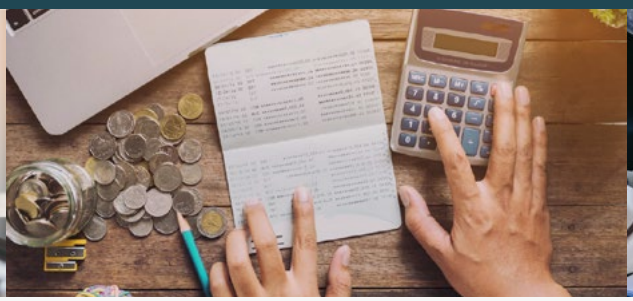
Customer Case Study


SuperConcepts Helps Clients Plan and Protect Their Financial Futures

SuperConcepts helps Australians plan for retirement as the country's largest provider of administrative services for self-managed superannuation funds (SMSFs). An SMSF is a self-managed version of the superannuation fund that's compulsory for Australian workers, similar to a hybrid of Social Security benefits and a 401(k) in the United States. For more than 30 years, SuperConcepts has supported accounting firms, financial advisers, and individuals as they navigate the complexities of this unique retirement savings vehicle.

SuperConcepts' business rests on two SMSF-related strategic pillars. One being SMSF administration services which ensures funds meet important tax and legal compliance obligations. The other, SuperMate, is a specialist SMSF accounting software for practitioners.

Because SMSFs receive at least 9.5% of their owners' salaries each year to build long-term savings, security is critical for data protection, customer trust, and peace of mind for investors, financial professionals, and the SuperConcepts security team. "We deal with bank statements, tax returns, share trading forms, and fund details, so we need to be very careful," said Jim Robinson, CIO.

In 2021, Robinson and his team of 20 were seeing more sophisticated email threats getting past Microsoft 365 and their secure email gateway. "One of the main attack vectors in financial services is email. We needed to find smart ways to protect our supply chain and our clients from email attacks," Robinson said.

SuperConcepts

Industry
Financial Services

Location
Sydney, Australia

Protected Mailboxes
830+

Number of Employees
650+

Phishing Targets Financial Services

Financial services was the most targeted industry for phishing attacks in Q4 2021, accounting for 23.2% of all phishing incidents. December 2021 saw the most phishing attacks ever recorded by the APWG, capping off a year in which phishing attacks tripled over 2020 rates. Between December 2021 and May 2022, phishing emails comprised 83% of the hundreds of attacks on SuperConcepts that Abnormal detected and stopped.

"We were looking to move to Mimecast, which was pretty cool. Then Abnormal came along and blew it out of the water with better functionality and a smarter way of doing things."

Jim Robinson
CIO

Customer Case Study

10

security team hours saved per month

21

compromised vendor email domains identified by VendorBase™

Zero

compromised accounts in 6 months

Identifying an API-Based Solution to Automate Email Security and Stop Attacks

Despite security awareness training, multifactor login authentication, and a SEG layered onto Microsoft 365, Robinson knew that the company was at increased risk of receiving sophisticated email attacks.

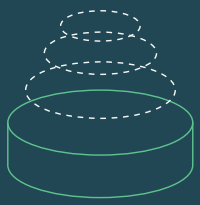
"We had this problem that was 80% fixed, but we were still getting attacks in our inboxes," he said. "There's an increased focus on cybersecurity in Australia and particularly in the financial services industry, and there have been a number of fines handed down to companies that didn't do enough to protect their client data." To prevent an email-related security incident, SuperConcepts' team manually remediated each threat that made it past their SEG.

"We would analyze the email, and if it was malicious, we'd run reports to see how many users had received it," Robinson said. "We'd contact those users and ask if they clicked on the message. Then we'd need to triage the email, potentially change their password, and monitor their account for suspicious activity. You could easily spend an afternoon on this type of thing." Robinson knew this was not scalable and he needed a new approach to address these sophisticated threats and reduce his team's manual workload.

Protecting the Entire SuperConcepts Email Ecosystem

After learning what Abnormal offers, Robinson started with the personalized risk assessment. "The integration of Abnormal with Microsoft 365 was literally the click of a button. Abnormal started ingesting data right away and learning our environment," he said. "During the proof of value, Abnormal flagged a number of VIP spear phishing attacks reaching our CFO and CEO."

Because Abnormal VendorBase™ monitors clients' vendor activity and accounts for indicators of compromise, Abnormal also found a third-party attack in progress. "The attacker used an existing email chain between one of our employees and one of our vendors to send malware." According to Robinson, after he asked the Abnormal team to explain the signals used to identify the attack, "I was like, 'we have to have it.' That was someone piggybacking on a legitimate email chain from a legitimate company that we have a history of doing business with. No secure email gateway can pick that up."



Federated Data Across Employees & Vendors

The data that SuperConcepts stores and its vendor ecosystem make it a target for financial supply chain compromise. VendorBase monitors SuperConcepts' vendors for compromised accounts and socially-engineered attacks sent from them.

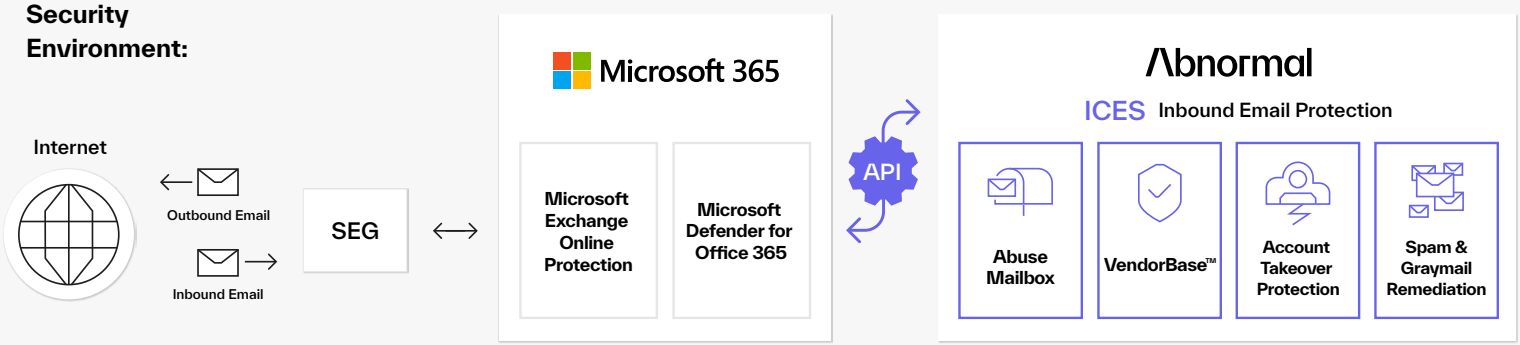
As a result, Abnormal detected the hijacking of a conversation between a SuperConcepts staffer and a company whose mailbox had been compromised and blocked an attack that could have cost the company hundreds of thousands of dollars.

$422K

value of just one business email compromise attack detected and blocked by the Abnormal deep learning attack model.

Customer Case Study

Security Environment:



Abnormal Behavioral Threat Detection Auto-Remediates Threats to Free Up Time

SuperConcepts has found incredible value in Abnormal's behavioral threat detection solution. Robinson shared, "I'm really happy with the way it's going. It picked up 1,000+ attacks that bypassed our SEG. I really like the account compromise feature that autodetects threats and locks users out of those mailboxes. That was the real cherry on top for me, because it gives me peace of mind that not only is Abnormal blocking all the attacks, but also that if one actually succeeded, Abnormal auto-remediates that mailbox." Abnormal's AI solution, combined with VendorBase continuous monitoring, provides comprehensive email protection in real time.

With Abnormal handling threat detection, blocking, and remediation, Robinson's cybersecurity, risk, and compliance team can address other security topics. "Now, we don't have to be so worried about email security," he said. "That allows us to talk about other things like privacy and data, confidentiality, and some of the other issues that were taking a bit of a backseat to 'don't click on the email.'"

SuperConcepts and Its Customers are Investing and Prepared for the Future

Since Abnormal blocks advanced threats against SuperConcepts, employees and executives can focus on the future, growing their software and administrative service businesses to help Australians build their retirement funds. "Protecting our customers is the bottom line," Robinson said. "I'm sleeping quite peacefully now, knowing that none of that spear phishing stuff is getting through and our email ecosystem is secure."

Customer Support Tier

Silver

"Abnormal solves a problem that other software is unable to address when it comes to advanced email threats like VIP spear phishing. Abnormal's modern approach with behavioral threat intelligence brings the trust back into email communication."

Jim Robinson
CIO

abnormalsecurity.com →