SEGA Europe

CASE STUDY

Gaming Giant Stamps Down Cyberattacks with Real-Time Threat Intelligence and Prevention

> “SEGA management is aware of cyberthreats we are facing and always understand cyber security concerns. The capabilities in the Palo Alto Networks platform played a very important role in helping us enhance our security processes. Instead of remediating, we now prevent malware or phishing attacks from causing disruption in the first place.”

Kashif Iqbal | Head of Corporate IT and Cyber Security | *SEGA Europe*

INDUSTRY

Media, Entertainment, and Technology

CHALLENGE

Gain greater visibility into network vulnerabilities across geographically distributed studios and establish a more proactive stance against increasingly sophisticated cyberthreats.

ANSWER

Palo Alto Networks Security Operating Platform provides unified next-generation security capabilities and single-pane-of-glass visibility across the enterprise with real-time threat intelligence to prevent successful cyberattacks.

SUBSCRIPTIONS

Threat Prevention, URL Filtering (PAN-DB), WildFire, GlobalProtect, MineMeld, AutoFocus, and Panorama

APPLIANCES

PA-200 (2), PA-500 (2), PA-3020 (2), PA-3050 (2), PA-5220 (2), M-100 (1)

OUTCOMES

- Transforms security from remediation to a prevention approach
- Stops zero-day attacks from disrupting the business
- Saves many hours of remediation with real-time threat intelligence
- Enforces consistent security policies across geographically distributed studios
- Simplifies policy creation and management with application-based rules

Customer Overview

SEGA Europe is the European distribution arm of SEGA Games Co., Limited, a market-leading publisher of video games and interactive entertainment. Headquartered in Brentford, Greater London, SEGA Europe wholly owns some of the brightest development studios in the gaming world, including Sports Interactive and Creative Assembly, the creators of *Football Manager* and *Total War*, respectively. The European team strives for excellence in bringing the best possible gaming experiences to its communities worldwide and is always exploring new commercial platforms, new channels to reach consumers, and new technology to keep SEGA on the cutting edge of such a fast-moving and competitive industry.

Summary

As a prolific game developer and publisher with five studios across four countries, SEGA Europe needed greater visibility into the vulnerabilities existing across its network and more granular control over application traffic to mitigate exposure to malware or other cyber exploits. By deploying the Palo Alto Networks Security Operating Platform, SEGA Europe serves its headquarters and studios with unified next-generation security capabilities and single-pane-of glass visibility. By taking advantage of application-based policies and sanctioning applications, the company adopted a philosophy of least-privileged access to regulate traffic into and out of the enterprise.

With advanced capabilities such as those of WildFire® malware prevention service and AutoFocus™ contextual threat intelligence service, SEGA Europe automatically stops zero-day attacks from disrupting its business and gains insights to identify the source IP addresses of sophisticated cyberattacks as well as prevent future attacks. In addition, GlobalProtect™ network security for endpoints enables SEGA Europe to extend consistent security to remote users, bringing an extra level of comfort and peace of mind. With the Palo Alto Networks platform, SEGA Europe has transformed from a detect-and-remediate approach to an intelligence-based, preventive security posture.

Looking for Greater Visibility into Cyber Risks

In the world of interactive electronic games, SEGA is a giant. With roots that trace back to the 1940s, SEGA (originally Service Games) has evolved over the decades from a maker of video game consoles to the world’s most prolific arcade game producer, with multimillion-dollar franchises such as *Sonic the Hedgehog*, *Total War*, and *Yakuza*. SEGA Europe is the entertainment and media publishing arm of the company that focuses on its diverse lineup of games and franchises, including *Total War*, *Football Manager* and *Company of Heroes*.

Based in London, SEGA Europe works with five world-class development studios spanning the UK, France, Bulgaria and Canada, each with its own IT department. With creative intellectual property at the core of the business, securing their infrastructure is of paramount importance. However, when Kashif Iqbal, SEGA Europe’s head of Corporate IT and Cyber Security, arrived on the job five years ago, he found a patchwork of security products and little insight into what was at risk or where cyberthreats were coming from. “We had the usual—IDS, IPS, proxies, antivirus, some elements of a SIEM—but nobody had a clue what our biggest challenges were or what our highest-risk targets were,” Iqbal says. “We lacked the visibility to even ask the right questions.”

> “The Palo Alto Networks Security Operating Platform offers such a comprehensive and unified approach to cybersecurity, we will be able to keep adding to the strong foundation we’ve built to stay ahead of threats, which grow more sophisticated every day. By continually strengthening our visibility, control, and threat intelligence, we no longer have to worry about what our users are doing. We know our network and business assets are protected.”
>
> **Kashif Iqbal** | Head of Corporate IT and Cyber Security | *SEGA Europe*

The answer to this situation was to choose a platform to serve SEGA Europe’s headquarters and the studios with unified next-generation security capabilities and single-pane-of-glass visibility. Iqbal researched the marketplace and decided to evaluate the Security Operating Platform. “I remember the first day my Palo Alto Networks rep showed up with his security engineer and started to show me what the platform could do. I said, ‘hang on a minute, you mean to tell me I can go into this monitoring tool and see the logs that happened two days ago?’ I immediately wanted to know more. And that led to talking about vulnerability and patch management, App-ID, WildFire, everything. I really liked that, if we had a vulnerability, the platform would catch exploits and prevent a successful attack before we start patching.”

You Cannot Protect What You Cannot See

Iqbal and his team began an extensive proof of concept, following the mantra, “you cannot protect what you cannot see.” Having granular control and complete visibility were top priorities, and the Palo Alto Networks platform proved it could deliver. Within a year, SEGA Europe had deployed Palo Alto Networks next-generation firewalls in its headquarters and at every studio, each configured with Threat Prevention, URL Filtering, and WildFire services.

“We got to work setting up policies that would give us visibility,” notes Iqbal. “We started sanctioning apps and adopted a philosophy of least privilege access using micro-segmentation and applying very granular policies with Threat Prevention to gain more control and to counter potential attacks. Where traffic breaks out to the internet, we have URL Filtering, which is really helpful. For example, there were some incidents where a user fell for a phishing campaign and thought the link didn’t work. That’s because it was picked up by Palo Alto Networks and blocked. The capabilities in the Palo Alto Networks platform played a very important role in helping us enhance our security processes. Instead of remediating, we now prevent malware or phishing attacks from causing disruption in the first place.”

To create efficient, effective policies, Iqbal and his team take advantage of App-ID™ technology to eliminate tedious port configurations and complex coding. Instead, they create plain language rules and specify the applications to which those rules apply. Iqbal remarks, “Moving to application-based policies was a big step for us. Instead of opening fifteen ports, we just enable a specific application, so we no longer need lines and lines of code, just a simple rule.”

Another big win for the security team is WildFire. Iqbal tells of their vision for a “magic box” that could automatically find new threats and stop them using real-time threat intelligence. “WildFire was exactly what we envisioned! We’ve seen it find zero-day attacks for us. Say a user tries to download a file with malware that has never been seen before. WildFire detects that this is a threat, and reprograms the network with protections. We were very impressed that WildFire could pick that up. And we’ve found if WildFire tells you something is malicious, it probably is. In the last four years there have been only a couple false positives, and those were on our own files.”

Extending Consistent Security to Remote Endpoints

In SEGA Europe’s larger studios, about 60 percent of the developers and artists work from home. Securing network access for those remote users was a major requirement met by GlobalProtect. With GlobalProtect, Iqbal can ensure that wherever remote users are located, they always connect to the network with the same security policies as the on-site staff who connect directly through the next-generation firewalls.

As an additional measure, Iqbal takes advantage of host information profiles (HIPs), which automatically match the security status of the remote endpoint (or end host) with defined profiles. “We call it network admission control,” says Iqbal. “The HIPs verify that any device connecting remotely to our network has the latest security patches and antivirus definitions installed, that it is properly authenticated, and otherwise complies with our security standards. It brings an extra level of comfort and peace of mind.”

Threat Intelligence Sharpens Edge Against Clever Cyberattacks

To speed threat analysis and response, SEGA Europe uses the AutoFocus contextual threat intelligence service, which provides root cause analysis, attribution, and insight into exploit behavior. AutoFocus proved its value immediately when, during deployment, SEGA Europe had an influx of spear phishing attacks. Emails were coming in and luring people into moving cryptocurrency to a specific wallet. Armed with the insight provided by AutoFocus, the security team quickly identified the source of the attackers and proactively deployed controls to stop future attacks.

“The first feedback I got on AutoFocus from the security operations team was ‘I love it,’” Iqbal reports. “They could conduct an investigation in a very efficient manner, with the ability to look at the wallet and see what IP address it's linked with, then cross-reference that with the global threat intelligence of WildFire. Now we are leveraging MineMeld with AutoFocus to analyze and extract all malicious indicators of compromise, and feed them back into the Palo Alto Networks platform. So now, if there is a malicious cryptominer somewhere out there, we will automatically extract that IP address and block it on our next-generation firewalls. AutoFocus contextual threat intelligence allows us to be more proactive in responding to attacks."

Going hand in hand with AutoFocus, the SEGA Europe security team also relies on Panorama™ management to simplify policy management and updates. For example, if Iqbal and his team determine that a certain IP address needs to be blocked based on threat intelligence sources, they can simply push an updated policy out to all the next-generation firewalls across SEGA Europe and its studios simultaneously. This saves time, minimizes the chance of human error, and ensures consistent policy enforcement.

Comprehensive, Unified Approach to Cybersecurity

On the horizon, Iqbal continues to look for additional ways to strengthen SEGA Europe's security posture and streamline threat analysis and prevention. One Palo Alto Networks offering with strong appeal is Cortex™ Data Lake (formerly Logging Service), which can serve as a centralized repository for all security data across the enterprise and clouds.

"I like that Cortex Data Lake could reduce complexity and simplify my administration," says Iqbal. "I wouldn't have to worry about backing up my logs. I'd have one place to chuck all my logs, and they'll be there when I need them."

Iqbal concludes, "The Palo Alto Networks Security Operating Platform offers such a comprehensive and unified approach to cybersecurity, we will be able to keep adding to the strong foundation we've built to stay ahead of the threats, which grow more sophisticated every day. By continually strengthening our visibility, control, and threat intelligence, we no longer have to worry about what our users are doing. We know our network and business assets are protected."