (Payment Card Industry Data Security Standard) to secure credit and debit card transactions against data theft and fraud. This required a shift from allowing each country to individually establish security practices, to forming a standardized cybersecurity strategy around ExtraHop network detection and response (NDR).

Central America experienced a surge in ransomware attacks in 2022 attributed to Conti and Hive. These attacks further highlighted the need for a strong security posture as more people realized any organization could be a target.

> “The ExtraHop dashboard demonstrates that over the past five months we've had no breaches, which creates a high degree of trust. This is even more important than detecting vulnerabilities. It sends a message to the entire organization: we have a healthy environment, we are committed to a strong cybersecurity posture, and we and our clients can sleep well.”
>
> **Vinicio Chaves Alvarado, Cybersecurity Manager**

THE TRANSFORMATION

Solution

Cybersecurity manager Vinicio Chaves's team focused on building a cybersecurity governance framework. He shares, "We recognized that we had a visibility challenge. A single unharmonized server, one application or a solitary user could create a vulnerability." BAC needed a solution that utilized artificial intelligence and machine learning capabilities to protect the organization against increasingly destructive threats.

"We chose ExtraHop Reveal(x) because it efficiently accelerates the detection of threats with superior visibility across our entire ecosystem," Chaves explains. "ExtraHop allows us to see which servers may be compromised by cryptomining, something that we were unable to do before."

Additionally, the Conti and Hive ransomware attacks in Costa Rica amplified concern among company executives about the potential for a similar event at BAC. ExtraHop enabled Chaves to create a dashboard to show all IOC (indicator of compromise) data for each country, for near real-time threat identification across the company.

Chaves says, "The ExtraHop dashboard demonstrates that over the past five months, we've had no breaches, which creates a high degree of trust. This is even more important than detecting vulnerabilities. It sends a message to the entire organization: we have a healthy environment, we are committed to a strong cybersecurity posture, and we and our clients can sleep well."

THE OUTCOME

Results

Holistic Visibility

Investments in process and technology have no value if they can't be protected. The ability to identify vulnerabilities is key to preempting attacks before they cause damage. In addition, because multiple teams are using ExtraHop—including operations and telecommunications—everyone can easily access the comprehensive security picture.

Optimized Resources

False positives waste valuable resources. Chaves notes, "We used to investigate roughly 5,000 events a month, most of which were false positives." ExtraHop has slashed that number, freeing the team to focus resources in more productive areas.

Efficiencies are also gained by centralizing key processes, thereby allowing BAC to maintain legacy technologies while complying with internal and external requirements.

Integration Amplifies Impact

BAC is capitalizing on integrations enabled by Reveal(x). Integrating ExtraHop with third-party tools gives BAC the ability to not only detect potential malware but to automatically respond and contain threats in real time. Chaves says, "We are taking ExtraHop data to the next level, adding end-user intelligence to automate threat assessment and response."

FIND MORE EXTRAHOP CUSTOMER STORIES AT **EXTRAHOP.COM/ CUSTOMERS/STORIES**

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop
520 Pike Street, Suite 1600
Seattle, WA 98101