



# CBOSS™ Ensures Secure Payment Processing with Trend Micro™ Deep Security in VMware™ NSX® Environment

**Website**

[www.cbooss.com](http://www.cbooss.com)

**Region**

Global

**Sector**

Information Technology, Financial Services

**Partner**

Rolta AdvizeX

**Trend Micro Solutions**

- Deep Security
- Smart Protection Suite
- Hosted Email Security

**IT Environment**

VMware NSX at secondary data center

**Business Benefits**

- Saves time for the IT security team
- Ensures regulatory compliance
- Closes security gaps
- Uses deep insight to ensure a proactive security posture

Organization builds security-first into the fabric of organization

## OVERVIEW

As a global payment processing service and online payment gateway, Ohio-based CBOSS is responsible for protecting sensitive customer information held by thousands of clients. To handle one-time payments, recurring payments, and bill presentment along with related analytics, CBOSS is integrated with many entities. It is connected with major banks and with major North American payment gateways such as PayPal, First Data, and CardConnect.

As companies process more payments through mobile devices and other channels, CBOSS expects their business to grow rapidly. Government agencies also value CBOSS' services, including a U.S. state that uses CBOSS to process the payments of license plate renewals.

In addition, CBOSS helps hospitals and banks meet stringent regulatory requirements. Its certifications include PCI DSS, Statement on Standards for Attestation Engagements (SSAE) Type 1 and 2, and International Organization for Standardization (ISO 27001:2013). It also aligns with industry-specific regulations from the Federal Financial Institutions Examination Council (FFIEC), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, and various U.S. states privacy regulations.

## CHALLENGES

While compliance plays an important role at CBOSS, the real emphasis is on security. "At CBOSS, security is built into the fabric of our organization. We focus on security first, knowing compliance will come as a byproduct," said Mo Faisal, Chief Information Security Officer and Director of IT Operations, Security and Compliance at CBOSS.



“Everything that flows through NSX is inspected first by Deep Security. The first gate is NSX and the second gate is Deep Security, which means we see things happening before the traffic hits the servers.”

Mo Faisal,  
Chief Information Security Officer, CBOSS

## CHALLENGES *Continued*

Day-to-day security challenges run high at CBOSS, where our employees focus on managing two data centers in a secure and compliant manner while processing billions of dollars annually. The company's high-profile government clients are targets for nation states around the world whose sophisticated methods include denial of service (DoS) attacks, zero-day attacks, and advanced persistent threats (APTs). Daily priorities at CBOSS include malware detection, patching, change management, packet analysis, log reviews, network segregation, and two-factor authentication.

Recently, CBOSS deployed VMware™ NSX® at the secondary site with help from Rolta AdvizeX, a systems integrator. NSX ensures an agile environment for onboarding and isolating new clients that CBOSS couldn't achieve in a hardware-defined environment. To benefit from this agility, CBOSS must secure logical segments just as quickly as it creates them. They also required advanced security controls to further support the protection provided by NSX.

## WHY TREND MICRO

With NSX, an effective security solution must be able to respond to the traffic flow on a VXLAN rather than a traditional VLAN. When they decided to go with Software Defined Networking, they looked for a security partner who could run with NSX in a fluid fashion. After looking at NSX integration capabilities from several major security vendors, CBOSS selected Trend Micro™ Deep Security, a solution that tightly integrates with VMware NSX to automatically protect new virtual machines.

CBOSS had strong reasons to consider Trend Micro, including the endorsement of Rolta AdvizeX and their own positive experience with Trend Micro Enterprise Security Suite. Since 2011, the company has relied on the integrated Security Suite to protect email and web gateways, endpoints, file servers, and mail servers. To see how NSX integration worked in Deep Security, Faisal requested a demo. “In one hour, the Trend Micro representative showed me how easy it was to deploy Deep Security. Demos from other security providers we considered were not as appealing,” said Faisal.

In addition, Rolta AdvizeX demonstrated for CBOSS how they use Deep Security, and Faisal used the separate data center to test some features. “I liked the fact that Deep Security was unified and believed it was the best solution for CBOSS based on what we needed to achieve,” he added.

## SOLUTION

With Deep Security, Faisal gained the unified solution he needed to protect CBOSS clients and save time for the security operations team. “I think of Deep Security as Unified Threat Management. Everything is built into one solution – web application firewall, file integrity monitoring, malware detection, web reputation, intrusion prevention, and intrusion detection systems (IPS/IDS), a syslog server,” said Faisal. “Every day, my team logs into one application where they can see what is happening throughout the data center and then go deeper to take appropriate actions.”

What impressed Faisal was that IPS/IDS in Deep Security goes beyond the network interface to inspect everything that passes through NSX. “The first gate is NSX and the second gate is Deep Security, which means we see things happening before the traffic hits the servers. As its name suggests, Deep Security works at a deeper level within the network. It provides more protection than isolated pieces running here and there,” said Faisal. The virtual patching feature of IPS/IDS is particularly valuable. “We don't have to immediately patch the system, because Deep Security provides a temporary shield to protect us until we have sufficient time to test and deploy the patch,” he added.

“Deep Security is built for modern data centers like ours that need a unified solution with complete visibility into the network. Trend Micro will be able to process everything we have without breaking a sweat.”

Mo Faisal,  
Chief Information Security Officer, CBOSS

## RESULTS

Faisal doesn't just believe Deep Security is doing a good job of preventing breaches, he proved it with a penetration testing exercise. “We hired ‘white hat hackers’ to try to break our applications where Deep Security was running with full control of the system. The professionals confirmed that Deep Security is a good solution that does what it claims,” Faisal said. “Deep Security finds all the vulnerabilities that could potentially be on a given host and customizes the IDS or IPS policy for the virtual machine rather than having one blanket policy for reviewing all packets.”

Unlike many organizations that see packet-by-packet analysis and log analysis as post-breach activities, CBOSS seeks to prevent breaches with real-time analysis of everything flowing through the network. “When I used to be a PCI DSS auditor, I saw the loopholes and the IT teams that were swamped with so many things that they weren't paying attention. Deep Security allows us to be proactive about security and put a good vulnerability management framework in place that closes the gaps,” said Faisal.

To accommodate future growth, CBOSS is currently upgrading its primary data center to Deep Security. “Deep Security is built for modern data centers like ours that need a unified solution with complete visibility into the network. Trend Micro will be able to process everything we have without breaking a sweat,” said Faisal.

## WHAT'S NEXT?

Unification continues to be a major goal for CBOSS, when they complete deployment of Deep Security at their primary data center. “Trend Micro has made a good start at fulfilling the needs of a software-defined data center,” said Faisal, who is phasing out traditional solutions to create a DevOps environment. “I see bringing together development teams and security operations teams, unifying under one platform and talking to each other in a unified language to do our jobs better.”

## MORE INFORMATION

For more information, please contact [www.trendmicro.com/datacenter](http://www.trendmicro.com/datacenter)



Securing Your Journey to the Cloud

©2016 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [CS-SuccessStory-CBOSS-120516US]