The benefits and strategic importance of

Kaspersky Web Traffic Security

the core application of Kaspersky Security for Internet Gateway

kaspersky

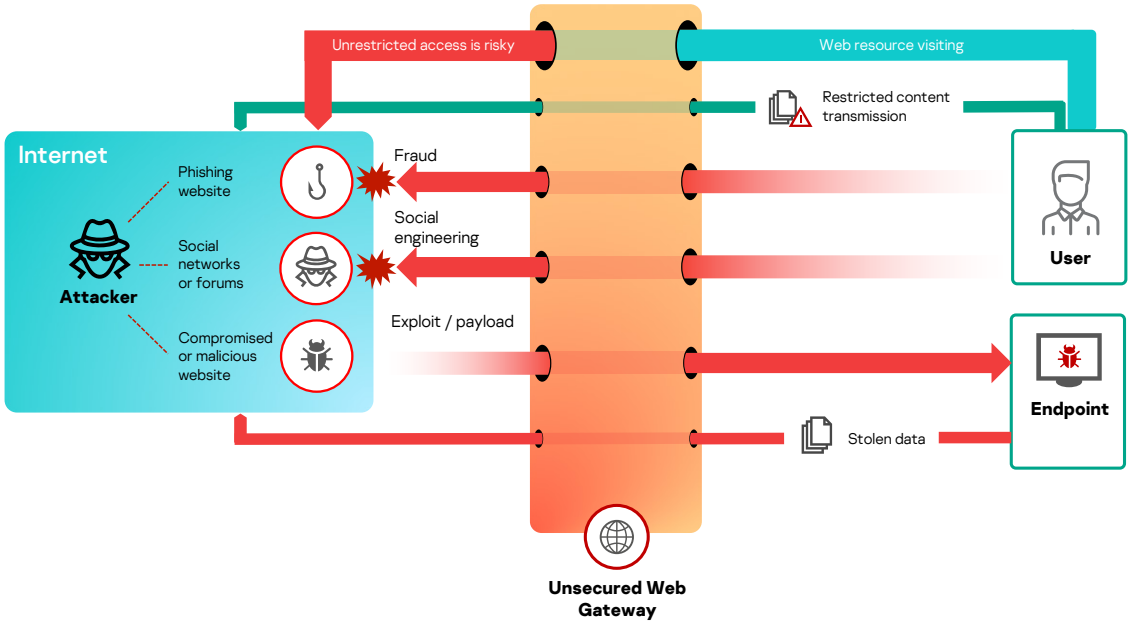
Web Gateway: a forefront to protect

A Secure Web Gateway (SWG) remains the first line defense for the majority of corporate security scenarios, despite the penetration of mobility into working processes. This is not going to change, even as it gives way to its cloud counterpart, the Cloud Security Gateway. As a natural bottleneck for all traffic passing between the corporate infrastructure and the outside world, SWG offers excellent capabilities for containing threats early and with relatively little effort.

With layered protection, mitigation of an infection before it reaches the endpoint offers a considerable reduction in risks, for example:

- At the endpoint level, the human factor is added to the equation, the impact of which is not easy to predict. The clever use of social engineering, especially if the working process doesn't allow for strict security policies, can sidestep even the most reliable endpoint-based protection. A gateway level security solution is not be affected by this.
- More risk reduction in case of gateway security layer implementation comes out of the typical preparation/testing model for the majority of malware. The attackers specifically research the endpoint, and their evasion techniques are usually focused on its specific environment. Endpoint protection is also the easiest to recreate in order to test malware. Proxy server protection is very different, and most attackers just don't bother to recreate a gateway defensive system for the sake of testing.
- When the endpoint-based protection successfully blocks malware, it usually alerts both the user and the administrator. If the attack is a mass one – or the malware has made it into the proxy server's cache – the entire network could start raising alarms with users and admin staff. This situation is likely to disrupt business operations, even more so for smaller businesses that may have a shortage of IT staff and lack a highly developed framework for dealing with these kinds of situations. In this environment, every specialist helpdesk hour adds to the financial strain – this in addition to lost revenues due to the whole disruption. Clearly, blocking the threat at an earlier stage, right at the network's entrance, can save much time and money.
- The last and the simplest: some endpoints, due to the nature of the tasks they're used for, can be deliberately left without any security solutions. Therefore, it's crucial to protect them at the gateway level.

Using an advanced threat detection solution in conjunction with a secure web gateway makes sense not only because the latter provides a gateway-level source of data for analysis. While the results of objects' deeper study are not available in real time, they can be used to prevent future deliveries of the same type, block communications with attackers' Command & Control centers, and so on, hence disrupting the targeted attack's sequence.



Without gateway protection, infections can spread

The proxy server is the one of two bottlenecks where incoming threats can be contained at the earliest stage of an attack's kill chain (the other being email). A security solution integrated with a proxy server protects the corporate IT network from the dangers of the Web and also increases productivity by governing internet use. Kaspersky Security for Internet Gateway, with its core application Kaspersky Web Traffic Security, offers this and more, being able to replace - or complement - the corporate web gateway with all-in-one Secure Web Gateway appliance. It can also act as an instrument for automated response when coupled with Kaspersky Anti Targeted Attack (KATA) solution.

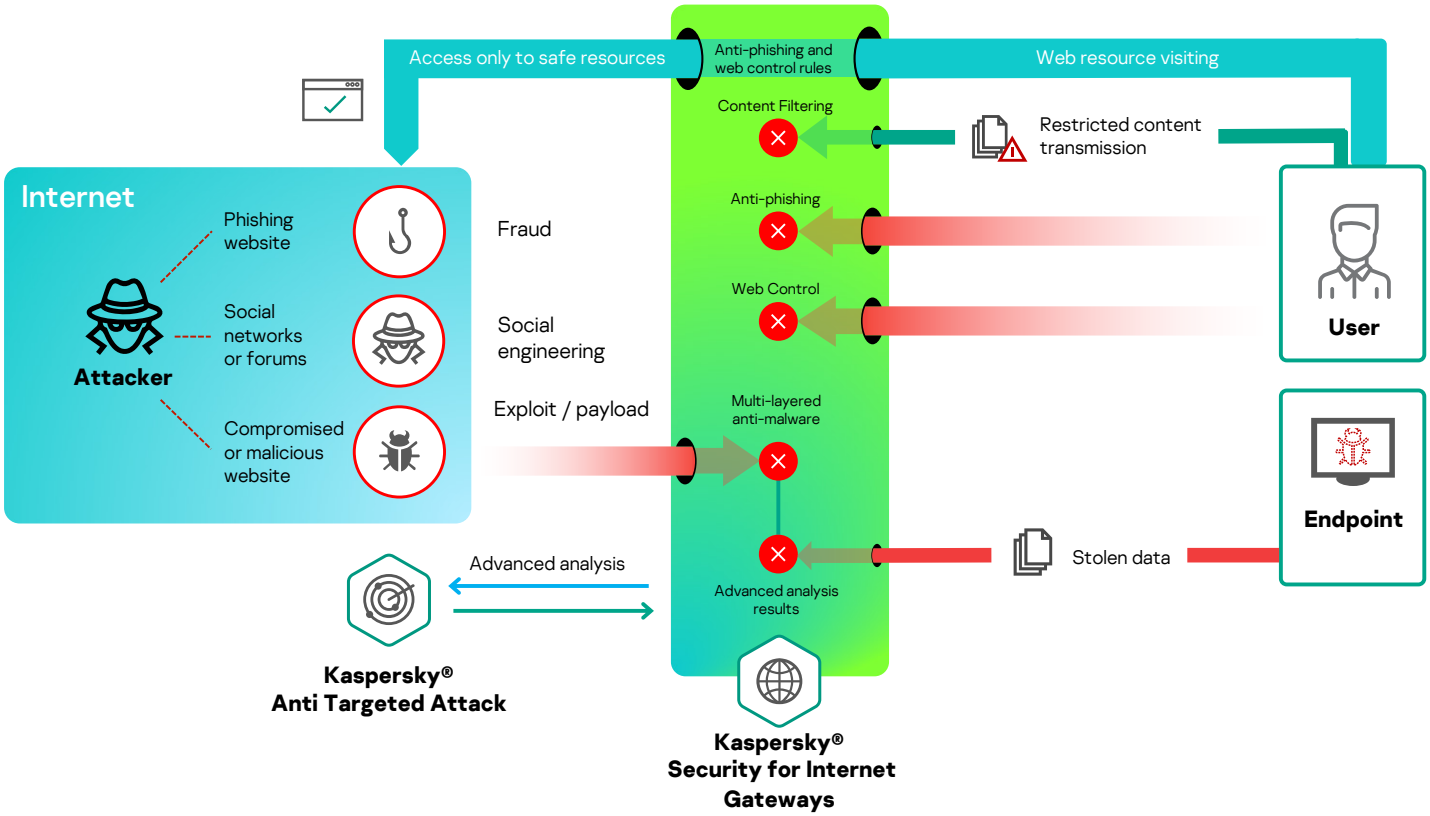
Key features and benefits of Kaspersky Security for Internet Gateway:

- Protects against the majority of web-delivered threats, including malware, ransomware and miners. Given the high rate of re-use of older tactics and techniques, static machine learning-based algorithms and emulative sandboxing filter out 95% of incoming threats.
- Precisely detects the newest threats without any false positives immediately after their discovery by Kaspersky – right from Kaspersky Security Network cloud; no waiting for updates.
- To simplify deployment, the solution is also offered as an all-in-one, ready-to-use Secure Web Gateway (SWG) virtual appliance, complete with a pre-configured proxy server ready to work with the bundled security application.
- The solution's architecture allows for the easy implementation of corporate traffic monitoring (also known as 'SSL/TLS bumping'). This controls and secures SSL/TLS-encrypted web traffic – essentially the de-facto standard for Internet communications.
- Leverages extensive threat intelligence together with specialized heuristic algorithms to block malicious and phishing websites - as well as web-based cryptocurrency miners - before the user is threatened.
- For high-load systems, the solution is scalable, offering multi-node, hierarchical deployment and high availability (HA) options.
- The demonstrable increase in targeted threats means that not just large enterprises, but also small to medium businesses, must be mindful of the possibility of becoming a victim of a targeted attack. The risk of this kind of attack succeeding is reduced considerably by the availability of a targeted attack-related hosts database, constantly updated by renowned Kaspersky APT hunters.

  And if your business is able to buy Kaspersky Anti-Targeted Attack (KATA), Kaspersky Web Traffic Security can integrate with it as a web sensor, further boosting its detection capabilities – and also use the verdicts provided by its advanced detection mechanisms to disrupt the attack's kill chain and prevent it from succeeding.
- The transmission of certain file types moving in and out of the network can be restricted by Content Filtering. This reduces the risks of infection and sensitive data leaks.
- Effective Web Control scenarios can be implemented to restrict the use of specific categories of web resources; custom rules can also be created. This can substantially lessen the chances of infection – certain web resources, such as those serving pirated software or illegal content can double as malware websites. This can also help boost productivity by preventing distractions.
- Good visibility is key to successful incident response. Kaspersky Web Traffic Security has broad capabilities that help administrators to react promptly to events requiring their attention. These include a web-based dashboard for event tracking, event-centric threat analysis and integration with existing Security Information Event Management (SIEM) systems.
- For managed service providers (MSPs) and diversified businesses, the multi-tenancy function facilitates the management of multiple systems from a single console. Each can have their own administrator with role-dependent privileges and an independent set of policies. At the same time, top-level global policies covering all tenants can be configured as well.
- For companies and institutions operating with highly sensitive data and/or with a low tolerance for security incidents, it makes absolute sense to employ Kaspersky Web Traffic Security application alongside existing web gateway protection. As a powerful additional security layer, Kaspersky Web Traffic Security boosts detection rates without generating additional false positives.
- Telecoms/xSPs interested in offering value-added services, such as blocking malicious objects and URLs in their customers' web traffic, aren't usually concerned with granular management and protection fine-tuning. They only need good performance and easy deployment within their existing infrastructure, and often go for multi-vendor traffic protection to boost protection effectiveness.
- Kaspersky Web Traffic Security is easily trimmed down, enabling only those security layers that are really necessary, thus further boosting performance levels. Flexible deployment options (application packages vs. an all-in-one appliance) support different infrastructure configurations, allowing either mono-vendor defense based solely on Kaspersky's solution, or multi-vendor protection of the same traffic 'tube'.

Conclusion

The value of forefront protection for any company's security cannot be overestimated. Having every level of your IT network covered with a comprehensive range of security solutions from Kaspersky – and establishing your corporate defenses at the earliest stages - will keep your business data safe and your business continuity on track.



Kaspersky Security for Internet Gateway blocks threats before they reach the user

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven. Transparent. Independent.