KPIT Technologies

SNAPSHOT

KPIT Embraces Digital Transformation With a Different Approach to Cybersecurity

Industry
Technology

Challenge
When KPIT introduced the concept of the "Smart Enterprise" – a digital transformation initiative consisting of Smart Campus, Smart Collaboration, Smart Business Systems, Smart Insights, Smart Infrastructure, Smart Workforce and Smart Relationships – it realized it needed a more flexible and secure approach to security and network management. Traditional network mapping no longer worked, policy management was inefficient and administration had become a major drain on resources.

Answer
Palo Alto Networks Security Operating Platform with the PA-5020 next-generation firewall, Traps, Panorama, WildFire, AutoFocus and Magnifier

Results

- Enables KPIT to scale, with no additional headcount, through automation
- Reduces malware attack success rate from 50 percent to zero
- Provides one-click insight from a single console
- Minimizes impact on device performance
- Employs user behavior analytics, along with network and endpoint behavior anomaly detection, for a prevention-based approach

Headquartered in Pune, India, KPIT® is a global technology company specializing in providing IT consulting and product engineering services to the automotive and transportation, manufacturing, life science, and energy and utilities industries. The company employs more than 12,000 professionals working at the forefront of technologies and processes to help global corporations become more productive, integrated and innovative.

As a company built on the knowledge of its workforce and the development of intellectual property, KPIT needs prevention-based technology to avoid possible cyberattacks and ensure 100 percent availability and security of its own infrastructure and business applications as well as those of its customers. For the last two decades, KPIT had a security infrastructure based on a standard firewall, intrusion detection and prevention technologies, web content filtering, and traditional endpoint protection products.

However, as the company developed native cloud applications, implemented IoT technologies and deployed mobile technologies to allow employees to work from any device or network, it decided to revamp its strategy and introduced its "Smart Enterprise" concept. At this time, it realized the need for a more flexible, prevention-based approach to security, network and endpoint management.

"It was a significant transition, embracing the idea of a smart workforce and smart, software-defined infrastructure running multiple new digital applications," explains Mandar Marulkar, chief digital officer for KPIT. "We went from having a 70-30 split between PCs and laptops to 30-70, while also moving lots of applications to the cloud and introducing initiatives such as BYOD. Mobility is at the heart of our new strategic approach to working."

The new approach of building native cloud applications and moving some critical workloads to a public cloud created a few challenges in managing secure access to these applications: some SaaS-based applications request dynamic IP addresses, and BYOD and mobility devices increased the risk of malware on endpoints from open, unmanaged networks. Ever-increasing vulnerabilities from packaged and open source applications further increased the risk of devices, data and applications being exposed to security breaches. Traditional network mapping no longer worked, policy management was inefficient and administration had become a major drain on resources.

"We needed more robust and automated security management that would reduce dependency on human intervention and proactively protect against malware and ransomware," adds Marulkar. "With increased mobility and many people working from home, devices are exposed to threats that can infect our

> "We can see on the Panorama console that we have proactively blocked a huge amount of malware – there hasn't been a single instance globally, which is quite an achievement. The biggest benefit is the simplicity of the platform approach. We didn't have to invest everything on day one. Instead, we were able to evolve the security platform with cloud-delivered services. Palo Alto Networks also provides agility, meaning our rollout cycles have decreased from six weeks to just two days."
>
> **Mandar Marulkar** | chief digital officer | *KPIT*

network. What we wanted was a comprehensive platform that would cover everything from endpoints to the network, that went beyond just using signature recognition."

KPIT set out to find a partner that could flexibly secure more than 8,000 endpoints in countries around the world, ensuring the safety of its business-critical data and intellectual property. After a comprehensive evaluation of security vendors, KPIT chose Palo Alto Networks®, first deploying the PA-5020 next-generation firewall, and then adding multiple integrated subscriptions and services that make up the Security Operating Platform. Traps™ advanced endpoint protection from Palo Alto Networks helps KPIT protect endpoints against advanced malware attacks, such as ransomware, as well as mitigate risks and reduce application vulnerabilities from endpoint, application and data exploits.

Magnifier™ behavioral analytics enables KPIT to quickly identify and prevent the stealthiest network threats. By analyzing rich network, endpoint and cloud data with machine learning, Magnifier accurately identifies targeted attacks, malicious insiders and malware. As such, security analysts can rapidly investigate threats and leverage the Security Operating Platform to block attacks before any damage is done.

To simplify, streamline and consolidate its core tasks and capabilities, KPIT turned to Panorama™ network security management. Centralized management enables KPIT to view its firewall traffic, manage all aspects of device configuration, more easily push global policies, and generate reports on traffic patterns and security incidents, all from a single console.

KPIT also needed to better understand the threats it was facing, particularly those requiring immediate action, so it selected AutoFocus™ contextual threat intelligence service to accelerate its analysis, correlation and prevention workflows. Unique, targeted attacks are automatically prioritized so KPIT can respond to critical attacks more quickly and without the need for additional IT security resources.

Completing KPIT's comprehensive security deployment is WildFire® cloud-based threat analysis service, which features the most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. This gives KPIT a unique, multi-technique approach that combines dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.

"Palo Alto Networks provided the most comprehensive security and network management portfolio, which we were able to seamlessly deploy in just a matter of weeks," says Marulkar. "Palo Alto Networks gave us training on product-specific features, enabling us to then deploy each component ourselves."

Zero Malware, No Performance Impact, Simple Administration

Previously, 50 percent of malicious attempts would have slipped through the company's network. At the same time, the lightweight Traps agent has eliminated any degradation of device performance.

"We can see on the Panorama console that we have proactively blocked a huge amount of malware – there hasn't been a single instance globally, which is quite an achievement," says Marulkar. "The biggest benefit is the simplicity of the platform approach. We didn't have to invest everything on day one. Instead, we were able to evolve the security platform with cloud-delivered services. Palo Alto Networks also provides agility, meaning our rollout cycles have decreased from six weeks to just two days."

KPIT has also been impressed with the ease of administration and management. The company hasn't needed to add staff to its security team, while those on the team have more bandwidth because automation removes the need to write rules and policy.

"The intention of our digital transformation vision is based on simplicity and transparency, and Palo Alto Networks gives us the visibility and insight we need with one click," concludes Marulkar. "We don't see Palo Alto Networks as a vendor but rather as our trusted cybersecurity partner. There is a constant dialogue, and they are always keen to listen to our challenges, and help us innovate and add value to our company."