



Strengthening trust in banking with intelligence-based Endpoint Security

Industry

Financial Services

Solutions and Services

- Trellix Endpoint Security
- Trellix Endpoint Detection and Response
- Trellix Advanced Threat Defense
- Trellix ePolicy Orchestrator

Benefits

- Achieved security compliance for 99.6% of endpoints
- Enabled isolation of infected device within minutes of detection
- Improved incident response efficiency of SOC team

Customer Profile

AU Small Finance Bank Limited is a scheduled commercial bank, a Fortune India 500 Company, and the largest Small Finance Bank in the country. With 27+ years legacy of being a retail-focused and customer-centric institution, AU has a deep understanding of rural and semi-urban markets, enabling it to build a robust business model facilitating inclusive growth for its investors and customers across India.

AU Small Finance Bank proactively defends against cyberattacks with Trellix

Securing endpoints in the face of ever-expanding cyber threats

In the world of banking, trust is everything. As Manish Sehgal, chief information security officer of AU Small Finance Bank points out, "If somebody is going to share their hard-earned money with us, they have to trust in our ability to keep their information secure."

In the modern digital age with growing amounts of data in the cloud, CISOs like Manish Sehgal must manage an ever-expanding attack surface and implement zero-trust policies that extend not only across the bank's assets but also out to its extended ecosystem of FinTech partners. "We are the custodian of our customers' data, and that means we must ensure effective security controls are being applied wherever that data resides and whenever it is accessed."

With new cyber threats constantly emerging and bad actors relentlessly looking for any weakness in an organization's

defenses, Manish Sehgal employs multiple layers of security. This "defense in depth" strategy has worked well for AU Small Finance Bank by placing security controls at all levels of the enterprise infrastructure, from cloud to endpoints. In fact, over the six years Manish Sehgal has been the CISO, the bank has successfully avoided any data breaches. At the endpoint level, Trellix has played a key role in this success.

"We are the custodian of our customers' data, and that means we must ensure effective security controls are being applied wherever that data resides and whenever it is accessed."

— Manish Sehgal, Chief Information Security Officer, AU Small Finance Bank



CASE STUDY



Bolstering cyber defenses with actionable security intelligence

To ensure its business and customer data are secure, AU Small Finance Bank proactively invests in the most advanced security technologies. When it comes to endpoint security, the bank worked with a global technology consulting firm to evaluate vendors, conducting an extensive market study and several proof-of-concept tests. At the conclusion of this intensive evaluation, Manish Sehgal says, "We identified Trellix as the best choice to meet our endpoint security requirements."

Today, AU Small Finance Bank has deployed Trellix Endpoint Security across the enterprise, spanning tens of thousands of endpoints. The solution incorporates next-generation antivirus protection and data encryption, providing proactive defense against intrusion. Additionally, the bank deployed Trellix Endpoint Detection and Response for AI-guided threat investigation, along with Trellix Advanced Threat Defense to catch zero-day malware and Trellix ePolicy Orchestrator for centralized endpoint security management.

In the event a cyberattack is detected—for example, if someone clicks a link and inadvertently downloads a malicious file—Advanced Threat Defense automatically sandboxes the file and sends an alert to the ePolicy Orchestrator, which is integrated with the bank's security information and event management (SIEM) system. Manish Sehgal explains the Trellix solution provides detailed intelligence to enable his security operations center (SOC) to pinpoint the threat and respond—quickly and effectively.

"Trellix tells us exactly which endpoint is affected, what kind of file was downloaded and the IP address used, so we can isolate that device from our network within minutes," Manish Sehgal says. "Trellix provides us with actionable intelligence that helps our SOC analysts work through the entire process of identification, response, and remediation. Without that intelligence it would be much more difficult and time-consuming for them."

He adds, "Our SOC team needs visibility to know what to monitor. Only then can we apply the right controls and take the appropriate actions when an incident occurs. Trellix provides us with these critical endpoint security capabilities."

"Trellix provides us with actionable intelligence that helps our SOC analysts work through the entire process of identification, response, and remediation."

— Manish Sehgal, Chief Information Security Officer, AU Small Finance Bank



CASE STUDY

Assuring endpoint compliance, customer confidence

"The Trellix solutions are delivering what they are supposed to. We are getting the required results from an endpoint security perspective, and I am quite happy with that."

— Manish Sehgal, Chief Information Security Officer, AU Small Finance Bank

Using the Trellix endpoint security solutions, Manish Sehgal has successfully increased security compliance for the bank's endpoints from around 60% when he came onboard to greater than 90% today. He notes, "I'm proud to say that we are maintaining compliance of 99.6% of our endpoints by securing them with Trellix solutions."

In fact, since deploying Trellix solutions, Manish Sehgal reports that AU Small Finance Bank has had no virus outbreaks or ransomware incidents, and the SOC team has not identified a single indicator of compromise (IOC) in any of the bank's endpoints. "The Trellix solutions are delivering what they are supposed to," Manish Sehgal says. "We are getting the required results from an endpoint security perspective, and I am quite happy with that."

Additionally, the Trellix solutions provide important building blocks for AU Small Finance Bank to implement Extended Detection and Response (XDR) capabilities. "With the advance of mesh security and telemetry feeding data from practically every asset in the enterprise, XDR will be a requirement for every organization," Manish Sehgal suggests. "The intelligence we get from Trellix to correlate data and enable our SOC analysts to take effective decisions are an important part of our journey to XDR."

Ultimately, the security solutions AU Small Finance Bank has put in place further strengthen the trust built with its customers. Manish Sehgal concludes, "When customers see the bank is taking strong measures to ensure their data is secure, they are confident entrusting their money with us."

Trellix

6000 Headquarters Drive
Plano, TX 75024
www.trellix.com

Visit [Trellix.com](https://www.trellix.com) to learn more.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at <https://www.trellix.com>.