

Trend Micro delivers security cloud

Trend Micro is shifting the burden of anti-malware signature scanning from customer endpoints into Trend's Smart Protection Network. This dramatic move is mandated with the realization that trying to distribute thousands of attack signatures per day to millions of endpoints in a timely manner is not a viable approach. Trend's innovative strategy enhances its detection network to also prevent attacks from even reaching customer endpoints and enterprise networks. The Ogren Group believes that signature scanning is best delivered as a service, and the new strategy places Trend Micro in a firm position to grab market share.

Trend Micro is extending their Smart Protection Network to correlate Web, email, and file attachment activity "in the cloud" to quickly detect and mitigate attacks against PCs. This is a major innovation by one of the Big 4 endpoint security vendors (McAfee, Microsoft, and Symantec being the other three) that looks very promising. Trend is one of the first vendors using the power of its world-wide attack detection network to directly prevent know attacks from reaching customer PCs. If done properly, users will get an approach to security that evolves as attacks evolve without excessive performance demands on the endpoint or pressures on IT to distribute signature updates.

Trend recognized that the traditional method of distributing signatures out to endpoint has been rendered obsolete by the exploding number of attacks and the speed in which these attacks do their damage. The result is an approach that leaves behavioral, heuristic, and whitelist filters in a thin client on the endpoint while processing signature checks against known attack profiles in the cloud as part of the Trend Micro Smart Protection Network. The Ogren Group believes that this is a truly innovative approach that can better protect endpoint devices and nicely positions Trend Micro to meet future security requirements. Customers that had assumed the burden of security can now let security clean traffic before it enters corporate endpoints.

Why Trend Micro's announcement is exciting

The Ogren Group believes that shifting the balance of power into the cloud is an approach that with careful execution may give Trend Micro a sustaining advantage in endpoint protection. The rate of attack discovery makes distribution of new signatures impractical. There are way too many attacks for traditional approaches relying on comparing against signature files to keep up. It is simple arithmetic - the discovery rate of new attacks (several thousand per day according to the independent AV-Test organization) far surpasses the ability for any security vendor to distribute up to date signature files to endpoints in any kind of effective timeframe. The most logical security

approach is to route traffic through a security service where it can be analyzed and scrubbed before it reaches your PC.

- **Enhanced detection:** Enhancing the Smart Protection Network with file reputation algorithms to existing email and Web site intelligence presents a more comprehensive view of malicious activity. Malicious attacks typically spread from spam email, infected web sites, and files that are attached to email messages or web downloads. Associating file activity, especially file containing executable code, with attacks gives Trend a powerful detection capability.
- **Enhanced protection:** A single action by Trend Micro technicians in the Smart Protection Network instantly protects the entire Trend customer base against the new attack. IT organizations that previously raced to apply signature updates before an attack could strike now are automatically protected without having to distribute new signatures. The latency of distributing signatures has finally been driven out of the endpoint security model.
- **Enhanced endpoint performance:** The new approach places intensive computation processing in the cloud, and leaves a thin agent on the endpoint to monitor behavioral heuristics and application white-lists for compliance with corporate security policy. With traditional endpoint security, the customer bears the burden of updating profiles of attack signatures, allocating storage for entire signature dictionaries, and donating processing performance for scanning. The new approach returns a significant level of performance to the end-user.
- **Enhanced corporate positioning:** Trend's security service fundamentally improves the long-term ability of Trend Micro to better protect enterprise and consumer endpoints. The Smart Protection Network can be leveraged with to increase parallel processing for performance, to insert new algorithms into its attack correlation system, and to optimally block malicious attacks at the email, Internet, and file levels.

Modern attacks are designed to steal electronic secrets using combinations of email spam, infected Web sites, and malicious code engines. Anti-malware techniques now require intelligent correlation of Web activity, messaging patterns and deep file content inspection to trace the origin of an attack and to mitigate the attack before damage occurs. For instance, it is one thing to tell if a file is corrupted on a PC, but it is far better if security can say that the file became corrupted after visiting a specific URL. Trend Micro can then apply an antidote filter that would instantly block the offending site for the entire Trend Micro user community – without distributing a single signature.

The Bottom Line Impact

While other endpoint security vendors are trying to improve the performance of traditional schemes or are bundling commoditized features to maintain price points, Trend Micro is embarking on a journey that promises to enhance protection for consumers and enterprises alike. The bottom line is that a cloud-based service has the world-wide visibility of malicious activity to be more effective than host-based systems in detecting new attacks, identifying the root source of the attack, and efficiently preventing attacks from reaching customer endpoints. The Ogren Group believes that Trend Micro is nicely positioned to leverage its Smart Protection Network in offering advanced detection algorithms and possibly even delivering pattern-matching oriented data loss protection services in the cloud. Organizations looking for more effective endpoint security are advised to look at the new Trend Micro offering.