Castellum Labs

WHITE PAPER 2021

End-Point Security. Most Critical. Even Today!

Endpoint security has been around, for at least three decades, since the intro, proliferation and mass adoption of personal computers, PCs, as productivity workstations in enterprises. And, it has evolved from being simple scan of what is present on your computer to 'heuristics based identification and interception' of threats.

Castellum Labs

WHITE PAPER 2021

Despite evolution in security technologies and solutions for endpoints, PCs and mobiles continue being susceptible to increasing level and severity of threats in rapidly changing computing environment. This article is an attempt to explore the reasons of continuous challenge to endpoint security. And, why CISOs and CIOs should consider 'endpoint protection portion' of security as one of the most important in their overall security strategy and planning.

- Signature based scan approach to heuristic based identification of threat
- Security content research and content delivery to endpoint DB
- Behavior and reputation data collection and usage at end point
- Real time consumption of threat data supplied by third party products
- Consolidation of 'type of protection' into single 'end-point protection'

Despite all this evolution, and, a wide adoption of endpoint solutions, threats to an organization at the endpoint are more severe than ever. These threats are caused by various elements and actors in today's computing and info setup.

" Shake hands with well crafted endpoint security strategy "

From Sprawl to Mobility Driven Explosion

Not only more endpoints more dispersed than ever!

Endpoint devices have exponentially grown in almost all enterprises because of mobile devices, their computing capacity and their utility to someone on the move. Security of endpoint in large sprawl of organizations was relatively easier as compared to fortifying endpoints when someone is accessing enterprise data on a mobile device in both 'connected' and 'disconnected' state. Traditional methods of protecting static information and content living at the endpoint does not work anymore, when people have it in their hands within their mobile with ever increasing computing and communication capabilities.

Endpoints and its security for CISOs and CIOs should have one of the top most priority. The above mentioned situational realities of today's computing world can help form a strategic thinking framework, to design a strategy for endpoint security.

An approach to "watching information movement" and taking security measures with "context of that movement" needs to be adopted at the endpoints of the today, which are largely mobile and carry superior computing power than PCs of 10 years ago. Such an approach is not possible with today's limited ability of heuristics based identification of threats.

User Behaviors are More Complex Today

User behaviors are not access patterns anymore!

Users behavior in a mobile world, where device in their hands is powerful and carries multi mode multi channel communication ability, are lot more complex. Users do a lot more on their mobile than just open an application or open some document and that poses a significant challenge to getting a grip on behavior & its patterns. Given the computing powers and availability of options, users have a lot more complex behavior in terms of their interaction with their mobile and info in it.

Most of the user behavior technology is based on "access pattern identification" and its storage in a static database for later usage. It served well in the days of PCs or even lower capacity mobile, when user's actions and their access had a predictable routine which could be identified and recorded as simple patterns.

Today's identification of user behaviors and using it to secure the information and access needs to shift towards context capturing.

Castellum Labs

WHITE PAPER 2021

Debilitating Threats are Mostly Real Time !

While threat/signature DB has research lag...!

Other than the usual suspects, quite a many threats today, even to endpoint are emerging on a continuous basis.. out there.. in the wilds of internet. And, the databases of threat elements, which are the basis of identification & intercepting a threat have a natural time lag. This time lag is the time which a vendor takes to notice a threat.. run it in their research lab.. prepare the threat signature and.. release it for endpoint DB update. This time lag exposes endpoint to significant risk which is posed by a threat which is known, identified, but has not been released by vendor yet, to be updated in their endpoint DB.

Though real time consumption of threat feed can address some of this issue, but, adoption of such feeds on a mass basis in enterprises has not started happening yet.

Hybrid Computing has its own Security Challenges

Security at the intersection of in-premise endpoint and in cloud resource!

Most of the companies today have hybrid models of computing infrastructure, where part of their servers and information is within their premise and part of it lives on cloud infra offered by a variety of vendors. Such hybrid infrastructure and its access to end users from their devices poses a "complete set of security challenges". Some of the endpoint security, in this specific case, ought to be at the virtual boundary of endpoint and cloud infra and access channels there.

Today, a good set of security options exist for cloud infra to protect a company's assets in the cloud. And, then there are protection technologies which take care of endpoints within enterprise boundaries. There seem to be lack of clear tech options when it comes to protecting the enterprise assets in context of endpoint interaction with cloud resources and in-house resources. For the most part, even today endpoint security in this context is mostly patchwork which an enterprise has to put together. To stay secure in a hybrid environment.

Information Lives in Silos

More than ever, now!

Information 'living in silos' was a perpetual troubling issue for organizations for long period of time. And, organizations went in overdrive over decade and half to ensure those silos are broken. Some of it simplified security of content & information, specifically for the organizations, which responded to information silos with consolidation of information to single place. Implementing security with a consolidated information infra was relatively simple.

But today, when you have the choice of dozen of different office productivity apps available in SaaS and cloud model, and many of them for free, it is impossible to ask people to use "one information repository" or use "one central productivity" app hosted within comfortable and secure confines of enterprise. A call between what is efficient and what is secure needs to be made and it is a real difficult call.

Most organization find it difficult today to create a clear approach to this, and, hence have continuous challenge at their endpoints, specifically mobile ones, where its employees might be using dozen different work related apps.

Movement of info and content across media

Information does not live at one place, anymore!

Today almost all info and all content, once accessed, can be rapidly moved from one form of storage device to another form of storage device. A file or an info piece, which may have been accessed & retrieved from a single secure repository can rapidly move from PC to mobile to mail to flash storage to USB drive. Most of our current protection at end point which relates to the content storage is based on interception of access and validating the access with a policy server.

When movement of content across storage places and format can take as rapidly as is possible today, an access and copy based protection method is not good enough at endpoints. An approach to movement based data leak prevention will probably help better in protecting the endpoints from data leakage.

Access to External Environment

Switching between an internal access to an external one is a routine!

Possibility is that your endpoints have a lot more interaction with external info infrastructure as compared to any of your server and storage infra. Well, unless the server is a web server with an external facing portal or application. A mobile device could be interacting with something on the cloud, an app on local storage, a website on internet and an application within your enterprise, all at the same time. This creates a wish garden for advanced persistent threat elements. Many of the "Advanced Persistent Threats" can take the benefits of a mobile device accessing multi modal and multi format info and resources across the enterprise and its boundaries.

Protecting your endpoint devices against intrusions and corresponding APT type of threats is not only difficult, it also needs advanced solution approach.

”

Endpoint security was always very important, it continues being so, even more critical than ever!

Castellum Labs

+91 97009 70397 info@castellumalbs.com www.castellumlabs.com

WHITE PAPER 2021