OPSWAT.

IT Sector Case Study

Critical Infrastructure Protection

EPAM® – Global Services Firm Ensures Secure Remote Access with OPSWAT MetaAccess®

epam

EPAM Systems, Inc. is a leading global provider of digital platform engineering and software development services to hundreds of Fortune 1000 clients. EPAM works with its clients to solve their business-critical challenges through the application of today's most advanced technology solutions.

CHALLENGES

High Volume of Remote / Global Projects and Shift to Work From Home (WFH) Drives Need for Secure Access, While Managing BYOD Security

EPAM Systems is a global leader in the fastest growing segment of the IT industry. From digital transformation programs, to consulting and design, to engineering and managed services, EPAM's globally distributed team of nearly 40,000 employees operate from more than 30 countries, working remotedly from home and from office locations.

Comprehensive Secure Access
for All Remote Workers and Clients

Protected 45,000+ Remote Devices
from Advanced Malware and 3rd Party Application Vulnerabilities

Security & Reliability
helps Meet Necessary Cybersecurity Compliance Requirements

Given the current situation, global security and reliability are a top priority. EPAM needed to adapt to the increasing risks from BYOD and WFH Programs. The critical nature of their clients' businesses requires EPAM to know whether users' devices—third-party contractors, employees' personal, or corporate-owned; on-premises or remote—meet their strict internal compliance requirements before permitting access to their network, central storage, and applications.

EPAM was looking for an integrated security solution for zero trust networks to securely provide access to digital assets placed on-premises, as well as in public and private clouds.

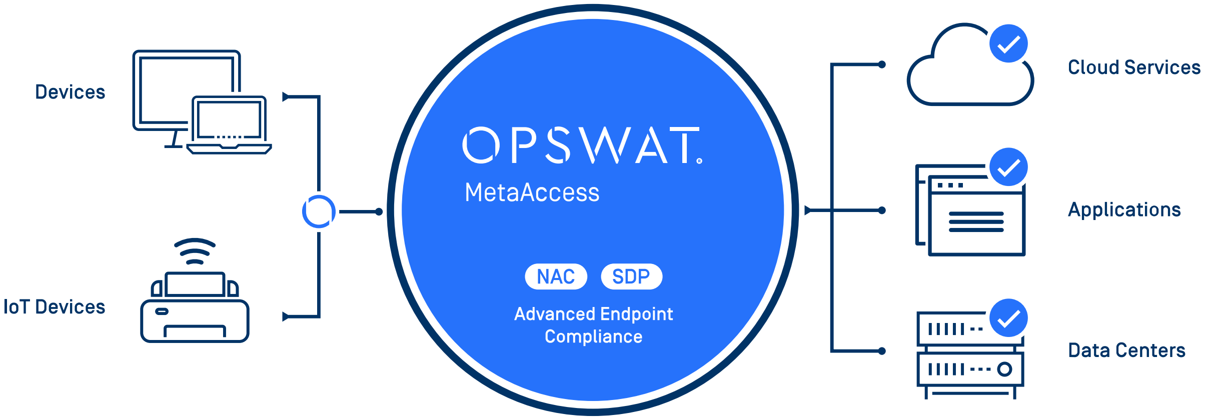
SOLUTION

Device Visibility, Control, and Compliance with MetaAccess

EPAM chose OPSWAT to deliver visibility, control, and compliance of every device across all employees and third-party contractors before accessing their network and applications. With MetaAccess, EPAM can perform the following device Security checks:

- **Vulnerability Checks –** The MetaAccess platform reported devices with unpatched applications or blocked access of devices with critical vulnerabilities of operating systems or 3rd party Applications, such as Adobe, Apple, and others.
- **Compliance Validation –** The MetaAccess platform reported non-compliant devices and configured some policies with self-remediations; for example, the status of antimalware definitions—non-compliant device protection to ensure devices are compliant with existing policies.
- **Unwanted Applications Detection –** MetaAccess continuously detects, blocks and disables unwanted applications such as peer-to-peer applications, browser plugins, and unauthorized remote access tools. This helps EPAM stay compliant, reduce the cyber-attack surface for malware, and reduce data loss prevention (DLP) and copyright infringement risks.
- **Advanced Threat Detection –** MetaAccess continuously scans device memory using more than 20+ anti-malware engines leveraging the MetaDefender® Cloud platform applications. This enables EPAM to ensure the highest rate of detection and block endpoints from malware that was not detected by the device-local anti-malware software.
- **Data Loss Prevention and Portable Media Scanning –** MetaAccess monitors USB and other peripheral media activity of remote workers to prevent data loss or malware originating from USB, SD Cards, and other peripherals.

Miroslav Sklanksy, Head of Information Security Technology at EPAM, said, "Working with OPSWAT was a very positive experience, a true partnership. What contributed to the success was their willingness to focus on what we needed. There was very good communication and a lot of transparency during the whole process. I am confident OPSWAT will address any new requirement in a timely, professional and scalable manner."



MetaAccess enables compliance on devices and secure access to services.

RESULTS

Compliance Across More Than 45,000 Devices

EPAM can validate that all endpoints entering the secured environment—whether BYOD, corporate-owned, or otherwise—are compliant with their security and access control policies, and they're not exposed. EPAM was able to gain device validation, visibility and control into point-to-point and ad hoc user access, including the state of security applications and their vulnerabilities on those devices across nearly 40,000 globally distributed employees, clients, and contractors. "With OPSWAT we get visibility and control—with high confidence—into every remote user's security compliance posture regardless of where they are and what device they're using," Miroslav said. EPAM is also allowing users to use their own devices to securely access the network.

45,000+ devices scanned for Advanced Threats with more than 20 Anti-malware Engines

During the implementation, EPAM leveraged OPSWAT MetaDefender Cloud, a cloud-based threat detection and prevention platform powered by OPSWAT technologies for multi-scanning of files and hash lookups on the controlled devices.

Miroslav Sklansky added, "We are also migrating our system's file storages to a central storage platform, looking for a secure way to verify all the files uploaded are safe and clean for our storage—I was glad to be exposed to the OPSWAT MetaDefender platform. It's a fantastic solution—in the Cloud or On-Prem—to check any file before it's uploaded to our systems. We use both Multi-scanning and Deep CDR (Content Disarm and Reconstruction) technologies to verify that no Malware or vulnerability is entering our central storage that includes our corporate and customer's sensitive information."

EPAM quickly saw the benefit of Advanced Threat Detection with MetaDefender Cloud bundled with their MetaAccess implementation. EPAM's MetaAccess instance was performing hash lookups and file scans using MetaDefender Cloud for more than 50 million files per day during peak times.

EPAM’s security and management team’s experience with OPSWAT’s level of service and the quality of the products exceeded expectations. EPAM has started introducing and recommending OPSWAT solutions to their clients.

Deployment and Customer Support

Despite EPAM’s network complexity, OPSWAT stood up to the challenge and ensured success. The OPSWAT Customer Success team worked shoulder-to-shoulder with the EPAM IT Security team, ensuring that the implementation supported EPAM’s key requirements across different countries, policies, device types, and user experience.

During the proof-of-concept stage, MetaAccess examined an initial 3,000 employee devices in a controlled production environment. Devices were validated against company policies before allowing access to the SDP, triggering automatic actions to ensure security was being enforced and preventing unauthorized access.

> *“Once the agents were deployed, we were quickly able to validate more than 45,000 remote user devices security before accessing our network, with no impact to productivity. OPSWAT’s products are crucial parts of our zero-trust strategy.”*
>
> Miroslav Sklansky
>
> Head of Information Security Technology, EPAM

About OPSWAT

To learn more about OPSWAT Critical Infrastructure Protection solutions, contact us today.