CASE STUDY

Hybrid Web Gateway Protection and Ease of Management Fortify Global Security and Facilitate Compliance

By implementing a hybrid solution of McAfee® Web Gateway and McAfee Web Gateway Cloud Service, this global business process management company maintains a comprehensive, 24/7 defense against web-borne malware for its users, whether on premises or off premises.

From the WNS Global Services headquarters in Mumbai, India, Head of Business Technology—Amit Khanna—and his team manage endpoint security, web security, and patch management across more than 40 delivery centers worldwide. Their goal is to enable the company's 30,000+ professionals to work securely wherever they are, and safeguard the data and operations of the company's more-than 200 clients.

The Company Needed a Better Web Gateway Solution, Especially for Off-Premises Users

In the past, one of the biggest challenges for Amit Khanna and his team was protecting those 30,000+ WNS users from inadvertently introducing malware while using the internet. "Our previous web proxy solution could not meet complex requirements without impacting performance and user experience," explains Mr. Khanna.

In addition, WNS Global needed to better protect its consultants and other users when not onsite. "As we began to look for a new web gateway protection solution, we put the ability to provide 24/7 robust protection for both on-premises and off-premises users as a non-negotiable point," notes Mr. Khanna. "Not being able to do so was a show stopper."

Superior, Hybrid Web Gateway that Protects All Users All the Time

WNS had successfully relied on McAfee solutions for almost a decade, starting with antivirus protection and adding other endpoint, data protection, and intrusion prevention solutions (IPS) over time. When looking for a new web gateway solution,

WNS
Extending Your Enterprise

WNS Global Services

Customer profile
Global business process management company.

Industry
BPM

IT environment
20,000+ endpoints in 46 delivery centers across four continents.

Challenges

- Protect sensitive corporate and client data.
- Defend against web-borne malware.
- Comply with PCI, HIPAA, Sarbanes-Oxley, and other regulations.
- Provide efficient, robust security.

the company naturally turned to McAfee, but also researched the other offerings within the Gartner Magic Quadrant.

Ultimately, the company decided to conduct a proof of concept (PoC) on the hybrid McAfee Web Gateway solution: McAfee Web Gateway and McAfee Web Gateway Cloud Service.

> ***"With hybrid McAfee Web gateway, we can administer the same security policies across all users all the time, whether or not they are onsite. Furthermore, the McAfee solution offers incredible granularity in analysis and policy setting. We expect McAfee Web Gateway Protection to meet our needs for many years to come."***
>
> — Amit Khanna, head of business technology, WNS Global Services

After a very successful PoC, Amit and his team purchased and deployed 16 Web Gateway appliances. To protect mobile workers while traveling on and off premises, the team then rolled out the location-aware McAfee Client Proxy across employee devices. When WNS users are inside the corporate network, McAfee Client Proxy directs internet traffic to the appropriate McAfee Web Gateway appliance. When they move outside the firewall, McAfee Client Proxy redirects web traffic from their device to the McAfee Web Gateway Cloud Service, maintaining consistent protection. Users connect transparently to either solution depending on location.

Now, Amit and his team manage all web gateways, for on-premises as well as remote users, from one central console. "With a hybrid McAfee Web gateway solution, we can administer the same security policies across all users all the time, whether or not they are on site," says Amit Khanna. "Furthermore, the McAfee solution offers incredible granularity in analysis and policy setting and uses only five percent of capacity. We expect McAfee Web gateway to meet our needs for many years to come."

Greater Control with Highly Granular, Customizable Web Gateway

With McAfee Web Gateway solution, WNS has much greater control over which sites its end users access and what they can do on those sites. Thanks to the ability to create rules with a very high level of granularity, WNS IT can customize policies to meet wide-ranging departmental and client needs. For example, some policies allow access to specific Citrix sites while others limit actions users can do on certain sites—for instance, disabling chat capability or blocking the ability to post or to stream video on social networking sites.

The Web Gateway conducts SSL scanning on all incoming web packets and matches them against more than 300 out-of-the-box and custom rules established by the WNS IT team. If an end user accesses an allowed site that conforms with security policies but the site is executing a questionable JavaScript in the background, Web Gateway will block the site immediately to ensure that potentially malicious activity is not allowed on the user's device.

Simplifying Management Across Endpoints

Amit Khanna and his team use the McAfee ePolicy Orchestrator® (McAfee ePO™) central console, integrated with Microsoft Active Directory, to manage multiple McAfee endpoint and data protection solutions—McAfee Endpoint Protection Suite, McAfee Endpoint Encryption, McAfee File and Folder Encryption, McAfee Host Intrusion Prevention, and McAfee Host Data Loss Prevention—across the WNS extended enterprise. With McAfee ePO, deploying and updating these solutions is simple. From one screen, administrators have rolled out encryption and other solutions without disrupting end-users.

WNS IS administrators depend daily on McAfee ePO software for regularly scheduled reports as well as on-the-fly queries. Amit's team also uses McAfee ePO software to scan regularly for vulnerabilities, push out security software updates, and perform troubleshooting or remediation activities. On average, the company sees 100 unique threat events each day. Thanks to continually updated threat intelligence from the cloud-based McAfee Global Threat Intelligence service, the vast majority are non-issues. For the few events that aren't, the intuitive McAfee

McAfee solution

- McAfee Client Proxy
- McAfee ePolicy Orchestrator software
- McAfee Endpoint Protection Suite
- McAfee Global Threat Intelligence
- McAfee Endpoint Encryption
- McAfee File and Folder Encryption
- McAfee Host Intrusion Prevention
- McAfee Host Data Loss Prevention
- McAfee Network Security Manager
- McAfee Web Gateway
- McAfee Web Gateway Cloud Service

Results

- Same web security policies applied to all users, on and off premises.
- Increased visibility and easier security management across a global enterprise.
- Easier compliance with PCI, HIPAA, Sarbanes-Oxley, ISO 20072, and other regulations.
- Path forward to continue fortifying threat defense.

ePO dashboards help administrators know whether the event needs immediate attention and enable them to drill down for details.

Increasing Visibility and Facilitating Compliance with McAfee Central Console

In addition to endpoint and data protection solutions, McAfee ePO is also integrated for reporting with McAfee Web Gateway and the company's IPS, McAfee Network Security Platform. As a result, the McAfee ePO console gives Amit's organization and WNS Security Operations Center (SOC) team a consolidated view of risk and compliance across the entire enterprise. This includes up-to-the-minute assessments of at-risk infrastructure based on system vulnerabilities, network defenses, web security threats, and endpoint security levels across the company's more than 20,000 endpoints.

"McAfee ePO software and the integrated McAfee platform have given us instant visibility across our enterprise," says Amit. "We can demonstrate compliance, pass security certifications more easily, and accelerate the audit process. McAfee ePO software is one of our most critical tools."

Future Plans to Fortify Threat Defense

To further strengthen defense across the entire threat lifecycle, WNS is currently conducting a proof of concept of McAfee Endpoint Threat Defense and Response, which rapidly detects, contains, investigates, and helps eliminate advanced threats, such as ransomware. A key component of this solution is McAfee Threat Intelligence Exchange, which combines multiple internal and external threat information sources and instantly shares the data with all of the security solutions that are connected to the McAfee Data Exchange Layer (DXL).

"We continue to partner with McAfee because the company and its products give us superior intelligent security," says Amit Khanna, "Besides being robust and easy to manage, McAfee solutions talk to one another and share pertinent information, which results in actionable intelligence that reduces response time and improves our security posture."

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 2872_0317
MARCH 2017

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com