voices

CrowdStrike Customer Case Study

ctos

CTOS Protects Customer Data, Meets Strict Compliance and Expands Globally with Advanced Security Solution

Established in 1990, CTOS Data Systems (CTOS) is Malaysia's leading credit reporting agency, facilitating credit extensions by empowering individuals and businesses with access to crucial credit information. CTOS delivers a complete portfolio of credit risk management solutions and services and is widely used by Malaysia's banking and financial institutions, insurance and telecommunication companies, large corporations, SMEs, legal firms and statutory bodies. CTOS maintains one of the most comprehensive databases of credit information of over 21 million individuals and 2.3 million companies in Malaysia. More recently, CTOS has launched a new set of consumer services giving individuals access to their own credit report and score, as well as an ongoing fraud protection and credit monitoring service.

Diversification of Geographies, Services and Customers Plus New Compliance Obligations Created a More Complex Security Landscape

As CTOS builds more digital platforms, holds more sensitive information on individuals and businesses, and engages in more diverse interactivity with customers, its security landscape has become more complex. CTOS not only needs to store information securely, but also provide access to information for an increasing number of customers. CTOS has also recently acquired two companies — one in Thailand and one in the Philippines — expanding the agency's geographic coverage.

"Our strategic direction is to become a significant regional player in the digital and credit reporting industry," said Benjamin Lau, General Manager IT, CTOS.

To address its security needs, CTOS had deployed a range of systems and applications that had become increasingly difficult to integrate, manage and keep up-to-date.

As a Malaysian credit reporting agency, CTOS has to comply with the requirements of the Credit Reporting Agencies Act 2010. While CTOS is legally empowered under the Act to collect and process information pertinent to credit evaluation, access to this information is strictly limited and controlled.

However, the Act doesn't stipulate the security compliance required, so CTOS operated under a best-effort model to ensure the security of its data and systems. Since July 2019, when the Malaysian central bank, Bank Negara Malaysia, released its Risk Management in Technology (RMiT) policy, CTOS has complied with a much stricter set of cybersecurity requirements.

INDUSTRY

Financial services

LOCATION/HQ

Kuala Lumpur, Malaysia

CHALLENGES

- Higher-level risk and security compliance required with new central bank policy in force
- Expansion into new countries through acquisition required rapid deployment of new security solutions
- Launch of new products and a much broader customer base changing the security landscape

SOLUTION

Cloud-native CrowdStrike Falcon platform reduces overhead, supports launch of new products and services, and increases customer, end user and core system protection

"When we talk about security, the biggest weak point is the human factor. With CrowdStrike we have more and more information on how the staff in our company behave, so we can design awareness campaigns targeted to change that behavior."

Benjamin Lau Chi Meng
General Manager of IT
CTOS

voices

CrowdStrike Customer Case Study

One of the issues CTOS identified in meeting the RMiT policy was the management of its legacy antivirus solution. The agents running on its devices were difficult and time-consuming to update, and the on-premises server hardware required ongoing maintenance.

"With our previous system, we had six modules, and each of these modules was actually a separate agent, meaning that if we wanted to use all six modules, we needed to push out six different agents to the end device," said Benjamin Lau.

CTOS Achieving Complete Visibility and Control of Endpoints

The rollout of the CrowdStrike Falcon Enterprise™ breach prevention bundle solution — including Falcon Prevent™ next-generation antivirus (NGAV) and Falcon Insight™ endpoint detection and response (EDR) — was completed for 750 devices, reducing administrative overheads, supporting the launch of new products and services, and increasing customer, end user and core system protection for CTOS.

"Because Falcon Insight next-gen antivirus doesn't run on signatures, we see what our users are trying to do. We get the assurance that, based on the Falcon platform dashboard, we have 100% coverage of all of our users' laptops for maximum protection," said Benjamin Lau.

CTOS systems administrators now have complete visibility and control on every file and program that a user is trying to install, ensuring that action can be taken to stop any potential harm from occurring. That safeguards CTOS so it isn't introducing any third-party applications into its environment that might compromise its security or result in the exposure of any important information or data.

CTOS operates a Microsoft Windows Server 2016 and Red Hat Linux server environment, and Windows 10 workstation clients. In addition to CrowdStrike's NGAV and EDR solutions, CTOS is also using Falcon OverWatch™ managed hunting, a 24/7/365 proactive service that combines rich telemetry data — collected and cataloged from millions of endpoints across Crowdstrike's worldwide install base — with a team of experts to see and stop hidden advanced attacks.

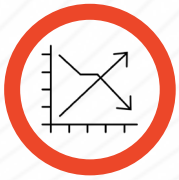
As part of CrowdStrike services, a quarterly business review is conducted with CTOS. This is a Q&A session, conducted by CrowdStrike's technical account manager, that provides an update on everything that has taken place, and been actioned and observed, over the previous three months. The session also provides advice and guidance on best practices for CrowdStrike's Falcon tools, giving the CTOS team a benchmark to aim for with its security measures.

Meeting Industry Compliance Obligations, Supporting International Expansion, Improving Internal Security Culture and Accelerating the Launch of New Services

The CrowdStrike solution has supported CTOS's successful expansion into new countries outside of Malaysia.

"Because the Falcon platform is cloud-based, there is no server to install or maintain, and the solution runs on a single, lightweight agent. That's making it much easier and faster to deploy and manage providing visibility of the endpoints, this fits into the business direction for regional expansion," said Benjamin Lau.

RESULTS



Reduced risk, increased visibility and remote management

Improved compliance

Accelerated detection and remediation limiting attacks

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Enterprise™ breach prevention bundle, including:
  - Falcon Prevent™ NGAV
  - Falcon Insight™ EDR
  - Falcon OverWatch managed threat hunting
  - Falcon for Mobile™ EDR
  - Falcon Express Support
  - CrowdStrike Services

voices

CrowdStrike Customer Case Study

The speed and effectiveness of security countermeasures are also key benefits.

"I'm glad to say we have the Falcon OverWatch service, where we can quickly detect and prevent possible attacks. A lateral movement attack is very hard to detect for legacy antivirus, but with the Falcon platform in place, we get the notification within seconds so we can take further action," said the Senior Systems Administrator, CTOS.

The problem is that with a conventional on-premises solution, it's possible that a lateral attack may stop whatever security agents are running on the device before they can alert the business or help to prevent the attack, or prevent the IT team from accessing the server to rectify any issues. With the Falcon platform operating as a cloud-based solution, this sort of lateral attack can be detected, and action taken to minimize the damage and rectify the issue.

"One of the plus points about the Falcon OverWatch service is that it not only gives us insights, but it also gives us the recommended steps on what we should do to prevent the attack," said Benjamin Lau.

"Technically, with the Falcon platform, we have less things to do. For example, if one of our laptops was being compromised, in the past we would need to hunt down that particular laptop and then physically take control. Worst case, you go into your core switch and pull the plug. Now with Falcon Insight EDR, we don't have to hunt it down, and it doesn't matter where it is, because we can remotely contain that particular laptop with the click of a button. Because it is already contained, it gives us some breathing space and we don't have to rush to fix the problem."

Preventing staff from downloading potentially dangerous third-party files and applications, then blocking network access for their devices if they persist, has also helped to change the entire culture of the company by improving the security awareness of all staff.

"When we talk about security, the biggest weak point is the human factor. With CrowdStrike we have more and more information on how the staff in our company behave, so we can design awareness campaigns targeted to change that behavior," said Benjamin Lau.

Most importantly, with the Falcon platform implemented across the organization, CTOS is meeting the risk and security compliance requirements under the central bank's RMiT policy, which allows CTOS to provide services to Malaysia's banking and finance organizations. CTOS is also able to develop and launch new services more quickly, knowing that the security is in place to support them, without having to configure and deploy new security infrastructure.