WITH COLORTOKENS XPROTECT, GMR GROUP AIRPORTS NOW HAVE PROACTIVE PROTECTION FROM INTERNAL & EXTERNAL THREATS

COLORTOKENS

Case Study

GMR group is amongst the top five private airport developers and operators globally.

GMR group, the largest private airport company in India, owns and operates the Indira Gandhi International Airport in Delhi and the Rajiv Gandhi International Airport in Hyderabad. They are also operating and developing the Mactan Cebu International Airport – the second largest airport of Philippines.

Key Benefits

- Protection from Advanced Persistent Threats (APT), malware, and ransomware
- Unified central dashboard for full process visibility and control
- Complete and customizable lock down of critical desktops and servers

The Challenge

The GMR group airports use external agencies to manage over 70% of its daily operations. Thousands of endpoints and critical resources are accessed by employees and third-party contractors with different security clearance levels. This makes most endpoints vulnerable to Advanced Persistent Threats (APT lateral threats), malware, and ransomware.

According to the European Aviation Safety Agency (EASA), aviation systems are bombarded with an average of one thousand attacks per month. Airports are responsible for public safety, and cyber-attacks on aviation systems could lead to flight delays, panic among passengers and staff, or even accidents on the runway. Any serious disruption to airport functions could potentially cause a catastrophe.

With the increasing sophistication of attacks, it's just a matter of time before a vulnerable endpoint gets infected, laterally spreading the malicious code to other critical systems across the network. Realizing the potential danger, the GMR group wanted to secure their endpoints from both external and internal cyberthreats, without additional operational complexity.

The Solution

GMR group deployed ColorTokens Xprotect to protect thousands of endpoints against cyber-attacks at five terminals handling a total capacity of 65 million passengers. All systems, including those that are not part of the airport common network, were secured and configured to a unified dashboard to get full visibility and control of the processes. The centralized dashboard was established in the AOCC (Airport Operations Control Centre) to align the SOPs of the respective Airport functions in case of cyber-attacks.

ColorTokens Xprotect also enabled process-level lockdown of special purpose systems like check-in kiosks, ticket vending machines, point of sale (POS) terminals, and other critical assets. This ensured complete protection from zero-day threats, fileless malware, ransomware, advanced persistent threats (APTs), return-oriented programming (ROP), remote access trojan (RAT), and many more.

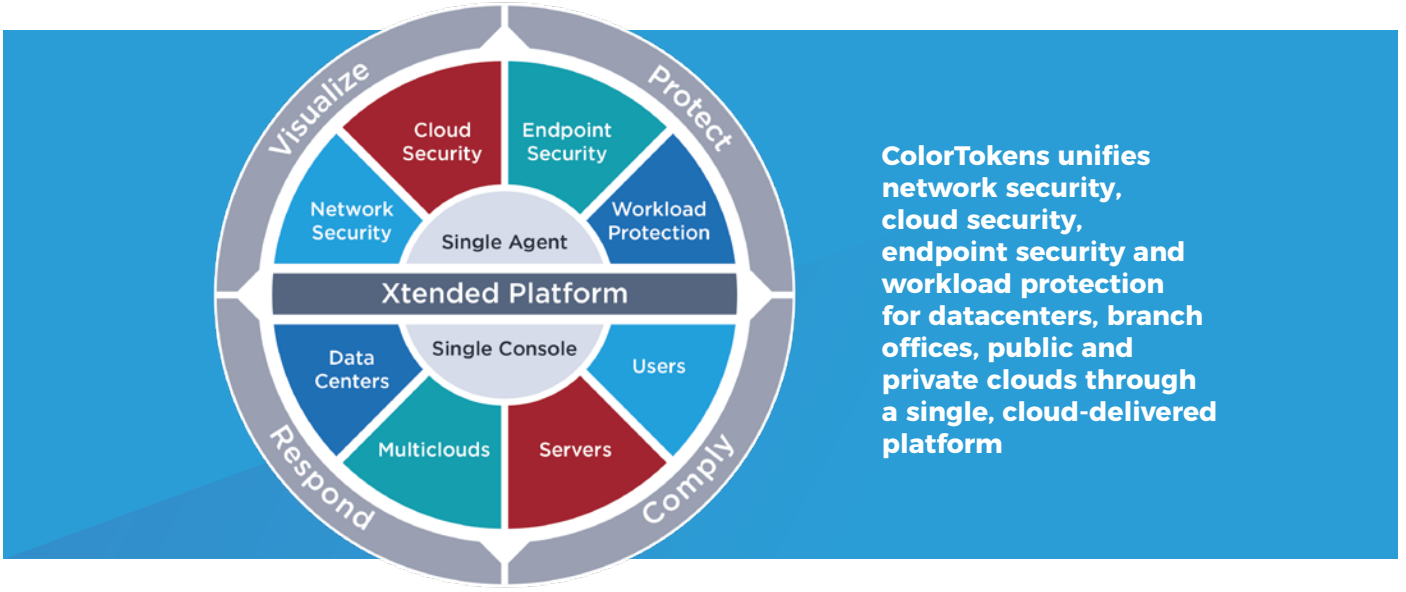
To quickly audit the security of special purpose systems, GMR group can now use ColorTokens Xprotect to download readily available reports such as suspicious file report, blocked processes report, and incident report. ColorTokens Xprotect also eliminated the need for multiple anti-virus tools, signature updates, and patch management. A total of 500+ servers running over 1000 applications were protected using ColorTokens Xprotect.

Systems That Were Protected

- Baggage Handling System (BHS) of Servers and Systems
- Baggage Reconciliation System (BRS)
- Passenger Boarding System
- Visual Docking Guidance System (VDGS)
- Gate Operating System (GOS)
- Fire Detection System (Servers)
- SCADA (Servers)
- Building Management System (BMS)
- Video Management System (VMS)
- Common User Passenger Processing System (CUPPS)
- Common User Self Service
- Airport Operations Control Centre (AOCC)
- Security Operations Control Centre (SOCC)
- Emergency Management Centre (EMC)
- Airside Operations Management Centre
- Airline Ticket Counters
- Point of Sales (POS) – Retailers, F&B
- Ground Handler Systems
- Cargo Systems
- Fire Station
- Maintenance Repair & Overhauling (MRO)
- Back-office Systems
- Car Parking System

ColorTokens Xtended ZeroTrust Platform

Built from the ground up to make zero trust a reality for any enterprise, the ColorTokens Xtended ZeroTrust Platform delivers a refreshing, new-generation of security to provide the following unique benefits:



ColorTokens unifies network security, cloud security, endpoint security and workload protection for datacenters, branch offices, public and private clouds through a single, cloud-delivered platform

Xview for Visualization

Xview – part of the Xtended ZeroTrust Platform™ – provides unified visibility across on-premises and mulitcloud infrastructure, giving a telescopic view into networks, clouds, applications and endpoints. The Xtended Visualization analytics engine integrates with market-leading threat intelligence to investigate suspicious behavior anywhere in the enterprise—while protecting against zero-day threats. Integrated widgets and canned reports enable security teams to achieve faster time-to-compliance for critical mandates like PCI, HIPAA and GDPR. And, the platform's built-in scanner hunts for vulnerabilities in real-time – providing an immediate return on your security investments.

Xshield for Workload Protection

Xshield – part of the Xtended ZeroTrust Platform – enables enterprises to achieve consistent visibility and control of all cloud workloads – regardless of the location or granularity of the instances. Built from the ground up for unrivaled software-defined micro-segmentation, ColorTokens enables the modern enterprise with instant workload visibility, automated and dynamic policy enforcement, and the ability to control any communications to/from the workload instances.

Xprotect for Endpoint Detect and response

Xprotect – part of the Xtended ZeroTrust Platform – provides enterprises with a robust signature-less approach that works at the kernel level to block unauthorized processes on endpoints, servers and legacy/fixed-function systems. Go beyond signature-based security, that blocks only 'known-bad' threats, with powerful whitelisting, prevent unauthorized software execution on endpoints – even with administrator rights and block malicious processes from spawning and infecting legitimate applications.

CIOs and security teams are frustrated with too many complex, reactive point products—and are still vulnerable to sophisticated threats and attacks. ColorTokens proactively secures enterprises through a single, cloud-based Xtended ZeroTrust Platform. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks – all while seamlessly integrating with existing security tools. ColorTokens makes end-to-end zero trust security a reality for any enterprise—covering protection, detection, investigation and response through a single-agent, single-platform architecture. Enterprises can now protect networks, multiclouds, containers, workloads and endpoints with the world's first single agent and platform that unifies network, cloud and endpoint security.

colortokens.com
sales@colortokens.com