

Patria Bank foils cybercrime group with latest security techniques

European bank thwarts targeted APT, complies with new EU data protection regulation, and reduces time on incident response and resolution by 33 percent



Patria Bank S.A. provides banking and other financial services to small-to-medium enterprises, microenterprises, agribusinesses, and retail clients in Romania. Financial services include current and special purpose accounts, capital loans, investment credits, credit lines, domestic and international payments, and foreign exchange transactions, among other offerings.

THE CHALLENGE

Banking was once regarded as a stable, often uneventful profession. That's all changed with the rise of cybercrime. Consider Patria Bank, a regional bank that was one of five financial firms in Romania targeted by the Cobalt Group, which was attempting to hack electronic payment systems. Fortunately for Patria Bank, the cybercriminals tipped their hand and initially attacked a decommissioned server isolated from the rest of the infrastructure.

Realizing Patria Bank would not be so lucky again, IT decided to evaluate alternative security solutions, such as Bitdefender GravityZone Ultra, McAfee Endpoint Security, and Symantec Endpoint Protection. After an in-depth evaluation, GravityZone Ultra emerged as the clear choice for Patria Bank.

Razvan Cioc, Chief Information Security Officer, Patria Bank, states, "We were impressed with the sophistication and automation of GravityZone's endpoint detection and response. GravityZone's cloud console was extremely user friendly and provided in-depth visibility and detailed reporting across our infrastructure. Compared to the other solutions, GravityZone Ultra was best value for the money."

Another factor in the bank's choice of GravityZone was the European Union General Data Protection Regulation (GDPR), a new law that imposes stiff fines when companies experience privacy or data breaches.

"GravityZone Ultra provides the best protection against data breaches, which provides us with the confidence to comply with the EU's GDPR law," says Cioc. "Data breaches can cost organizations in fines up to four percent of their total revenue or 20 million euros depending on which is greater. That's not something a lot of businesses can survive."

THE SOLUTION

Patria Bank depends on Bitdefender GravityZone Ultra to provide endpoint detection and response (EDR) capabilities to 1,100 Windows desktops and laptops, Windows servers, and VMware ESXi and Microsoft Hyper-V virtual servers.

Industry

Financial Services

Headquarters

Bucharest, Romania

Employees

800 (IT staff, 20)

Results

- Spend eight hours on incident responses per week versus 12 hours before
- Thwarts advanced persistent threats
- Completes security investigations 33 percent faster
- Achieves compliance with EU GDPR

The bank has been pleased with Bitdefender Professional Services, which provided installation and configuration of GravityZone, and Bitdefender Premium Support.

"Our security and IT specialists have been extremely impressed with the fast response and deep knowledge of Bitdefender's services and customer support teams," comments Cioc. "Bitdefender's culture is very customer-centric, which shows up in virtually every interaction we have with them."

THE RESULTS

A top priority for Patria Bank is protecting its assets and data from increasingly aggressive advanced persistent threat (APT) groups and other organized crime entities.

"GravityZone Ultra's EDR capabilities help us maintain a nimble, agile security posture capable of rapid response to a spectrum of attacks, including signature-based and behavior-based threats," Cioc says. "Since deploying GravityZone, we prevented any outbreaks from infiltrating our infrastructure."

With GravityZone's automation and intelligence, Cioc estimates the security team spends about eight hours a week on incident response and resolution versus 12 hours before—a 33 percent reduction.

"We're a small bank with a small security team," Cioc reflects. "GravityZone Ultra helps extend our security team's capabilities by automating the blocking of threats. When we need to get involved, we're able to complete security investigations about 33 percent faster than before."

He concludes, "With GravityZone, we've freed time for additional vulnerability management activities, such as system hardening, performance management, and perimeter security. These efforts provide us with yet another layer of security."

Cioc appreciates that GravityZone differentiates between threats that must be immediately blocked versus those that require alerts to security analysts for investigation.

"GravityZone enables security analysts to easily pinpoint behavior of certain machines at various points in time instead of reverse engineering incidents, which takes more time and is less effective," Cioc says.

"GravityZone Ultra's EDR capabilities help us maintain a nimble, agile security posture capable of rapid response to a spectrum of attacks, including signature-based and behavior-based threats."

Razvan Cioc, Chief Information Security Officer, Patria Bank

Bitdefender Footprint

- GravityZone Ultra

IT Environment

- Microsoft Hyper-V
- VMware ESXi

Operating Systems

- Microsoft Windows