



CrowdStrike Customer Case Study



INFOCEPTS

## Global Data Analytics Company Builds Brand Reputation and “Bulletproof” Security with CrowdStrike

InfoCepts is a global leader of end-to-end data and analytics solutions with nearly 20 years' experience. The company's core aim is helping customers make smart, data-driven decisions. Underpinning that vision is ensuring customers, as well as their and InfoCepts' data, are protected.

“What keeps me awake at night is data theft,” said Rajendra “Raj” Jodhpurkar, global CIO at InfoCepts.

InfoCepts works with large organizations in sectors such as retail, banking and finance, life sciences, and healthcare, and has a duty of care to protect customers when handling their data. For instance, some customers want their data hosted inside the InfoCepts IT environment. Here, the company is extremely careful and watchful about data security. However, while the business had established a robust overall security infrastructure that includes an antivirus product, it felt endpoint protection could be improved. The company brought in an external security assessment adviser to identify vulnerabilities and recommend how to strengthen its information security posture.

### City-Specific Malware Strike Influences Security Improvements

Approximately 25% of InfoCepts' staff work offsite when advising and supporting customers, widening the potential attack surface. This was exacerbated during the COVID-19 pandemic and lockdown when staff were forced to work from home and outside the company's protected environment.

Jodhpurkar and his staff did not know what sort of software was running on home devices and could not sufficiently protect them. Lockdown or not, InfoCepts has over 1,200 staff located across 70 Indian cities and in the Far East and North America.

InfoCepts wanted a solution that was able to detect any kind of suspicious activity such as ransomware or malware and stop it in its tracks. InfoCepts evaluated several solutions but only one — CrowdStrike — stood out from the rest.

Even before any contract was signed, CrowdStrike ran a pilot to protect InfoCepts against the Nagpur attack. “What impressed us was its responsiveness,” said Jodhpurkar. “CrowdStrike had installed agents on many of our endpoints and within two days was getting alerts about potential threats. This pre-purchase pilot was so good, we fell in love with it, and it showed CrowdStrike was the right partner for us.”

### INDUSTRY

Technology

### LOCATION/HQ

Washington, D.C.

### CHALLENGES

- Ensuring customers and their data are protected
- Enhancing reputation for safely managing customer data
- Making managing security less time- and resource-constrained

### SOLUTION

InfoCepts, a global leader of end-to-end data and analytics solutions, is using CrowdStrike Falcon Complete™ to reinforce brand reputation, ensure the safety of customer data and protect 1,500 endpoints and employees located across India and around the world.

### LINKS

[InfoCepts](#)

[LinkedIn](#)

“CrowdStrike has improved security at InfoCepts 100%. This is because of the visibility CrowdStrike brings, the clarity over software running on endpoints, detecting and protecting against malware and enabling us to manage security effectively. CrowdStrike puts us back in control.”

### Rajendra (Raj) Jodhpurkar

Global CIO  
InfoCepts



## CrowdStrike Customer Case Study



### CrowdStrike is “Bulletproof”

Within just two weeks, InfoCepts had deployed CrowdStrike Falcon Complete™ managed detection and response (MDR) to protect against breaches on endpoints, workloads and identities, as well as provide threat hunting, monitoring and remediation, backed by the CrowdStrike Breach Prevention Warranty. Falcon Complete is protecting 1,500 endpoints globally, comprising laptops, iPads, 22 servers and 250 virtual machines hosted on AWS and Azure clouds.

One of the advantages of CrowdStrike is minimal impact on users and endpoint performance. “The moment you put any agent like antivirus on a device, users hate it because it slows down the machine,” said Jodhpurkar. “CrowdStrike does not do that, and users hardly know their laptops are being monitored. So far, we have not had any complaints. In fact, staff seem to have a sixth sense that they are safe even when there is an incident. CrowdStrike is reporting events and stopping them within minutes. CrowdStrike is bulletproof and users love it.”

Managed from the InfoCepts security operations center, the CrowdStrike dashboard monitors incidents hitting endpoints in real time. CrowdStrike also highlights false positives that improve intelligence. The application enables InfoCepts to see what is happening with a particular endpoint, for example, if software has been installed and whether it is legitimate.

Information security is essential for protecting InfoCepts’ data analytics company, yet because its management requires a lot of expertise, time and investment to master, the company gave that responsibility to CrowdStrike. “I want to make sure that my customers and their data are secure,” said Jodhpurkar. “So, I rely on partners like CrowdStrike — best in class — to help me and the business give that reassurance to our prospects and customers.”

### Security is Improved 100%

“CrowdStrike has improved security at InfoCepts 100%,” said Jodhpurkar. “This is because of the visibility CrowdStrike brings, the clarity over software running on endpoints, detecting and protecting against malware and enabling us to manage security effectively. CrowdStrike puts us back in control.”

Building trust and reassurance with customers is essential, especially when organizations like banks and hospitals rely on InfoCepts to not only maximize but also protect their data. “Solutions like CrowdStrike are extremely important to our brand reputation,” said Jodhpurkar. “If I put myself in my customers’ shoes and have InfoCepts work on my data, the number one thing I need is assurance the data is secure. We get that and invest heavily in the best security products.”

Jodhpurkar is clear that CrowdStrike instills confidence in InfoCepts’ customers, who know they are coming into an environment with absolutely the best security hygiene. It demonstrates InfoCepts takes an intelligent and researched approach to finding partners like CrowdStrike.

By automating endpoint detection and response, CrowdStrike has increased visibility, improved productivity and significantly lightened the security management burden. “When you have smart software like CrowdStrike, you do not need an army of people,” said Jodhpurkar. “CrowdStrike is doing it all for us and giving clear alerts via the dashboard as well as telling us exactly what needs to happen. And it is precise, and easy to use. In one click we see the endpoint, the users and exactly what is happening. CrowdStrike is extremely efficient and what used to take hours is now done in minutes.”

### RESULTS



Reduces incident response time from hours to minutes



No impact on or reduction to endpoint performance



Improves productivity by reducing demands on IT staff

### ENDPOINTS



### CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response
- Falcon Device Control
- Falcon Discover™ IT hygiene
- Falcon Insight™ endpoint detection and response
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management



CrowdStrike Customer Case Study



Visibility also is critical for InfoCepts' board of directors because it communicates clearly and simply how CrowdStrike protects the organization and customers. "When we talk about security, there are a lot of compliance regulations and laws," said Jodhpurkar. "From that perspective, it is extremely important for the board that we have the right kind of information security for compliance. For example, we have SLAs in contracts that state we must tell customers of an attack within a certain number of days. We are growing at 40% per year and any new prospect wants to understand our security information policy."

Saving money is measured in terms of what would happen without a solution like CrowdStrike and how much it costs to recover from an attack, how much it impacts business operations and how much it damages reputation. "In many ways, cost is not the issue," said Jodhpurkar. "But rather it is the value that CrowdStrike brings to InfoCepts and our customers."

InfoCepts sees its relationship with CrowdStrike as a strategic partnership and has embarked on a journey with CrowdStrike to continually improve and enhance endpoint security. "As we develop our information security platform, we look to partners like CrowdStrike for education and guidance to strengthen our roadmap," said Jodhpurkar. "I want our business, users and customers to be as safe as possible and we are doing that with technologies like CrowdStrike, but also through education. In one sense it is simple: if you go out of your house, you need to remember to lock your door."

## ABOUT CROWDSTRIKE

[CrowdStrike](#) Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

© 2022 CrowdStrike, Inc. All rights reserved.