How IT First Responder went beyond next-gen security

IT First Responder, a Sydney based managed services provider (MSP) that delivers and manages security and IT services to medium to small businesses across Australia, had a problem.

The company sought to replace its cyber security application with technology beyond traditional anti-virus and even next generation anti-virus, capable of delivering the levels of protection their customers need.

“The threats are deeply serious today,” said Dan Boufarhat, Director of IT First Responder. “Every 10 seconds another business is infected with ransomware somewhere in the world.

“We knew we needed to move beyond traditional security products to protect our customers. Working from home has changed forever the way in which businesses use devices, and they are often wide open to hackers and malware.”

“No longer are employees behind the corporate firewall or VPN, they are directly connecting to cloud applications all day, every day. They are more exposed than they have ever been, and attackers are far more sophisticated than they were only 12 or 18 months ago.”

IT First Responder’s management team spent months investigating the ‘traditional’ vendors and realised they were essentially hitting their heads against a brick wall.

“Once we drilled down and bypassed the marketing hype, we discovered that traditional vendors deliver traditional products that stop traditional attacks. We needed to protect our customers from zero day, never-before-seen and even supply chain attacks,” said Boufarhat.

The SolarWinds Orion breach over last Christmas, and most recently the Kaseya ransomware attack were an eye-opener for the company, and for most other MSPs.

They were instantly aware of an urgent need to ensure their business was protected from all types of cyber attack. Only then could they protect their customers adequately against these attacks and the evolving more sophisticated, as well as targeted, new-wave generation attacks.

“When we discovered Comodo, they were establishing their Australia and New Zealand operations. I met Greg Wyman, Regional VP for Australia and New Zealand, and was highly impressed with the Comodo story,” said Boufarhat.

“Being cynical, I needed to validate the concepts behind Comodo, and our team did an extensive and extended evaluation. Happily we have now standardised on Comodo.”

The three key reasons for their decision were:

1) Comodo’s auto-containment technology stops all unknown and potentially malicious files from being able to write to disk, COM interface and the registry – it actually stops breaches before the breach occurs.

2) The fact that over nine layers of security are built into their standard platform - this dramatically reduces the attack surface and closes the gaps that other products can’t detect, or they charge extra.

3) Ease of integrating Comodo into IT First Responder’s PSA solution, Synchro. Now most of the processes that we require are fully automated.

The MSP has rolled Comodo out to its entire customer base, which includes legal firms, construction businesses, real estate agents and all sizes of medium to small businesses.

“The fact that no-one even noticed the migration is an endorsement to just how invisible and non-disruptive a security platform should be to the day-to-day operations of our customers,” said Boufarhat.”

“Now we are exploring Comodo SOC-as-a-Platform extension, which delivers 24/7 threat hunting across endpoints and optional M365 and network extensions that move Comodo beyond the endpoints to the network to stop malware, hackers and ransomware from infecting our customers."

Media contacts

Greg Wyman, Comodo

greg.wyman@comodosecurity.com.au

0402 259 359

Dan Boufarhat, Director, IT First Responder

dan@itfr.com.au

61 2 8003 4009

Contacts

David Frost
(02) 7903 9567
mailto: david.frost@prdeadlines.com